Organisatorische Betrachtung der Durchführung eines Phishing-Awareness-Trainings

Bachelorarbeit

im Studiengang Wirtschaftsinformatik

Vorgelegt von

Severin Zimmermann

am

27.05.2023

an der ZHAW School of Management and Law

Betreut von

Dr. Tim Geppert

Management Summary

In den letzten Jahren haben Phishing-Angriffe immer mehr zugenommen. Diese Tendenz wird unter anderem durch den Faktor «Mensch» geprägt, welcher für die Mehrheit der Cybersicherheitsvorfälle verantwortlich ist. Um sich vor Phishing-Angriffen zu schützen, wird in der Praxis vermehrt auf das Phishing-Awareness-Training zurückgegriffen. Dementsprechend wird das Thema «Phishing-Awareness-Training» in der wissenschaftlichen Literatur umfangreich diskutiert. Dabei wird mehrheitlich auf die Effektivität oder auf bestimmte Methoden und Tools von Phishing-Awareness-Trainings eingegangen. Hingegen kaum untersucht wird in der wissenschaftlichen Literatur die organisatorische Sicht eines Phishing-Awareness-Trainings.

Die vorliegende Arbeit greift diese Lücke auf und untersucht die Durchführung eines Phishing-Awareness-Trainings aus der organisatorischen Sicht. Zu diesem Zweck wird das Technology-Organization-Environment-Framework kurz TOE-Framework verwendet. Für jeden Blickwinkel aus dem TOE-Framework werden in der Arbeit Chancen und Risiken ermittelt. Ebenfalls wird in der Arbeit untersucht, wie ein Phishing-Awareness-Training bei den Mitarbeitenden aufgenommen wird.

Die Ermittlung der Chancen und Risiken aus den TOE-Blickwinkeln erfolgt zum einen anhand einer systematischen Literaturrecherche, zum anderen anhand von Experten:inneninterviews. Bei beiden Vorgehen werden eine deduktive und eine induktive Kategorienbildung angewendet. Die Untersuchung der Wahrnehmung des Trainings bei den Mitarbeitenden erfolgt anhand eines bereits erhobenen Datensatzes aus dem OptiPhish-Projekt, welcher mittels einer deduktiven und induktiven Kategorienbildung ausgewertet wird. Die Erkenntnisse, die aus der Literaturrecherche, den Experten:inneninterviews und dem Datensatz resultieren, werden einander gegenübergestellt und miteinander verglichen.

Aus der Gegenüberstellung resultierten in allen Bereichen des TOE-Frameworks generelle Chancen und Risiken. Die Chancen beinhalten unter anderem Risikominimierungen, die Sensibilisierung der Mitarbeitenden auch im Privatleben, das Aufzeigen technischer Grenzen bei der Abwehr von Phishing-Angriffen und die Reduzierung rechtlicher Konsequenzen. Ausserdem ergaben sich generelle Risiken, die unter anderem Folgende umfassen: hohe Zeitaufwendungen bei den Mitarbeitenden, Verärgerung der Mitarbeitenden,

Erstellungen von Sicherheitslücken bei Freischaltungen als auch weitere Risiken. Neben den generellen Risiken ergaben sich auch gestalterische Chancen und Risiken, welche sich anhand des Aufbaus des Trainings ergeben, wie beispielsweise die Erkennung echter Phishing-Angriffe oder die Überlastung des Servicedecks, wenn eine Meldeplattform integriert wird.

Aufgrund der zunehmenden Bedrohung durch Phishing-Angriffe wird für die Praxis ein kontinuierliches Phishing-Awareness-Training angeraten. Für die Implementierung des Phishing-Awareness-Trainings wird ebenfalls empfohlen, die in dieser Arbeit ermittelten generellen und gestalterischen Chancen und Risiken zu beachten. Jedoch sollten die Chancen und Risiken industrie- und landesspezifisch beurteilt werden.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

CISO	Chief Information Security Officer
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
ISTE	Information Security Training and Education
SaaS	Software as a Service
SOC	Security Operations Center
SPF	Sender Policy Framework
TOE	Technology-Organization-Environment
URL	Uniform Resource Locator
ZHAW	Zürcher Hochschule für Angewandte Wissenschaften

Vorwort/Danksagung

In diese Arbeit waren diverse externe Parteien involviert, welche mich unterstützt haben. Bei diesen Parteien möchte ich mich hiermit bedanken.

Ein besonderer Dank gilt Dr. Tim Geppert für die Betreuung sowie die kritischen Anregungen zur vorliegenden Arbeit.

Ebenfalls ein besonderer Dank gilt allen Interviewpartnern, die sich Zeit für diese Arbeit genommen haben und wertvolle Erkenntnisse lieferten. Nur mit ihrer Hilfe war es möglich, die Arbeit in diesem Rahmen durchzuführen.

Severin Zimmermann

1 Einleitung

Der technologische Fortschritt schreitet schnell voran und mit ihm die Gefahr von Cyberkriminalität (SoSafe, 2023). Eine beliebte Art der Cyberkriminalität ist dabei das sogenannte E-Mail-Phishing. Beim E-Mail-Phishing werden von den Betrügenden Social-Engineering-Taktiken angewendet, die ihre Opfer dazu verleiten sollen, sensitive Informationen preiszugeben oder Schadsoftware zu installieren (NIST). Die Betrügenden versuchen, ihre Opfer dazu zu animieren, auf einen Link zu klicken oder einen Anhang herunterzuladen und zu öffnen (NIST). Mit dieser Technik versuchen die Cyberkriminellen, die Zugangsdaten ihrer Opfer zu erlangen oder das System mit einer Schadsoftware zu kompromittieren. Um sich vor solchen Angriffen zu schützen, müssen Unternehmen geeignete Massnahmen ergreifen. Eine weitverbreitete Massnahme ist das Schulen der Mitarbeitenden, bei dem diese für solche Angrife sensibilisiert werden und dadurch das Risiko, von einem Phishing-Angriff betroffen zu sein, minimirt wird (Alabdan, 2020, S. 24; Kävrestad et al., 2022, S. 2; Steves et al., 2020, S. 1).

Diese Arbeit untersucht die Durchführung eines Phishing-Awareness-Trainings aus der organisatorischen Perspektive. Für die Untersuchung werden verschiedene Blickwinkel eingenommen. Die Blickwinkel beziehen sich auf die interne, die externe sowie die technologische Sicht gemäss dem «technology-organization-environment framework», kurz TOE-Framework, nach Tornatzky et al. (1990). Ziel ist es, unterschiedliche Aspekte zu identifizieren, die aus der Durchführung eines Phishing-Awareness-Trainings resultieren können. Die identifizierten Aspekte werden anhand des TOE-Frameworks kategorisiert und können entweder eine Chance oder ein Risiko darstellen.

Die Untersuchung teilt sich in drei Bereiche auf. Im ersten Schritt wird die aktuelle Literatur auf mögliche Aspekte, welche durch die Durchführung eines Phishing-Awareness-Trainings entstehen können, untersucht. Im zweiten Schritt werden Experten, die umfangreiche Erfahrungen mit der Durchführung eines Phishing-Awareness-Trainings besitzen, interviewt. Ziel des zweiten Schritts ist es, die Aspekte, welche in Praxis tatsächliche Relevanz besitzen, zu identifizieren. Im dritten Schritt werden die Erkenntnisse aus der Literatur und die Erkenntnisse aus den Experten:inneninterviews zusammengeführt. Daraus resultieren generelle Aspekte, welche unanbängig von der Gestaltung des Trainings entstehen, und gestalterische Aspekte, die sich aus bestimmten Gestaltungsformen, wie die Verwendung von Belohnungen oder Bestrafungen, ergeben.

Neben der organisatorischen Betrachtung der Durchführung eines Phishing-Awareness-Trainings wird in dieser Arbeit zusätzlich die Wahrnehmung der Geschulten begutachtet. Als Grundlage für die Betrachtung der Wahrnehmung von Geschulten dient das OptiPhish-Projekt, eine von der Zürcher Hochschule für Angewandte Wissenschaften, kurz ZHAW, durchgeführte Studie. Im OptiPhish-Projekt wurden unter anderem 31'940 Probanden mit simulierten Phishings konfrontiert und es wurde ihr Verhalten untersucht (Sutter et al., 2022, 3). Im Anschluss an die Studie wurden 1339 zufällig ausgewählte Probanden mittels Fragebogen zur Studie befragt, wobei sich 487 Rückmeldungen ergaben. Der daraus entstandene Datensatz wurde im Rahmen des OptiPhish-Projekts noch nicht weiter untersucht, weshalb er in dieser Arbeit als empirische Datenquelle verwendet und augewertet wird. Im Datensatz werden vorzugsweise die individuellen Rückmeldungen betrachtet. Diese individuellen Rückmeldungen werden dabei in die Kategorien der positiven und der negativen Wahrnehmung von Phishing-Awareness-Trainings eingeteilt. Anschliessend wird untersucht, inwiefern die Anfälligkeit der Geschulten Einfluss auf die Wahrnehmung des Phishing-Awareness-Trainings hatte. Die Anfälligkeit wird anhand der Rückmeldungen der strukturierten Fragen sowie der persönlichen Rückmeldungen beurteilt und in einen Kontext damit gesetzt, ob die jeweiligen Mitarbeitenden auf ein Phishing hereingefallen sind oder nicht. Ziel ist es zu identifizieren, ob die Anfälligkeit einen Einfluss auf die Wahrnehmung gegenüber Phishing-Awareness-Trainings besitzt.

Mit dieser Arbeit wird ein Beitrag zur Forschung über die Durchführung eines Phishing-Awareness-Trainings geleistet. Zudem gibt die Arbeit Unternehmen einen Überblick über die Aspekte, die aus der Durchführung eines Phishing-Awareness-Trainings resultieren können. Die Aspekte können sowohl Chancen sein, die durch das Training entstehen und den Unternehmen dabei helfen, ihre Phishing-Trainings besser zu organisieren, als auch Risiken, die sich bei der Durchführung von Phishing-Awareness-Trainings ergeben können.

1.1 Problemstellung

Phishing ist ein zunehmendes Problem, das die Online-Sicherheit von Unternehmen und Verbrauchern gefährdet (APWG, 2022; DBIR, 2020). Angreifer nutzen gefälschte E-Mails, Websites und andere Methoden, um vertrauliche Informationen wie Passwörter, Bankdaten oder andere private Daten zu stehlen (Jampen et al., 2020, S. 1). Gemäss einer öffentlichen Ankündigung des Federal Bureau of Investigations Public Service Announcements (2020) werden die durch kompromittierte E-Mails entstandenen Kosten für US-Unternehmen in den Jahren 2014–2019 auf 2,1 Milliarden US-Dollar geschätzt. Um sich vor solchen Angriffen zu schützen, setzten viele Unternehmen eine zweistufige Abwehrstrategie ein. Diese zweistufige Abwehrstrategie beinhaltet zum einen den technischen Schutz, bei dem Systeme so konfiguriert werden, dass diese Phishing selbstständig erkennen und blockieren, und zum anderen einen menschlichen Schutz, bei dem die Mitarbeitenden sensibilisiert werden (Alabdan, 2020, S. 23; Huang & Pearlson, 2019, S. 6406; Wash & Nthala, 2021, S. 387). Die technischen Schutzmassnahmen sind von essenzieller Bedeutung, da es schwierig ist, alle Benutzenden immer aufmerksam zu halten (Mims, 2016). Dennoch reicht es nicht aus, wenn sich Unternehmen nur auf technologische Abwehrmassnahmen zu beschränken (Talley, 2018). Cyberkriminelle entwickeln immer wieder neue Möglichkeiten, technische Sicherheitsmassnahmen zu umgehen, und gelangen so an den Menschen, der letztlich über Legitimität oder Phishing entscheidet (Proctor & Chen, 2015). Dabei besteht die Gefahr, dass das Fehlverhalten eines einzelnen Benutzenden die Sicherheit einer Unternehmung bedrohen kann (Lambat et al., 2021, S. 17). Zusätzlich zeigt sich die Gefahr auch darin, dass die meisten Sicherheitsverletzungen im Bereich von Cybersecurity aus dem Fehlverhalten der Benutzenden resultieren und nicht durch technische Fehler entstehen (Ebner, 2018, S. 46). Gemäss Wilkinson (2022) soll der menschliche Faktor sogar für mehr als 80 % der Sicherheitsverletzungen verantwortlich sein. Damit diese Gefahr reduziert und die zweite Schicht der Abwehrmassnahme gegen Cyberbedrohungen gestärkt werden kann, ist das Phishing-Awareness-Training nach wie vor eine der beliebtesten Methoden (Alabdan, 2020, S. 24; Kävrestad et al., 2022, S. 2; Steves et al., 2020, S. 1). Im Bereich «Phishing-Awareness-Training» gilt das eingebettete Training als die effektivste Methode (Kweon et al., 2021, S. 361; Steves et al., 2020, S. 1). Die Effektivität des Phishing-Awareness-Trainings belegt, dass die Implementierung und Pflege eines Phishing-Awareness-Trainings in jeder Unternehmung beachtet werden sollte. Alwanain (2019, S. 323) geht sogar einen Schritt

weiter und empfiehlt, die Schulung von Mitarbeitern speziell im Bereich «Phishing» als obligatorische Pflicht einzuführen.

1.2 Forschungslücke

Das Thema «Phishing und Phishing-Awareness» ist in der Literatur umfangreich diskutiert. Die Aspekte, welche in der Literatur aufgegriffen werden, befassen sich grösstenteils mit Folgendem:

- dem Verhalten und den Eigenschaften der Mitarbeitenden und dem Zusammenhang mit der Anfälligkeit gegenüber Phishing,
- der Art und dem Aufbau und dessen Effektivität bei Phishing-Awareness-Trainings,
- den Normen und Richtlinien für den Aufbau einer Cybersicherheitskultur;
- dem Aufbau und der Implementierung von Warnhinweisen oder Meldeplattformen,
- den technischen Abwehrmassnahmen gegenüber Phishing,
- dem Einbezug externer Firmen bei der Durchführung eines Phishing-Awareness-Trainings.

Die Forschenden untersuchen in diesen Bereichen meistens die Durchführung und die Effektivität bestimmter Lösungen und nicht die Organisation eines Phishing-Awareness-Trainings. Jedoch lassen sich in den Literaturen Hinweise auf mögliche organisatorische, technische oder umfeldbezogene Aspekte identifizieren. Beispielsweise sprechen Kumaraguru et al. (2009) die Thematik an, dass Mitarbeitende aufgrund der Schulung auch keine legitimen Links mehr anklicken, und Butavicius et al. (2020) merken die Problematik eines übermässigen Vertrauens in die Technik oder die eigenen Fähigkeiten an. Diese organisatorischen Aspekte werden in der Literatur erwähnt, jedoch nicht genauer betrachtet. Die Durchführung eines Phishing-Awareness-Trainings aus organisatorischer Sicht wird in der Literatur bis anhin nur von Volkamer et al. (2020) thematisiert und behandelt. Aufgrund dessen wird das Thema der organisatorischen Durchführung eines Phishing-Awareness-Trainings noch nicht ausreichend kritisch behandelt.

1.3 Forschungsfrage

Wie in Kapitel 1.2 erläutert wurde, ist das Phishing-Awareness-Training ein in der Literatur viel diskutiertes Thema. Die Forschenden untersuchen dabei weitgehend die Durchführung und Effektivität bestimmter Lösungen von Phishing-Awareness-Trainings. Kaum untersucht ist jedoch die organisatorische Perspektive bei der Durchführung von Phishing-Awareness-Trainings. Die vorhandene Literatur liefert in den meisten Fällen nur Hinweise auf mögliche Aspekte, welche jedoch nicht im Fokus der eigentlichen Arbeit stehen. Dieser Arbeit knüpft an der vorhandenen Forschung an, untersucht diese Hinweise und hinterfragt bestehende Aspekte kritisch. Im Mittelpunkt dieser Arbeit steht die Frage:

Welche Chancen und Risiken ergeben sich entsprechend den TOE-Blickwinkeln bei der Durchführung eines Phishing-Awareness-Trainings?

Für die Beantwortung der Forschungsfrage wurden vier Arbeitsfragen entworfen, die als Grundlage dieser Arbeit dienen. Die Arbeitsfragen helfen, die Arbeit zu strukturieren und die Forschungsfrage präzise zu beantworten. Die vier leitenden Fragen werden im Folgenden genannt und als AF1–AF4 bezeichnet.

AF1: Wie wird ein Phishing-Awareness-Training von den Teilnehmenden aufgenommen?
AF2: Welche organisatorischen Aspekte ergeben sich bei der Durchführung eines Phishing-Awareness-Trainings?
AF3: Welche Aspekte im Umfeld ergeben sich bei der Durchführung eines Phishing-Awareness-Trainings?
AF4: Welche technischen Aspekte ergeben sich bei der Durchführung eines Phishing-Awareness-Trainings?

1.4 Abgrenzungen

In dieser Arbeit wird die Durchführung eines Phishing-Awareness-Trainings aus der organisatorischen Sicht untersucht. Für die Untersuchung werden eine Literaturrecherche sowie Experten:inneninterviews durchgeführt und diese aus Sicht des TOE-Frameworks

betrachtet. Nicht Bestandteil dieser Arbeit ist die Untersuchung der Effektivität unterschiedlicher Trainingsmethoden oder der Effektivität unterschiedlicher Aufbauarten des Phishing-Awareness-Trainings. Ebenfalls werden keine technischen Abwehrmassnahmen gegen Phishing-Angriffe untersucht. Die Datenerhebung besteht in der vorliegenden Arbeit aus drei Bestandteilen. Der erste Teil beinhaltet eine systematische Literaturrecherche zum Thema «Phishing-Awareness-Training». Der zweite Teil der Datenerhebung wird mithilfe von Experten:inneninterviews und deren Transkription erstellt. Der dritte Teil der Datenerhebung erfolgte im OptiPhish-Projekt, wobei mittels Umfrage die Geschulten des OptiPhish-Projekts befragt wurden. Im Rahmen dieser Arbeit werden ausser den oben genannten Datenquellen keine weiteren Datenerhebungen durchgeführt.

1.5 Beitrag der Arbeit

Diese Arbeit liefert einen Beitrag sowohl für die zukünftige Forschung als auch für die Praxis. Der Praxisbeitrag soll Unternehmen einen Überblick über die Aspekte geben, die aus der Durchführung eines Phishing-Awareness-Trainings resultieren können. Diese Aspekte können mögliche Chancen für die Unternehmen aufzeigen, aber auch Risiken, welche bei der Durchführung eines Phishing-Awareness-Trainings beachtet werden sollten. Der Beitrag zur Forschung resultiert entweder aus den in der Literatur gewonnenen Erkenntnissen, welche nicht anhand der Experten:inneninterviews für die Praxis bestätigt werden konnten, oder aus den durch die Experten:inneninterviews gewonnenen Erkenntnissen, welche nicht anhand der Literatur bestätigt werden konnten. Diese einseitig gewonnenen Erkenntnisse liefern Hinweise darauf, welche Aspekte in der Literatur, aber nicht in der Praxis relevant sind, oder umgekehrt, welche Aspekte in der Praxis relevant sind, jedoch noch nicht in der Literatur untersucht oder festgestellt wurden. Anhand dieser Hinweise können zukünftige Forschungen stärker auf die Thematik eingehen und die Relevanz der Aspekte genauer betrachten und beurteilen.

1.6 Relevanz

Die steigenden Cyberbedrohungen insbesondere im Bereich der Phishing-Angriffe, wie in Kapitel 1.1 beschrieben, verdeutlichen die Aktualität und die Relevanz des Themas

«Phishing-Awareness-Training». Aufgrund dieser Aktualität beschäftigen sich viele Forschungen mit der Effektivität, der Gestaltung und möglichen Phishing-Awareness-Programmen. Jedoch wird in der Literatur die organisatorische Durchführung eines Phishing-Awareness-Trainings kaum betrachtet. Wie in Kapitel 1.2 beschrieben, liefern die meisten Literaturen und Forschungen nur Hinweise auf mögliche Chancen und Risiken bei der Durchführung eines Phishing-Awareness-Trainings, untersuchen dies aber nicht explizit. Die Arbeit von Volkamer et al. (2020), welche als einzige Arbeit direkt auf die organisatorische Durchführung eines Phishing-Awareness-Trainings eingeht, wurde bis anhin zu wenig kritisch hinterfragt und von anderen Quellen bestätigt oder widerlegt. In dieser Arbeit werden die Hinweise aus den unterschiedlichen Quellen sowie die Arbeit von Volkamer et al. untersucht und kritisch hinterfragt. Ebenfalls werden die Erkenntnisse aus den Literaturen mittels Experten:inneninterviews verifiziert und beurteilt. Damit liefert diese Arbeit, wie in Kapitel 1.5 beschrieben, einen Beitrag im Bereich der Forschung sowie für die Praxis. Die Arbeit deckt Erkenntnisse auf, die entweder in der Praxis oder in der Literatur bis anhin zu wenig Anwendung gefunden haben und somit in der Forschung weiter untersucht werden sollten. Ebenfalls stellt die Arbeit einen Beitrag zur Praxis, indem sie Erkenntnisse, welche in der Praxis von Bedeutung sind und auch in der Literatur Relevanz finden, zusammenfasst. Unternehmen erhalten mit dieser Arbeit eine übersichtliche Grundlage von Aspekten, welche sich bei der Durchführung eines Phishing-Awareness-Trainings ergeben, und können mögliche Chancen und Risiken besser beurteilen.

1.7 Aufbau der Arbeit

In Kapitel 2 werden das Vorgehen sowie die angewandten Methoden, welche in dieser Arbeit verwendet werden, vorgestellt. Das Kapitel ist unterteilt in «Literaturanalyse», «Experten:inneninterviews», «Datensatzanalyse» sowie das Vorgehen für die Zusammenführung aller gefundenen Erkenntnisse. Der Hauptteil dieser Arbeit besteht aus drei Teilen. Im ersten Teil, dem Kapitel 3, werden die Erkenntnisse aus der vorhandenen Literatur festgehalten. Innerhalb des Kapitels werden die Unterkapitel nach dem TOE-Framework in «technologisch», «organisatorisch» und «Umfeld» gegliedert. Zum Ende des Kapitels folgen eine Zusammenfassung der gewonnenen Erkenntnisse sowie eine Übersicht der gesamten Literatur. Im zweiten Teil, Kapitel 4, werden die gewonnenen Erkenntnisse aus den Experten:inneninterviews festgehalten. Wie in Kapitel 3 werden die

Ergebnisse aus Sicht des TOE-Frameworks beurteilt, kategorisiert und in die jeweiligen Unterkapitel gegliedert und beschrieben. In Kapitel 5 werden die gewonnenen Erkenntnisse aus dem Datensatz des OptiPhish-Projekts festgehalten. Zum Schluss werden in Kapitel 6 die Erkenntnisse aus der Literatur, den Experten:inneninterviews sowie den Resultaten aus dem Datensatz zusammengeführt, beurteilt und miteinander verglichen. Ebenfalls werden zum Schluss der Arbeit die Handlungsempfehlungen, die Limitationen sowie auf dieser Arbeit aufbauende mögliche Forschungsrichtungen, beschrieben.

2 Vorgehen und Methoden

In diesem Kapitel werden das angewendete Vorgehen sowie die in dieser Arbeit verwendeten Methoden beschrieben und in Abbildung 1 visuell dargestellt. Die Arbeit besteht aus vier Phasen, in welche auch die folgenden Unterkapitel unterteilt werden. In der ersten Phase wird eine systematische Literaturrecherche gemäss Döring (2023) sowie Webster und Watson (2002) durchgeführt. In der zweiten Phase wird ein qualitativer Datensatz mittels Experten:inneninterviews empirisch erstellt und ausgewertet. In der dritten Phase wird ein bereits vorhandener Datensatz, welcher in der Studie «OptiPhish» der ZHAW quantitativ und empirisch erhoben wurde, untersucht und ausgewertet. Zum Schluss werden die Erkenntnisse aus den beiden Datensätzen sowie die Erkenntnisse aus der Literatur zusammengeführt und es werden Schlussfolgerungen abgeleitet.

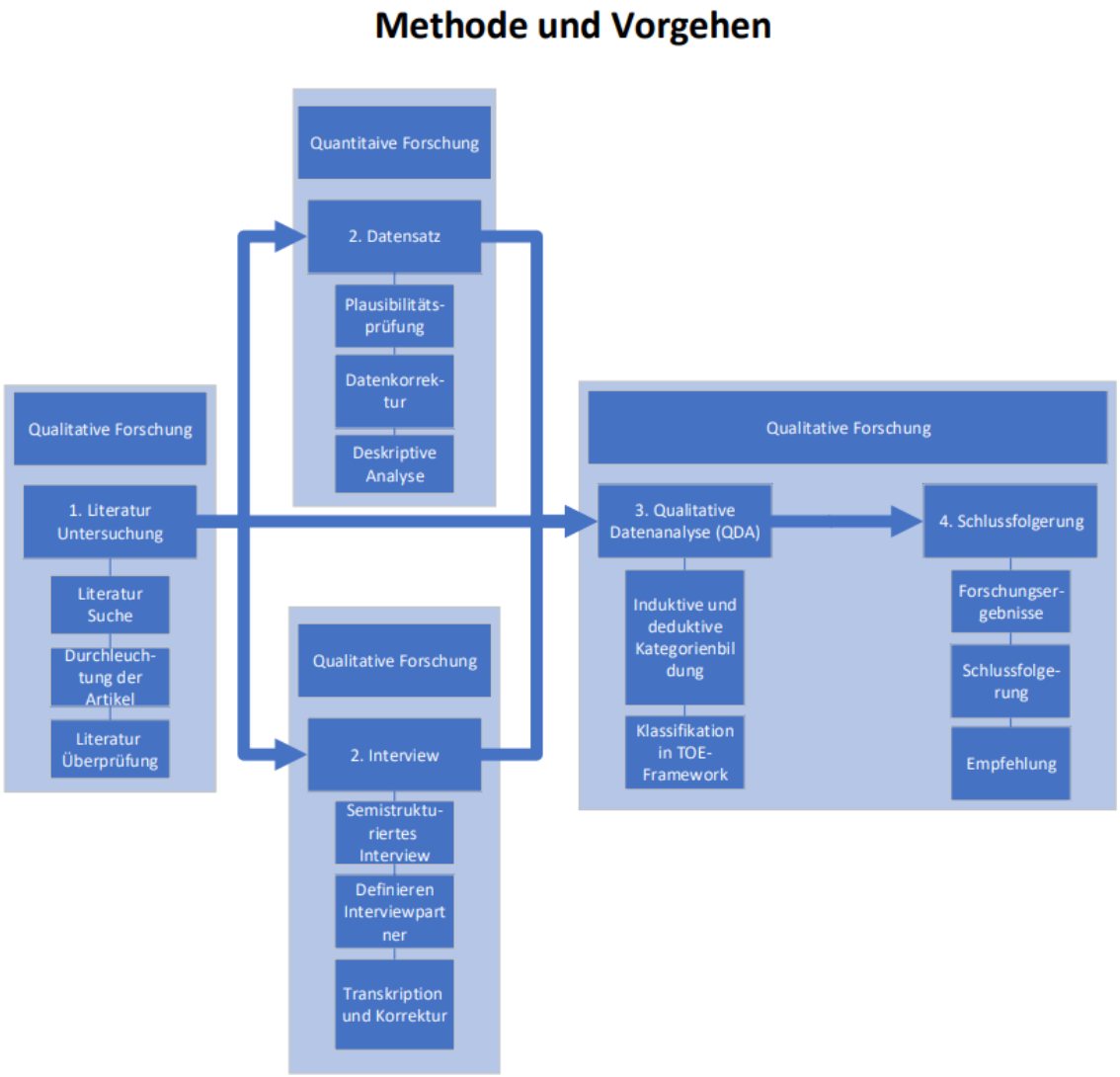

Abbildung 1: Methode und Vorgehen der vorliegenden Arbeit

2.1 Literaturanalyse

In der ersten Phase der Arbeit werden relevante Literaturen ermittelt und beurteilt. Das Vorgehen und die Methoden für die systematische Literaturrecherche werden in diesem Unterkapitel beschrieben.

Für die Ermittlung der relevanten Literaturen wird eine systematische Literaturrecherche gemäss Döring (2023) sowie Webster und Watson (2002) durchgeführt. Hierzu werden im ersten Schritt die in Tabelle 1 ersichtlichen Suchbegriffe in primäre und sekundäre Suchbegriffe unterteilt (Döring, 2023, S. 162). Teilweise werden Suchbegriffe wie «TOE» sowohl als primäre als auch als sekundäre Suchbegriffe verwendet. Damit wird sichergestellt, dass Suchbegriffe, die für die Arbeit eine hohe Relevanz darstellen, nicht nur anhand ihres Vorkommens im Titel, sondern auch anhand des Vorkommens in Abstracts, als Suchergebnisse resultieren.

Tabelle 1: Relevante primäre und sekundäre Suchbegriffe

Primäre Suchbegriffe	**Sekundäre Suchbegriffe**
Phishing	Response
TOE	Campaign, Education, Training
Awareness	TOE
Organizational, Organization, Organizations, Organisation, Organisations	Organizational, Organization, Organizations, Organisation, Organisations
Anti-phishing	Risk, Chance
Cybersecurity, Cyber security, Informationsecurity, Information Security	Human, User, Users, Participant
	Behaviors, Behavior, Behaviours, Factor, Factors, Attitude, Attitudes

Anhand der Suchbegriffe werden Abfragen erstellt, die anschliessend in wissenschaftlichen Datenbanken abgefragt werden (Döring, 2023, S. 162; Webster & Watson, 2002). Anhand der Spezialisierung der unterschiedlichen Datenbaken werden folgende vier Datenbanken verwendet:

- Google Scholar
- Proquest
- Web of Sience
- ACM Digital Library

Weiter werden die Abfragen aufgrund der Aktualität des Themas auf die Publikationsjahre 2018–2023 sowie in der Datenbank Proquest auf wissenschaftliche Zeitschriften und Fachmagazine eingeschränkt. Diese Einschränkung ermöglicht es, die Suchergebnisse auf relevante sowie aktuelle Literatur zu limitieren. Aufgrund der unterschiedlichen Abfragemöglichkeiten in den verschiedenen Datenbanken stellen gewisse Abfragekombinationen keine Sinnhaftigkeit dar und werden deshalb ausgelassen. Beispielsweise ist es bei Google Scholar nicht möglich, Abfragen anhand von Schlüsselwörtern in Abstracts einzuschränken. Eine Abfrage mit dem Aufbau «Phishing» im Titel und «TOE» im Abstract würde bei Google Scholar die Suche auf nur «Phishing» im Titel einschränken. Der Begriff «Phishing» als einzelner Suchbegriff stellt in dieser Arbeit jedoch keine Relevanz dar. Die Anzahl der Ergebnisse pro Abfrage sind in Tabelle 2 zusammengefasst dargestellt, die detaillierten Abfragen sind im Anhang A ersichtlich.

Tabelle 2: Anzahl der Suchergebnisse aus der Literaturrecherche

Abfragennr.	Google Scholar	Proquest	Web of Sience	ACM Digital Library
1	18	7	6	2
2	85	8	20	3
3	0	0	0	0
4	0	0	0	0
5	-	1	1	0
6	-	189	435	67
7	0	30	81	157
8	0	10	123	10
9	9	3	12	50
10	-	60	129	239
Zwischen Total	112	308	807	528
Gesamt Total	**1755**			

Die Ergebnisse aus den Abfragen werden exportiert und nach Döring (2023, S. 165) anhand ihrer Titel und Abstracts gesichtet. Ungeeignete oder nicht relevante Literaturen werden aussortiert. Die weiterhin relevanten Artikel werden inhaltlich auf die Relevanz

untersucht und ggf. aussortiert. Aus dem beschriebenen Vorgehen ergaben sich 49 Literaturen, die für diese Arbeit als relevant eingestuft wurden. Ausserdem wurden aus diesen 49 Literaturen relevante Referenzen und Referenzierungen gemäss den Schritten 2 und 3 nach Webster und Watson (2002) untersucht. Die Referenzen und Referenzierungen werden anhand des gleichen Vorgehens nach Döring (2023, S. 165) auf die Relevanz beurteilt. Mittels dieses Vorgehens wurden weitere 24 relevante Literaturen identifiziert, wodurch sich eine Gesamtanzahl an relevanten Literaturen von 73 ergab. Die Kennzahlen des Vorgehens sind in Tabelle 3 ersichtlich.

Tabelle 3: Kennzahlenübersicht relevanter Literaturen

	Anzahl
Total Literaturen	1755
Duplikate aussortiert	–461
Titel aussortiert	–918
Abstracts aussortiert	–233
Inhaltlich aussortiert	–94
Referenzen hinzugefügt	24
Total relevanter Literaturen	**73**

Für die Inhaltsanalyse wird eine Kombination der deduktiven und der induktiven Kategorienbildung nach Mayring und Fenzl (2019, S. 637–638) angewendet. Die deduktive Kategorienbildung erfolgt anhand des TOE-Frameworks mittels des in Tabelle 4 ersichtlichen Kodierleitfadens in Anlehnung an Mayring und Fenzl (2019, S. 638–639). Die induktive Kategorienbildung erfolgt auf Basis des Inhalts der relevanten Literatur gemäss Mayring und Fenzl (2019, S. 637–638). Die Kategorien sowie eine Literaturübersicht mit der zugeordneten Kategorie befinden sich in Anhang B.

Tabelle 4: Kodierleitfaden anhand des TOE-Frameworks in Anlehnung an Mayring und Fenzl (2019, S. 638–639)

Kategorie	Definition	Ankerbeispiele	Kodierregeln
Organisatorisch	Chancen oder Risiken, welche sich aus organisatorischer Sicht bei der Durchführung von Phishing-Awareness ergeben.	«Viele Chief Information Security Officers (CISOs) haben sich besorgt geäussert, wenn die Klickraten ihrer Schulungen hoch sind.» (Steves et al., 2020, S. 1–12) «Die Benutzer könnten sich selbst anstrengen, um ein höheres Niveau zu erreichen, als sie es ohne ein personalisiertes Programm tun würde.» (Jampen et al., 2020, S. 34)	Die Textpassage oder Äusserung beinhaltet die Nennung von organisatorischen Chancen oder Risiken bei der Durchführung von Phishing-Awareness-Trainings.
Technisch	Chancen oder Risiken, welche sich aus technischer Sicht bei der Durchführung von Phishing-Awareness ergeben.	«Obwohl Organisationen und Internet-/E-Mail-Dienstanbieter das Risiko des Spoofing von E-Mail-Konten durch Lösungen wie SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) und DMARC (Domain-based Message Authentication, Reporting and Conformance) verringern können, ist es nicht möglich, diese Risiken zu vermeiden.» (Abroshan et al., 2021b, S. 44940) «Hinzu kommt, dass Phisher genau die Tatsache, dass Phishing-Kampagnen durchgeführt werden, nutzen können, um gezielte reale Phishing-Angriffe vorzunehmen.» (Volkamer et al., 2020, S. 519–520)	Die Textpassage oder Äusserung beinhaltet die Nennung von technischen Chancen oder Risiken bei der Durchführung von Phishing-Awareness-Trainings.
Umfeld	Chancen oder Risiken, welche sich aus Umfeldfaktoren bei der Durchführung von Phishing-Awareness ergeben.	«Die Ergebnisse der Datenanalyse bestätigen, dass eine längere ISTE-Zeit die Wahrscheinlichkeit von Informationssicherheitsvorfällen verringern kann. Wenn der ISTE von professionellen Anbietern durchgeführt wird, würde die positive Auswirkung der ISTE auf die Verringerung der Vorfälle verstärkt werden.» (Kweon et al., 2021, S. 370) «Insbesondere wenn die Kampagne nicht ausschließlich institutionsintern durchgeführt wird, sind im Fall von simulierten Phishing-Nachrichten außerdem Marken- und Urheberrechte von externen Anbietern zu prüfen.» (Volkamer et al., 2020, S. 519–520)	Die Textpassage oder Äusserung beinhaltet die Nennung von Chancen oder Risiken aus der Sicht des Umfeldes, bei der Durchführung von Phishing-Awareness-Trainings

Die Auswertung der relevanten Literatur und ihre Inhaltsanalyse wird in Kapitel 3 beschrieben. In Kapitel 6 werden die Erkenntnisse aus der Literatur mit den Erkenntnissen aus den Experten:inneninterviews verglichen und es werden Schlussfolgerungen abgeleitet.

2.2 Experten:inneninterviews

In der zweiten Phase der Arbeit werden die Experten:inneninterviews durchgeführt, transkribiert und ausgewertet. Das Vorgehen und die Methoden für die Experten:inneninterviews wird im Folgenden beschrieben.

Die Experten:inneninterviews dienen in dieser Arbeit als qualitative empirische Datenquelle. Ziel ist es, Chancen und Risiken bei der Durchführung eines Phishing-Awareness-Trainings aus der Praxis zu identifizieren. Die gewonnenen Erkenntnisse werden in einem zweiten Schritt mit den aus der Literatur gewonnenen Erkenntnissen verglichen und ausgewertet. Als Interviewpartner werden Experten gewählt, welche bereits Erfahrungen mit der Durchführung von Phishing-Awareness-Trainings hatten und dadurch mit möglichen Chancen und Risiken in Berührung kamen. Die interviewten Experten sowie ihre jeweilige Funktion in ihren Unternehmen sind in Tabelle 5 aufgeführt.

Tabelle 5: Übersicht der Experten

Name	**Organisation**	**Funktion**	**Transkript Kapitel**
Experte 1	ZHAW	Leiter der Studie «OptiPhish»	Anhang D
Experte 2	ThriveDX Enterprise	General Manager EMEA & LATAM	Anhang E
Experte 3	ZHAW	Security Engineer ZHAW	Anhang F
Experte 4	ZHAW	CISO ZHAW	Anhang G
Experte 5/6	ZHAW	SOC-Mitarbeiter	Anhang H

Experte 7	Datimo	Phishing-Awareness-Verantwortlicher bei Datimo	Anhang I
Experte 8	UMB	Produkt Manager Security	Anhang J

Für die Experten:inneninterviews wird nach dem in Anhang C ersichtlichen, halbstrukturierten Interviewleitfaden vorgegangen (Döring, 2023, S. 368). Der Interviewleitfaden ist aufgebaut in allgemeine Kontextfragen, Hauptfragen und Detailfragen (Döring, 2023, S. 367–368). Vorzugsweise werden die Interviews als Einzelinterviews durchgeführt, eine Ausnahme besteht bei den Experten 5 und 6, die ein Paarinterview wünschen (Döring, 2023, S. 368). Die Interviews finden jeweils online statt und werden, sofern vom Interviewpartner nicht ausdrücklich abgelehnt, aufgezeichnet. Alle Experten:inneninterviews werden gemäss Döring (2023, S. 575) voll transkribiert. Für die Transkription werden nach Dresing und Pehl (2020, S. 838–842) Transkriptionsregeln erstellt. Die Transkriptionsregeln sind in Tabelle 6 ersichtlich.

Tabelle 6: Angewendete Transkriptionsregeln

Nr.	**Regel**
1	Das Schweizerdeutsche wird ins Standarddeutsche übersetzt.
2	Umgangssprachliche Ausdrücke und Redewendungen werden mit Anführungszeichen gekennzeichnet, bspw. «trifft den Nagel auf dem Kopf».
3	Füllwörter wie «ähm», «mhh» etc. werden ausgelassen.
4	Nicht relevante Wortwiederholungen werden ausgelassen.
5	Pausen und Stottern werden nicht markiert.
6	Satzabbrüche werden mit «/» gekennzeichnet.
7	Unklare und nicht verständliche Textpassagen werden mit «(unv., #hh:mm:ss-x#)» gekennzeichnet.
8	Die Zeichensetzung erfolgt auf Basis des sinngemässen Satzinhalts.

Als Hilfestellung für die Transkription der aufgenommenen Interviews wird die Software «f4transkript» der Firma Audiotranskription verwendet. Die Analyse der Interviews wird, wie die Analyse der Literatur, mittels deduktiver und induktiver Kategorienbildung nach Mayring und Fenzl (2019, S. 637–638) durchgeführt. Die deduktive Kategorienbildung erfolgt ebenfalls anhand des TOE-Frameworks mittels des in Tabelle 4 abgebildeten Kodierleitfadens in Anlehnung an Mayring und Fenzl (2019, S. 638–639). Die induktive Kategorienbildung erfolgt anhand der Inhalte der Experten:inneninterviews gemäss Ma-

yring und Fenzl (2019, S. 637–638). Die Inhaltsanalyse und die induktive Kategorienbildung werden mithilfe der Software «f4analyse», ebenfalls von der Firma Audiotranskription, durchgeführt. Die induktiven Kategorien aus den Experten:inneninterviews können dabei mit den induktiven Kategorien aus der Literaturanalyse übereinstimmen. Gleichzeitig können auch zusätzliche Kategorien generiert werden oder Kategorien wegfallen, falls das entsprechende Thema nur im Experten:inneninterview oder ausschliesslich in der Literatur erwähnt wird. Eine Übersicht der Kategorien aus den Experten:inneninterviews befindet sich in Anhang K. Die Erkenntnisse aus der Analyse werden anhand der identifizierten Kategorien in Kapitel 4 beschrieben.

2.3 Datensatzanalyse

In der letzten Phase des Hauptteils wird der Datensatz aus dem OptiPhish-Projekt analysiert und ausgewertet. Das Vorgehen und die Methoden, die für die Auswertung verwendet werden, werden im Folgenden beschrieben.

Zum Abschluss des OptiPhish-Projekts wurde eine Umfrage an die Studienteilnehmer versendet, um ihre Empfindung gegenüber dem Projekt und dem Phishing-Awareness-Training zu eruieren. Der daraus entstandene Datensatz wurde bis anhin noch nicht weiter untersucht. Aus der Umfrage ergaben sich 487 Rückmeldungen. Im ersten Schritt wird der Datensatz auf seine Plausibilität geprüft und es wird eine Datenkorrektur vorgenommen (Döring, 2023, S. 585). Unvollständige, nicht plausible Antworten sowie falsche Rückmeldungen werden in diesem Schritt aussortiert (Döring, 2023, S. 585). Es werden nur Antworten zugelassen, welche vollständig sind. Ausnahmen bei der Vollständigkeitsprüfung bilden die Frage, ob das Trainingsmaterial hilfreich war, sowie die Rückmeldung zur ankzeptablen Anzahl an Simulations-E-Mails pro Jahr und die individuelle Rückmeldung. Gründe für diese Ausnahmen sind, dass die Frage zum Trainingsmaterial nur diejenigen erhielten, die auch angaben, dass sie ein Training durchgeführt haben, und die Fragen zur Anzahl an E-Mails und die individuelle Rückmeldung optional waren. Die Plausibilitätsprüfung ist aufgrund der anonymisierten Daten nur bedingt durchführbar. Angesichts dessen wird die Plausibilitätsprüfung anhand der individuellen Rückmeldungen durchgeführt. Nach der Datenkorrektur betrug die Anzahl an gültigen Rückmeldungen 438.

Diese 438 Rückmeldungen werden in zwei Schritten untersucht. Im ersten Schritt werden die Rückmeldungen generell ausgewertet. Die Auswertung wird, sofern dies sinnhaft ist, auch im Zusammenhang, ob Teilnehmende auf ein simuliertes Phishing-E-Mail hereingefallen sind, ausgewertet und beurteilt. Im zweiten Schritt werden die individuellen Rückmeldungen ausgewertet. Hierzu wird nach Mayring und Fenzl (2019, S. 637–638) eine deduktive und eine induktive Kategorienbildung durchgeführt. Die deduktiven Kategorien bestehen aus positiven, negativen und anderen Rückmeldungen. Aufgrund der Tatsache, dass die individuellen Rückmeldungen sowohl positiv als auch negative Punkte enthalten können, wird zusätzlich die Kategorie «Positiv/Negativ» gebildet. Die deduktive Kategorienbildung erfolgt nach dem in Tabelle 7 ersichtlichen Kodierleitfaden in Anlehnung an Mayring und Fenzl (2019, S. 638–639).

Tabelle 7: Kodierleitfaden für die individuellen Rückmeldungen aus dem Datensatz

Kategorie	**Definition**	**Ankerbeispiele**	**Kodierregeln**
Positiv	Rückmeldungen, die eindeutige positive Informationen gegenüber dem Training oder der Studie enthalten.	«Thank you for raising awareness for this important problem.»	Die Rückmeldung beinhaltet positive Aspekte gegenüber der Durchführung von Phishing-Awareness-Trainings oder der Studie.
Negativ	Rückmeldungen, die eindeutige negative Rückmeldung gegenüber dem Training oder der Studie enthalten.	«E-Mail is an insecure way of communication. Putting responsibility on the users to detect phishing is not acceptable and does not work. Stop using e-mails, improve phishing detection on the mail servers, etc., but don't burden us with this!»	Die Rückmeldung beinhaltet negative Aspekte gegenüber der Durchführung von Phishing-Awareness-Trainings oder der Studie.
Positiv/Negativ	Rückmeldungen, die sowohl postive als auch negative Rückmeldungen gegenüber dem Training oder der Studie enthalten.	«It was kind of anoying for a while, just because of the number of e-mails that were sent, but I see that the training effect is good. I actually wish there was something similar for my parents, both retired and not very expierenced with computers.»	Die Rückmeldung beinhaltet sowohl positive als auch negative Aspekte gegenüber der Durchführung von Phishing-Awareness-Trainings oder der Studie.

Andere	Rückmeldungen, die weder positive noch negative Rückmeldungen gegenüber dem Training oder der Studie enthalten.	«Actually, I am fearing the worst. For example the escalating conflict by Russian regime and Putin. We will even more affected by Russian cyber attacks.»	Die Rückmeldung beinhaltet weder positive noch negative Aspekte gegenüber der Durchführung von Phishing-Awareness-Trainings oder der Studie.

Weiter wird anhand der Inhaltsanalyse der individuellen Rückmeldungen eine induktive Kategorienbildung nach Mayring und Fenzl (2019, S. 637–638) durchgeführt. Die induktive Kategorienbildung soll dabei die Gründe für die positiven und negativen Rückmeldungen identifizieren.

Die Ergebnisse aus der Datensatzanalyse werden in Kapitel 5 beschrieben. Weiter werden im Schlussteil dieser Arbeit die Ergebnisse aus dem Datensatz interpretiert und mit der aktuellen Literatur sowie den Ergebnissen aus den Experten:inneninterviews abgeglichen.

2.4 Auswertung

Die Auswertung der erhaltenen Erkenntnisse erfolgt in den jeweiligen Hauptkapiteln, die Auswertung der Literatur in Kapitel 3, die Auswertung der Experten:inneninterviews in Kapitel 4 und die Auswertung des Datensatzes in Kapitel 5. Die Erkenntnisse werden im Schlussteil, dem Kapitel 6.1, zusammengeführt und verglichen. Ebenfalls werden in Kapitel 6.1 die erhaltenen Erkenntnisse miteinander verglichen und beurteilt. Gewonnene Erkenntnisse, die sich sowohl in der Literatur als auch in den Experten:inneninterviews oder dem Datensatz zeigen, werden als aktuell relevant identifiziert. Erkenntnisse, welche sich einzig in der Literatur, den Experten:inneninterviews oder dem Datensatz zeigen, werden als noch nicht ausreichend untersucht oder relevant eingestuft und ebenfalls kritisch hinterfragt. In Kapitel 6.2 erfolgen zusätzlich die Handlungsempfehlungen anhand der gewonnenen Erkenntnisse.

3 Related Work

In diesem Kapitel werden die Erkenntnisse aus der systematischen Literaturrecherche anhand des Vorgehens, welches in Kapitel 2.1 beschrieben wurde, festgehalten. Eine Übersicht der Erkenntnisse ist in Abbildung 2 ersichtlich.

Abbildung 2: Übersicht der Erkenntnisse aus der Literaturrecherche

3.1 Organisatorisch

Im Folgenden werden alle organisatorischen Chancen und Risiken, welche aus der Literatur ermittelt wurden, beschrieben. Ebenfalls Bestandteil dieses Abschnitts sind Hinweise auf Chancen und Risiken, die sich anhand der Literatur antizipieren lassen. Zur Verbesserung der Lesbarkeit des Abschnitts werden die ermittelten Chancen und Risiken

sowie die entsprechenden Hinweise in Unterkategorien, die zugleich die Unterkapitel bilden, unterteilt.

3.1.1 Personenbezogene Einflussfaktoren

Eigenschaften der geschulten Mitarbeitenden

Vier von fünf Sicherheitsverletzungen werden gemäss Wilkinson (2022) durch den Menschen verursacht. Als Folge dessen werden in der Literatur menschliche Einflussfaktoren wie die Eigenschaften einer Person und deren Anfälligkeit gegenüber Phishing umfangreich diskutiert. Bardsley-Marcial untersucht die vier Eigenschaften «Alter», «Geschlecht», «Computererfahrung» und «Persönlichkeitsmerkmale». Die Autorin stellt dabei fest, dass das Geschlecht einen Einfluss auf die Anfälligkeit bei Phishing hat (Bardsley-Marcial, 2022, S. 98). Sowohl Bardsley-Marcial (2022, S. 102) als auch Abroshan et al. (2021b, S. 44939–44944) stellen fest, dass Frauen anfälliger für Phishing-Angriffe sind als Männer. Bardsley-Marcial (2022, S. 102) betont hingegen auch, dass sich Erfahrungen sowie Wissen und Bildung positiv auf die Phishing-Resistenz auswirken und Frauen aufgrund mangelnder Erfahrung und nicht aufgrund des Geschlechts einem erhöten Risiko in Bezug auf Phishing-Angriffe ausgesetz sind. Anawar et al. (2019, S. 2877–2878) gehen ebenfalls auf die eigenschaftsbezogene Anfälligkeit für Phishing ein und untersuchen die Anfälligkeit anhand eines Modells mit unterschiedlichen Persönlichkeits-Eigenschaften. Sie betonen, dass Personen, welche extrovertiert sind, gefährdeter bei Phishing-Angriffen sind. Neben den demografischen Eigenschaften und Persönlichkeitseigenschaften werden in der Literatur auch weitere Eigenschaften wie die Position in einem Unternehmen oder Kontextvariablen diskutiert. Bora et al. (2020, 1168–1169) stellten unter anderem fest, dass die Position einer Person mit der Anfälligkeit für Phishing korreliert und dass Personen, welche eine höhere hierarchische Position in einem Unternehmen einnehmen, anfälliger auf Phishing-Angriffe reagieren. Weiter stellen Merz et al. (2019, S. 34) und Abroshan et al. (2021a, S. 121926) fest, dass auch Kontextvariablen, wie die emotionale Lage, Müdigkeit oder andere, Einfluss auf die Anfälligkeit für Phishing haben. Alseadoon et al. (2013, S. 6) erkannten die umfangreichen Einflussfaktoren bereits 2013 und empfehlen, die Mitarbeitenden in geeignete Gruppen zu unterteilen und diese individuell zu schulen, um einen angemessenen Schutz zu gewährleisten.

Eine weitere häufig diskutierte Eigenschaft bezieht sich auf die technische Affinität insbesondere des IT-Personals und dessen Anfälligkeit für Phishing-Angriffe. In der Fach-

literatur überwiegt die Meinung, dass das IT-Personal oder technisch versierte Mitarbeitende eine genauso hohe Anfälligkeit bei Phishing-Angriffen zeigen wie technisch weniger versierte Mitarbeitende (Alwanain, 2019, S. 327; Anawar et al., 2019, S. 327; Ebner, 2018, S. 46; Jampen et al., 2020, S. 22). In einer Umfrage von Wilkinson (2022) gaben sogar 47 % der IT-Mitarbeitenden an, bereits einmal auf einen Phishing-Angriff hereingefallen zu sein. Dies ist insofern problematisch, als IT-Mitarbeitende mehr Rechte und umfangreiche Zugänge zu Systemen besitzen, was die Bedrohung bei einem erfolgreichen Phishing-Angriff zusätzlich erhöht (Wilkinson, 2022).

Verhalten der geschulten Mitarbeitenden

Neben den eigenschaftsbezogenen bestehen auch verhaltensbezogene Einflussfaktoren, die sich auf die Anfälligkeit für Phishing-Angriffe auswirken. Abroshan et al. (2021b, S. 440939) stellen beispielsweise in ihrer Untersuchung fest, dass Mitarbeitende, welche eine höhere Risikobereitschaft aufweisen, auch anfälliger für Phishing-Angriffe sind. Hingegen liefern Kumaraguru et al. (2009) den Hinweis, dass bei sicherheitsaffinen Mitarbeitenden das Risiko entstehen kann, auch legitimen Links nicht mehr zu vertrauen. Auch wenn dies in ihrer Studie nicht bestätigt wird, kann es in anderen Fällen zu einem solchen Risiko kommen. Zu einer ähnlichen Wirkung wie bei der Risikobereitschaft von Mitarbeitenden kann es kommen, wenn simulierte Phishing-Nachrichten zu leicht erkennbar aufgebaut sind. In einem solchen Fall führen die Trainings zu einer Phishing-Desensibilisierung und beeinflussen das Verhalten der Geschulten, indem sie ihre Fähigkeiten der Phishing-Erkennung überschätzen, was dem «Knowing-Doing-Gap» entspricht (Chen et al., 2020, S. 1; Kearney & Kruger, 2016, S. 55). Im Gegenzug ist es gemäss Chen et al. (2020, S. 1–9) auch von Bedeutung, dass Geschulte die Möglichkeit haben, simulierte Phishings zu erkennen, da sich positive Erfahrungen in der Phishing-Erkennung ebenso positiv auf das Verhalten bei der Erkennung echter Phishing-Angriffe auswirken.

Die bei den eigenschaftsbezogenen Einflussfaktoren beschriebenen Kontextvariablen beziehen sich nicht nur auf die Eigenschaften, sondern wirken sich auch auf das Verhalten der Mitarbeitenden aus. Der Einflussfaktor «Müdigkeit» kann sich unter anderem auf die Konzentration und somit auf das Verhalten gegenüber einem Phishing-E-Mail negativ auswirken (Merz et al., 2019, S. 34). Ebenfalls beeinflussen andere kontextbezogene Verhaltensfaktoren, wie das soziale Verhalten oder das Verhalten bei bestimmten Aufgaben,

die Reaktion gegenüber einem Phishing-Angriff (Frank et al., 2022, S. 1). Diese kontextbezogenen Verhaltensfaktoren sorgen für eine falsche Handlung bei einem Phishing-Angriff. Sie können wiederum den Druck und die Geschwindigkeit, in der Aufgaben erledigt werden müssen, erhöhen (Wilkinson, 2022). Wilkinson (2022) empfiehlt daher einen Geschwindigkeitsbegrenzer, um diesen kontextbezogenen Verhaltensfaktoren entschleunigend entgegenzuwirken.

Eine der bedeutendsten Herausforderungen im Bereich des menschlichen Verhaltens besteht darin, dass die Mehrheit der Mitarbeitenden Sicherheit lediglich als eine sekundäre Priorität betrachtet (Roepke et al., 2020, S. 42). Diese Priorisierung kann insbesondere dazu führen, dass sich Mitarbeitende weigern, Zeit in Sicherheitsschulungen zu investieren (Hurt, 2018). Dieses Problem besteht unter anderem bei Mitarbeitenden in höheren hierarchischen Positionen, da diese das Gefühl haben, nicht über genügend Zeit oder Energie für die Schulungen zu verfügen (Hurt, 2018).

Schlussfolgerung eigenschafts-/verhaltensbezogene Einflussfaktoren

Die Literatur zeigt diverse eigenschafts- und verhaltensbezogene Einflussfaktoren. Die Erkenntnisse aus der Literatur ermöglichen es, Schulungen auf diese Faktoren abzustimmen und so einen angemessenen Schutz zu gewährleisten (Alseadoon et al., 2013, S. 6). Abroshan et al. (2021b, S. 44939) und Frank et al. (2022, S. 6) äussern in ihren Untersuchungen sogar, dass es unabdingbar sei, Schulungen auf die entsprechenden Einflussfaktoren abzustimmen. Hingegen sind die Einflussfaktoren umfangreich und komplex und hängen zugleich von weiteren Kontextvariablen ab, was es erschwert, die Mitarbeitenden in Kategorien zu unterteilen und, wie von Alseadoon et al. (2013, S. 6) empfohlen, individuell zu schulen.

3.1.2 Art und Aufbau einer Schulung

Schulungsmethode

Grundsätzlich gibt es zwei Arten von Schulungen, die direkte und die eingebettete Schulung (Kumaraguru et al., 2007, S. 72). Die direkte Schulung kann entweder als Inhalt eines E-Mail versendet oder als Lektion, Workshop sowie in einer Geschichte als Face-to-Face-Schulung abgehalten werden (Alhashmi et al., 2021, S. 30; Kumaraguru et al., 2007, S. 72). Beim «Eingebetteten-Training» werden simulierte Phishing-E-Mails verwendet, welche einen Link oder einen Anhang enthalten. Reagieren die Empfangenden

auf diese E-Mails falsch, klicken auf den Link oder öffnen den Anhang, werden sie zu einer Schulung aufgefordert (Alabdan, 2020, S. 24). Auch bei der eingebetteten Variante kann die Schulung anschliessend auf unterschiedliche Varianten erfolgen, wie «Face to Face» bei der direkten Schulung oder per Zusenden des Schulungsmaterials über E-Mail (Alhashmi et al., 2021, S. 30; Kumaraguru et al., 2007, S. 72). In der Literatur wird aktuell die eingebettete Schulung als die wirksamste Schulungsmethode betrachtet. Der Grund für die Wirksamkeit liegt darin, dass die Forschung feststellen konnte, dass Mitarbeitende nach dem Hereinfallen auf ein simuliertes Phishing-E-Mail effektiver lernen (Jaeger & Eckhardt, 2021, S. 429–449; Jampen et al., 2020, S. 34). Daher sollten gemäss William et al. (2022, S. 813) Schulungen immer als eingebettete Schulung durchgeführt werden.

Schulungsmedium

Wie bei den Schlunungsmethoden gibt es auch beim Schulungsmedium unterschiedliche Möglichkeiten, das Wissen den zu Schuldenden zu vermitteln. Die Offline-Medien greifen dabei auf die Face-to-Face-Schulungsmethoden zurück (Alhashmi et al., 2021, S. 30). Ebenfalls eignen sich in der Praxis Online-Schulungsansätze, besonders in Kombination mit eingebetteten Schulungen (Darem, 2021, S. 7948). Zu den bekannte Online-Medien gehören video-, spiel-, text- oder webbasierte Medien als Schulungsmaterial (Alhashmi et al., 2021, S. 30). Die spielbasierten Medien gelten als eine der beliebtesten Methoden aufgrund des hohen Motivationspotenzials in Bezug auf die Geschulten. Jedoch sind spielbasierte Medien mehrheitlich preisintensiv, weshalb Roepke et al. (2020, S. 42) in ihrer Arbeit frei zugängliche spielbasierte Schulungsmedien untersuchen. In ihrer Arbeit stellten sie fest, dass kaum frei zugängliche spielbasierte Schulungsmedien zur Verfügung stehen und diejenigen, die frei zugänglich sind, nicht ausreichend Wissen vermitteln. Ein weiterer Faktor der Schulungsmedien besteht im Zeitbedarf, der für die Schulung aufgewendet werden muss, dieser kann je nach Schulungsmedium ebenfalls stark variieren (Volkamer et al., 2018, S. 120). Nicht nur das Schulungsmedium und der Zeitbedarf haben bei der Wissensvermittlung einen signifikanten Einfluss, sondern auch der Schulungsinhalt und die Komplexität des Inhalts sind von entscheidender Bedeutung. Wash und Cooper (2018, S. 1–2) stellen in ihrer Untersuchung fest, dass die Vermittlung des Wissens unterschiedlich effektiv sein kann, abhängig vom Inhalt und den Mitarbeitenden, an die das Wissen weitergegeben werden soll. Die Komplexität des Inhalts muss hingegen

gemäss Jensen et al. (2017, S. 620) nicht hoch sein, um eine effektive Schulung zu gewährleisten. Wohingegen Roepke et al. (2020, S. 54) berichten, dass die Tiefe des Inhalts schwierig zu definieren ist und individuell betrachtet werden sollte.

Schulungsbestimmungen

Unabhängig von der Schulungsmethode und dem Schulungsmedium gilt es, bei der Durchführung eines Phishing-Awareness-Trainings diverse Bestimmungen festzulegen. Ein häufiger Fehler ist hierbei, eine Schulungskampagne zu schnell zu implementieren (Alshaikh et al., 2018, S. 5091–5092). Grund für diesen Fehler ist der Zeitdruck bei der Erreichung von Sicherheitsstandards (Alshaikh et al., 2018, S. 5091–5092). Entgegen diesem Zeitdruck sollte vorgängig bestimmt werden, welche Mitrarbeitenden ein Phishing-Awareness-Training absolvieren sollten. Besonders in Bezug auf das IT-Personal sind die Meinungen unterschiedlich. Obwohl diverse Studien zeigten, dass technische Berufe genauso anfällig auf Phishing-Angriffe sind wie nicht technische Berufe (Alwanain, 2019, S. 327; Anawar et al., 2019, S. 327; Ebner, 2018, S. 46; Jampen et al., 2020, S. 22). Das Problem entsteht insofern, als gemäss Kumaraguru et al. (2009) und Miranda (2018, S. 9–10) die betroffenen Stellen, in denen auch die IT-Mitarbeitenden enthalten sind, informiert werden sollten, um falsche Handlungen durch das IT-Personal zu verhindern. Das Informieren des IT-Personals über eine bevorstehende Phishing-Simulation steht jedoch im Kontrast mit der Effektivität der Kampagne, da die Mitarbeitenden deutlich vorsichtiger sind. Diese Tatsache zeigt das Risiko, dass Mitarbeitende, die auf ein echtes Phishing hereinfallen würden, nicht identifiziert werden können (Miranda, 2018, S. 9–10). Die Entscheidung, ob Mitarbeitende über eine bevorstehende Phishing-Simulation informiert werden sollten, und deren Einfluss auf die Effektivität sollten aber gemäss Volkamer et al. (Volkamer et al., 2020, S. 519–520) für alle Mitarbeitenden abgewägt werden. In jedem Fall sollten die Mitarbeitenden aber nach einer Phishing-Simulation über die Kampagne informiert werden (Volkamer et al., 2020, S. 519–520). Unabhängig von der Effektivität aufgrund einer Vorankündigung sollten alle Mitarbeitenden inklusive dem IT-Personal geschult werden (William et al., 2022, S. 813). Ebenfalls gilt es zu bestimmen, wie die Mitarbeitenden im Fall eines Fehlverhaltens während einer laufenden Phishing-Simulation informiert werden sollten (Singh et al., 2023, S. 1–2; Volkamer et al., 2020, S. 519–520). Es gibt die Möglichkeit, die Mitarbeitenden sofort über das Fehlverhalten zu informieren oder die Information erst nach abgeschlossener Kampagne zu kommunizieren. Die sofortige Information steigert den Lerneffekt, da das Fehlverhalten

noch aktuell ist, birgt jedoch das Risiko einer internen Informationsverbreitung über die Phishing-Kampagne. Eine weitere Problematik sowohl bei direkten als auch bei eingebetteten Schulungen besteht darin, dass die Mitarbeitenden das zur Verfügung gestellte Schulungsmaterial ignorieren und das Training nicht absolvieren (Bona & Paci, 2020, S. 9). Um diesem Problem entgegenzuwirken, können ebenfalls Schulungsbestimmungen wie eine Absolvationspflicht oder Bestrafungen eingeführt werden (Alwanain, 2019, S. 323; Bora et al., 2020, S. 1165). Jedoch sind auch Absolvationspflichten und Bestrafungen mit Risiken verbunden, indem die Motivation gesenkt wird und dadurch der Lerneffekt oder das Sicherheitsbewusstsein gemindert werden.

Aktualität des Schulungsmaterials

In diesem Anschnitt wird auf die Aktualität des Schulungsmaterials eingegangen. Cyberkriminelle passen ihre Strategien ständig an, um technische Sicherheitsmassnahmen zu umgehen oder neue Schwachstellen der Mitarbeitenden auszunutzen (Zainab et al., 2021, S. 17). Das macht es für Unternehmen beschwerlich und teuer, da sie ihre technischen Sicherheitsmassnahmen ständig anpassen und Schulungsmaterialien aktualisieren müssen (Zainab et al., 2021, S. 17). Dennoch ist es von essenzieller Bedeutung, Schulungsmaterialien auf dem aktuellen Stand zu halten, um einen effektiven Schutz zu gewährleisten (Rosser et al., 2022, S. 133). Bereits bei der Evaluation eines Schulungsprogramms sollte darauf geachtet werden, dass die Aktualität und Aktualisierung gewährleistet werden (Rosser et al., 2022, S. 130).

Personalisierung der Schulung

Die Personalisierung des Trainings ist eine bedeutende Massnahme, um Phishing-Awareness-Trainings effizienter zu gestalten. Zusätzlich bietet die Personalisierung von Phishing-Awareness-Trainings die Möglichkeit, die Motivation der Mitarbeitenden gegenüber den Schulungsmassnahmen hochzuhalten (Alshaikh et al., 2021, S. 1; Rizzoni et al., 2022, S. 11; Röpke et al., 2020, S. 65). Aufgrund der Tatsache, dass Angreifer auch auf persönliche Informationen zurückgreifen und ihre Phishing-Angriffe personalisieren, bietet die Personalisierung des Schulungsmaterials eine Verbesserung des Trainingseffekts (Alshaikh et al., 2021, S. 1; Rizzoni et al., 2022, S. 11; Röpke et al., 2020, S. 65). Die Personalisierung bei simulierten Phishing-E-Mails sollte sich dabei unter anderem auf den Inhalt und die vom Benutzenden verwendeten Tools und Aufgabenbereiche beziehen (Rizzoni et al., 2022, S. 11; Röpke et al., 2020, S. 65; William et al., 2022, S. 812–

813). Solche Inhaltsanpassungen können helfen, die Geschulten herauszufordern und den Lerneffekt und somit die Effektivität des Trainings zu verbessern (Jaeger & Eckhardt, 2021, S. 449). Ebenfalls eine bedeutsame Methode ist das Variieren des Schwierigkeitsgrads sowohl im Trainingsinhalt als auch bei simulierten Phishing-Angriffen (Jampen et al., 2020, S. 34; Steves et al., 2020, S. 2). Eine Möglichkeit, Schwierigkeitsgrade zu implementieren, bezieht sich auf das Versenden von initialen simulierten Phishing-E-Mails und eine anschliessende Unterteilung anhand des Klickverhaltens der Geschulten (Younis & Musbah, 2020). Eine weitere Möglichkeit ist das Einbeziehen von Verhaltensweisen der Mitarbeitenden (Alshaikh et al., 2019, S. 8). Hierzu empfiehlt es sich, eine vorgängige Verhaltensanalyse durchzuführen und die zu Schulenden in geeignete Kategorien einzuteilen (Alshaikh et al., 2019, S. 8).

Auch wenn die Relevanz von personalisierten Schulungen aus der Literatur hervorgeht, wird dies in der Praxis dennoch zu wenig umgesetzt. Es zeigt sich, dass in der Praxis zu wenig auf die Personalisierung eingegangen wird und zu wenig unterschiedliche Ansätze verwendet werden (Alshaikh et al., 2021, S. 8; Alshaikh et al., 2018, S. 5091).

Intervall der Schulungen

Ein weiterer bedeutender Aspekt bei der Durchführung eines Phishing-Awareness-Trainings ist das Intervall, in dem die Schulung durchgeführt werden sollte. Schulungen in regelmässigen Abständen zu wiederholen, ist entscheidend, damit die Geschulten ihr Wissen auch über eine längere Zeit anwenden können und das Gelernte nicht aufgrund einer grossen Zeitspanne wieder vergessen (Volkamer et al., 2018, S. 123). Bei der Bestimmung des Zeitintervalls ist jedoch zu beachten, dass Phishing-Awareness-Trainings zeitintensiv sind und dadurch die Arbeitslast der Geschulten weiter erhöhen (Desolda et al., 2022, S. 26; Rizzoni et al., 2022, S. 11). Der Abstand der Trainingseinheiten sollte daher mit Bedacht definiert werden, um die Arbeitslast der Mitarbeitenden nicht überzustrapazieren oder die Motivation der Mitarbeitenden aufgrund von hohen Wiederholungszahlen zu beeinträchtigen (Jampen et al., 2020, S. 38). Reinheimer et al. (2020, S. 267) empfehlen ein Intervall von sechs Monaten und Jampen et al. (2020, S. 40) eines von fünf Monaten. Dementsprechend kann sich ein Intervall von ca. fünf bis sechs Monaten als geeigneter Rhythmus erweisen.

Schlussfolgerung

Die Art sowie der Aufbau eines Phishing-Awareness-Trainings beinhalten viele Aspekte, die im Rahmen einer Durchführung beachtet werden sollten. Die genaue Beachtung von Schulungsmethoden, Schulungsmedium, Schulungsbestimmungen, der Aktualität des Schulungsmaterials, der Personalisierung des Schulungsmaterials sowie der Intervalle können dabei helfen, eine Schulung effektiv und effizient zu gestalten und gleichzeitig die Motivation der Mitarbeitenden hochzuhalten. Im Gegenzug sind viele Aspekte zu berücksichtigen, welche die Gestaltung eine Phishing-Awareness-Trainings umfangreich und komplex gestalten. Eine Nichtbeachtung der Aspekte kann zudem dazu führen, dass die Motivation der Mitarbeitenden gesenkt wird, indem unter anderem das Intervall zu kurz definiert wird oder der Schwierigkeitsgrad falsch abgestimmt wurde. Dadurch können andere, gegenteilige Effekte, entstehen, als eigentlich durch die Schulung erhofft wurde.

3.1.3 Normen, Richtlinien und kulturelle Aspekte

Eine Möglichkeit, Phishing-Angriffe abzuwehren, ist das Erstellen und Implementieren von Normen und Richtlinien, um dadurch eine effektive Cybersicherheitskultur zu schaffen. Das Aufbauen und Pflegen von Normen und Richtlinien als kultureller Aspekt ist in der Literatur umstritten. Corradini et al. (2019, S. 194) beschreiben in ihrer Arbeit den Aufbau von Normen als wirksamere Möglichkeit, um das Verhalten der Mitarbeitenden positiv gegenüber Cyberbedrohungen zu beeinflussen, als andere Methoden. Der gleichen Meinung sind auch Petrič und Roer (2022, S. 12), die in ihrer Arbeit feststellten, dass das Verhalten der Mitarbeitenden beeinflusst werden kann, ohne diese in aufwendigen Verfahren überzeugen zu müssen. Eine Möglichkeit, Normen und Richtlinien zu entwickeln, untersucht Alshaikh (2020, S. 7–8) in seiner Arbeit, indem er ein Model entwickelt, mithilfe dessen die Cybersicherheitsrichtlinien erstellt werden können und dadurch das Verhalten der Mitarbeitenden positiv beeinflusst werden kann. Gegen die Implementierung von Cybersicherheitsrichtlichtlinien und entsprechende Normen spricht zum einen die Untersuchung von Shahbaznezhad et al. (2021, S. 545), die feststellen, dass der Schutz vor Phishing-Angriffen mittels Normen deutlich schlechter abschneidet als technische und schulungsbasierte Massnahmen. Zum anderen sprechen die Schwierigkeit und Langwierigkeit, um Normen in einer in einem Unternehmen aufzubauen und in der Kultur zu verankern, dagegen (Leidner & Kayworth, 2006, S. 357).

Normen und Richtlinien als Massnahme gegen Phishing-Angriffe sind in der Literatur umstritten und bergen das Risiko einer ineffektiven sowie zeitintensiven Massnahme. Hingegen bietet der Aufbau von Normen und Richtlinien mittels Phishing-Awareness-Training gleichzeitig die Chance, ein Unternehmen langfristig effizient gegen Cyberbedrohungen zu schützen und als ergänzende Massnahme zu fungieren.

3.1.4 Ethische Aspekte

Das Durchführen eines Phishing-Awareness-Trainings gilt als ethisch und moralisch fraglich. Deswegen sind ethische Hinterfragungen bei der Durchführung eines Phishing-Awareness-Trainings unerlässlich. Die Durchführung eines Phishing-Awareness-Trainings, insbesondere im Bereich von Phishing-Simulationen, gilt aufgrund von irreführenden E-Mails als ethische Grauzone (Sutter et al., 2022, S. 2). Es empfiehlt sich daher, Phishing-Awareness-Trainings vor der Durchführung mit einer ethischen Kommission zu prüfen und genehmigen zu lassen. Ebenfalls sollte die Phishing-Awareness-Kampagne auf Basis von ethischen Richtlinien geprüft und abgestimmt werden (Sutter et al., 2022, S. 5). Bei der Prüfung ethischer Richtlinien sowie Genehmigungen durch ethische Kommissionen ist jedoch zu beachten, dass diese viel Zeit in Anspruch nehmen und dadurch eine Verzögerung des Phishing-Awareness-Trainings verursachen können (Nijland, 2022, S. 7).

Schlussfolgernd kann ermittelt werden, dass ethische Prüfungen und Genehmigungen das Risiko von Verzögerungen bei der Durchführung von Phishing-Awareness-Trainings bieten können. Unabhängig davon helfen diese Prüfungen und Genehmigungen, eine ethisch korrekte Kampagne durchzuführen und rechtliche Konsequenzen zu vermeiden.

3.1.5 Aspekte der internen Rechtfertigung

Die Klickraten bei Phishing-Simulationen werden in der Praxis als Messpunkte für den Erfolg der Schulungsmassnahmen verwendet. Weiter werden die Klickraten als Rechtfertigung für die Weiterführung oder die Abschaffung von Phishing-Awareness-Trainings genutzt (Steves et al., 2020, S. 1–12). Die Rechtfertigungen auf Basis der Klickraten sind besonders für die Chief Information Security Officers kurz CISOs eine Herausforderung (Steves et al., 2020, S. 1–12). Infolge unterschiedlicher Schwierigkeitsgrade können Klickraten verschieden ausfallen und sollten dahingegen entsprechend ihrem individuellen Schwierigkeitsgrad beurteilt werden (Steves et al., 2020, S. 2).

Obgleich Klickraten ermöglichen, Phishing-Awareness-Trainings zu begründen und gegenüber höheren Instanzen zu rechtfertigen, sind Klickraten zugleich irreführend. Die Rechtfertigung mit Klickraten stellt das Risiko einer falschen Beurteilung der Phishing-Awareness-Massnahmen dar. Daher sollten Klickraten immer in Bezug auf den Schwierigkeitsgrad beurteilt werden, damit anhand des Schwierigkeitsgrades korrekte Schlüsse aus den Ergebnissen gezogen werden können.

3.2 Technologisch

Nach der Ermittlung der organisatorischen Chancen und Risiken bei der Durchführung eines Phishing-Awareness-Trainings werden nun die Chancen und Risiken aus der technologischen Perspektive beschrieben und beurteilt. Wie im vorangegangenen Abschnitt werden Hinweise auf und Antizipationen von Chancen und Risiken sowie bereits definitiv identifizierte Chancen und Risiken aus der technologischen Perspektive erläutert.

3.2.1 Systemlösungen

Auf dem Markt bestehen diverse Systeme und Lösungen, die für die Durchführung eines Phishing-Awareness-Trainings verwendet werden können. Die vielen Anbieter von Systemlösungen vertreiben ein breites Spektrum an möglichen Tools. Entsprechende Lösungen können dabei helfen, Phishing-Awareness-Trainings schnell und effizient zu implementieren, allerdings sollten die Lösungen ausführlich evaluiert werden. Um die Effektivität zu gewährleisten, ist es von essenzieller Bedeutung, dass die Anbieter ihre Inhalte und Methode aktuell halten und den Methoden von echten Phishing-Angriffen anpassen (Higashino et al., 2019, S. 82). Systemlösungen beziehungsweise Anbieter, welche die Aktualität und auch weitere Individualisierungsmöglichkeiten gewährleisten, sind mehrheitlich finanziell aufwändig (Burita et al., 2022, S. 12). Hinzu kommt, dass Angreifer teilweise simulierte Phishing-Kampagnen ausnutzen, um echte Phishing-Angriffe durchzuführen (Volkamer et al., 2020, S. 519–520). Die Nutzung externer Systemlösungen birgt dabei das Risiko, das Angreifende möglicherweise über den Anbieter an die Informationen der Durchführung von Phishing-Simulationen gelangen.

Systemlösungen stellen die Chance bereit, ein effektives und effizientes Phishing-Awareness-Training durchzuführen. Hingegen ist die Evaluation des Anbieters und der Systemlösung von essenzieller Bedeutung. Seriöse Anbieter weisen dabei die Gefahr hoher

Kosten auf, während bei kostengünstigen oder kostenlosen Anbietern das Risiko ineffektiver Schulungen oder sogar der Verstärkung der Sicherheitsrisiken besteht.

3.2.2 Technische Abwehrmassnahmen

Wie in Kapitel 1.1 erläutert, bestehen Abwehrmassnahmen gegen Phishing-Angriffe aus technischen sowie menschlichen Massnahmen. Die in der Praxis verwendeten technologischen Abwehrmassnahmen beginnen mit unkomplizierten Spamfiltern, welche E-Mails anhand ihrer Wörter im Inhalt klassifizieren und als Spam deklarieren oder blockieren (Kumaraguru et al., 2009). Weiter werden in der Praxis sogenannte White- und Blacklists auf den Mailrelays welcher empfangenden E-Mails entgegennimmt und weitergibt, eingerichtet. Diese Mailrelays prüfen eingehende E-Mails auf Basis des Absenders, Domains oder der IP und blockieren oder erlauben das empfangene E-Mail anhand von Regeln (Alabdan, 2020, S. 24; Althobaiti et al., 2021, S. 11–12). Ebenfalls werden in der Praxis Sender Policy Framework kurz SPF, Domain Keys Identified Mail kurz DKIM und Domain-based Message Authentication Reporting and Conformance kurz DMARC eingesetzt, welche den Absender auf dessen Richtigkeit verifizieren (Abroshan et al., 2021b, S. 44940). Diese Massnahmen unterstützen die Cybersicherheitsmassnahmen, indem sie eingehende Phishing-E-Mails bereits vor der Zustellung an den Mitarbeitenden blockieren. Gleichzeitig können diese Massnahmen auch die Zustellung von simulierten Phishing-E-Mails blockieren und somit das Phishing-Awareness-Training beeinträchtigen (Kumaraguru et al., 2009). Die fälschliche Blockierung der simulierten Phishing E-Mails kann hingegen mittels Whitelisting, also dem generellen Freischalten gewisser Absender, verhindert werden (Volkamer et al., 2020, S. 519–520). Die Einrichtung solcher Whitelisting-Massnahmen führt zu dem Risiko, dass diese für echte Phishing-E-Mails mittels E-Mail-Spoofing, bei dem ein falscher Absender vorgetäuscht wird, ausgenutzt werden (Volkamer et al., 2020, S. 519–520).

Zusammengefasst kann ermittelt werden, dass technische Massnahmen die Chance bieten, echte Phishing-E-Mails bereits vor der Zustellung an den Endbenutzenden zu blockieren. Gleichzeitig wird dadurch das Risiko geschaffen, dass auch simulierte Phishing-E-Mails abgefangen werden und das Phishing-Awareness-Training negativ beeinträchtigt wird. Die Umgehung dieser Beeinflussung mittels Whitelisting schafft wiederum ein zusätzliches Sicherheitsrisiko, welches von Angreifern ausgenutzt werden kann.

3.2.3 Vertrauen in die Technik

Wie im vorangegangenen Kapitel beschrieben, werden in der Praxis technische Sicherheitsmassnahmen als Schutz gegen Phishing-Angriffe implementiert. Diese technischen Sicherheitsmassnahmen helfen, echte Phishing-Angriffe abzuwehren. Gleichzeitig können die technischen Massnahmen auch zu einem falschen Vertrauen in die Technik bei den Mitarbeitenden führen (Butavicius et al., 2020, S. 2; Jampen et al., 2020, S. 19–29). Das falsche Vertrauen wird hierbei hauptsächlich durch ein mangelndes Verständnis der Grenzen von Technik hervorgerufen (Butavicius et al., 2020, S. 8). Dies führt dazu, dass Mitarbeitende die E-Mails zu ungenau prüfen und riskante Handlungen durchführen (Butavicius et al., 2020, S. 8).

Technische Massnahmen bieten die Chance, das Unternehmen vor echten Phishing-Angriffen zu schützen. Gleichzeitig können die technischen Sicherheitsmassnahmen aber auch das Risiko eines falschen Vertrauens bewirken und dadurch eine Gefahr für das Unternehmen darstellen (Jampen et al., 2020, S. 19–29). Es ist daher von Bedeutung, innerhalb eines Phishing-Awareness-Trainings klarzustellen, wo die Grenzen der technischen Massnahmen liegen, um das Risiko eines falschen Vertrauens zu minimieren.

3.2.4 Technische Warnhinweise

In der Praxis werden ebenfalls häufig Warnhinweise für den Endbenutzenden verwendet. Diese Warnhinweise werden beispielsweise bei externen E-Mails oder beim Laden einer Webseite angezeigt. Kävrestad et al. (2022, S. 3) sowie Yang et al. (2017) stellten in ihrer Untersuchung fest, dass Training allein nicht ausreichend Schutz vor Phishing-Angriffen bietet. Stattdessen sollten neben dem Training Warnhinweise als ergänzende Schulungs- und Sensibilisierungsmassnahme implementiert werden (Kävrestad et al., 2022, S. 3; Yang et al., 2017). Die Implementierung von Warnhinweisen bietet die Chance einer ergänzenden Sicherheitsmassnahme und dadurch einen zusätzlichen Schutz gegenüber Phishing-Angriffen. Warnhinweise können zugleich aber auch auf Phishing-Awareness-Trainings hinweisen und dadurch den Lerneffekt der Schulungsmassnahme negativ beeinträchtigen. Hinzu kommt die Problematik, dass Warnhinweise aufgrund einer Überflutung mehrheitlich ignoriert werden (Desolda et al., 2019, S. 144; Jampen et al., 2020, S. 35–36). Dieses Problem kann durch den Aufbau sowie gestalterische Massnahmen an den Warnhinweisen minimiert werden (Desolda et al., 2019, S. 144).

Warnhinweise bieten die Chance, als ergänzende Schutzmassnahme implementiert zu werden. Zugleich bieten sie das Risiko, dass sie ignoriert oder auch bei Phishing-Awareness-Trainings angezeigt werden und dadurch den Effekt der Massnahme verringern. Die Gestaltung und die Konfiguration sollten in der Praxis somit genau definiert und auch auf das Phishing-Awareness-Training abgestimmt werden.

3.2.5 Unterschiedliche Plattformen

Der technische Fortschritt führt zu einer immer höheren Mobilität und dadurch auch dazu, dass E-Mails nicht nur an Desktoprechnern, sondern auch auf Mobiltelefonen, Smartwatches etc. geprüft werden. Schulungsmaterialien lehren den Umgang mit Phishing-E-Mails hauptsächlich anhand der meistgenutzten Plattform, dem Desktoprechner. Dies führt dazu, dass Geschulte ihr Wissen gegenüber Phishing-Angriffen an Desktoprechnern korrekt anwenden können, jedoch dieses Wissen nicht an andere Plattformen wie das Mobiltelefon adaptieren können (Dixon et al., 2022, S. 2). Das Problem liegt daran, dass das Prüfen von Links auf Mobiltelefonen nicht so funktioniert wie das Prüfen an Desktoprechnern (Rizzoni et al., 2022, S. 11). Auf Mobiltelefonen bestehen beispielsweise keine Möglichkeiten, über einen Link zu hovern und so die tatsächliche Uniform Resource Locator kurz URL anzuzeigen, wie dies an einem Desktoprechner möglich ist (Rizzoni et al., 2022, S. 11). Aufgrund der zunehmenden Nutzung von mobilen Plattformen und der damit verbundenen Risiken sollten Schulungsmassnahmen ebenfalls darauf ausgelegt sein, Wissen für die Prüfung auf mobilen Plattformen zu vermitteln.

Das Inkludieren unterschiedlicher Plattformen im Schulungsmaterial bietet die Chance, geschulte Mitarbeitende auch auf anderen Plattformen zu sensibilisieren und zu einem sicheren Verhalten zu führen. Hingegen kann es schwierig sein, das Schulungsmaterial anzupassen und Nutzer von mobilen Plattformen zu identifizieren, für welche ein solches angepasstes Training sinnvoll wäre. Das generelle Schulen von unterschiedlichen Plattformen hingegen kann wiederum die Arbeitslast für das Training verstärken und dadurch, wie in Kapitel 3.1.2 beschrieben, negative Effekte auslösen.

3.2.6 Interne Meldeplattform

Aufgrund der steigenden Bedrohung durch Phishing-Angriffe sollte, unabhängig von einem Phishing-Awareness-Training, in jeder Organisation eine Meldeplattform zur Verfügung stehen. Mithilfe der Meldeplattform wird es den Mitarbeitenden ermöglicht, verdächtige Mails der zuständigen Abteilung zu melden und somit ein korrektes Verhalten

auszulösen. Solche Meldeplattformen können sowohl Chancen als auch Risiken im Zusammenhang mit dem Phishing-Awareness-Training auslösen. Der Aufbau einer Meldeplattform, worüber Mitarbeitende verdächtige Mails melden oder Informationen erhalten können, ist ein bedeutsamer Punkt in der Cybersicherheit einer Organisation (Alshaikh, 2020, S. 8). Die Relevanz einer Meldeplattform ergibt sich unter anderem aus der Tatsache, dass Phishing-Angriffe mehrheitlich nicht nur auf einen einzelnen Mitarbeitenden abzielen, sondern mehrere Mitarbeitende eines Unternehmens betreffen (Protasova & Mazko, 2021, S. 130). Mithilfe der Meldeplattform kann die zuständige Abteilung informiert und angemessene Gegenmassnahmen können ergriffen werden. Dieses Vorgehen ist ein bedeutender Bestandteil der Cybersicherheit und beeinflusst die Phishing-Awareness der gesamten Unternehmung (Bayl-Smith et al., 2022, S. 66). Das Melden verdächtiger E-Mails findet gemäss der Untersuchung von Jaeger und Eckhard aber immer noch zu selten statt (Jaeger & Eckhardt, 2021, S. 450). Es ist daher von Bedeutung, den Mitarbeitenden den Umgang mit verdächtigen E-Mails beizubringen und sie darin zu schulen, diese an der zuständigen Stelle zu melden (Jaeger & Eckhardt, 2021, S. 450; Protasova & Mazko, 2021, S. 130; Zainab et al., 2021, S. 17). In der Praxis bestehen jedoch selten klare Melde- und Rückmeldeprozesse oder es ist unklar, wie diese korrekt gestaltet werden sollen (Jampen et al., 2020, S. 50; Volkamer et al., 2020, S. 519–520). Mit den unklar gestalteten Meldeverfahren wird im Rahmen eines Phishing-Awareness-Trainings das Risiko generiert, dass die zuständige Abteilung währen einer Phishing-Simulation mit Meldungen überlastet wird (Althobaiti et al., 2021, S. 9–11). Dieses Risiko führt zu einem weiteren Risiko, indem echte Phishing-Angriffe aufgrund der Vielzahl an Meldungen, welche durch eine Phishing-Simulation generiert werden, übersehen werden (Althobaiti et al., 2021, S. 11; Mihelic et al., 2019, S. 1471–1472). Um diesen Risiken entgegenzuwirken, empfiehlt Miranda (2018, S. 9–10) in ihrer Untersuchung, die betroffenen Stellen zu informieren und dadurch das Nichterkennen echter Phishing-Angriffe oder eine falsche Reaktion durch das IT-Personal zu verhindern. Das Informieren der Betroffenen steht hingegen in Konflikt mit der in Kapitel 3.1.2 beschrieben Problematik, dass technisch versierte Mitarbeitende ebenfalls anfällig für Phishing-Angriffe sind und entsprechend geschult werden sollten.

Der Aufbau einer Meldeplattform bietet die Chance, die Awareness im Unternehmen weiter zu steigern und als zusätzliche Massnahme innerhalb eines Phishing-Awareness-Trainings zu agieren. Gleichzeitig kann eine unklare Meldeprozessgestaltung das Risiko erzeugen, dass echte Phishing-Angriffe aufgrund einer Überlastung der zuständigen

Stelle übersehen werden. Ebenfalls verstärkt die Überlastung die umstrittene Problematik, ob betroffene Stellen über Phishing-Awareness-Trainings informiert werden sollten oder nicht.

3.3 Umfeld

Es folgt die dritte Perspektive des TOE-Frameworks. Im Folgenden werden die Chancen und Risiken, welche in Bezug auf das Umfeld im Rahmen der Durchführung eines Phishing-Awareness-Trainings entstehen können, beschrieben. Wie in den beiden Abschnitten zuvor werden Aspekte untersucht, welche Hinweise auf mögliche Chancen und Risiken liefern, und bereits identifizierte Chancen und Risiken betrachtet.

3.3.1 Einbindung externer Firmen

Bei der Durchführung von Phishing-Awareness-Trainings hat es sich in der Praxis bewährt, auf die Unterstützung von externen Partnern zurückzugreifen oder das Phishing-Awareness-Training ganz auszulagern. Externe Partner können dabei die Chance bieten, das Phishing-Awareness-Training noch effizienter und effektiver durchzuführen aufgrund ihrer Spezialisierung in diesem Bereich (Kweon et al., 2021, S. 370). Die Zusammenarbeit mit externen Anbietern bietet hingegen auch diverse Risiken. Burita et al. (2022, S. 12) stellten in ihrer Arbeit die Problematik fest, dass sie durch die Verwendung externer Tools und Partner unzureichende Informationen über die Durchführung und Auswertung von Phishing-Awareness-Trainings erhielten. Weiter kann es bei der Zusammenarbeit mit externen Partnern zu zusätzlichen Sicherheitsproblemen kommen. Entstehen bei einem externen Anbieter Daten-Leaks also ein Abhandenkommen der Daten, können sensitive Daten wie Name, E-Mail-Adresse oder Informationen zur Durchführung von Phishing-Simulationen in die Hände von Cyberkriminellen fallen und dadurch die Sicherheit eines Unternehmens zusätzlich gefährden (Higashino et al., 2019, S. 82). Dieses Risiko kann noch verstärkt werden, wenn der externe Partner hauptsächlich im Ausland tätig ist, wo andere Sicherheitsbestimmungen oder rechtliche Aspekte gelten. Burita et al. (2022, S. 12) und Innab (2018, S. 4) weisen in ihrer Arbeit auf diese Problematik hin und zeigen auf, dass ausländische Partnerunternehmen mit Vorsicht gewählt werden sollten oder unter Umständen aufgrund der Landesbestimmung rechtlich sogar verboten sind.

Die Unterstützung durch externe Partner bietet die Chance, Phishing-Awareness-Trainings effektiver zu gestalten aufgrund der Nutzung der Expertise der Partnerunternehmen. Hingegen können Partnerunternehmen das Risiko von zusätzlichen Sicherheitslücken schaffen aufgrund der sensitiven Daten, die sie für die Durchführung eines Phishing-Awareness-Trainings benötigen. Die Zusammenarbeit mit ausländischen Firmen kann dieses Risiko noch verstärken wegen der Möglichkeit, dass in anderen Ländern unterschiedliche Regelungen und Rechtsgrundlagen prävalieren.

3.3.2 Rechtliche Aspekte

Das Versenden von Phishing-Simulationen als Phishing-Awareness-Training ist eine der meist genutzten Methoden in der Praxis. Mehrheitlich werden für die Phishing-Simulationen bekannte Marken wie Google, Microsoft etc. verwendet (Sutter et al., 2022, S. 6). Aufgrund markenschutzrechtlicher Gesetzgebungen kann es jedoch bei der Verwendung fremder Marken zu rechtlichen Konsequenzen kommen (Sutter et al., 2022, S. 6; Volkamer et al., 2020, S. 519–520). Diese rechtlichen Grundlagen können von Land zu Land variieren und sollten daher immer in Bezug auf das Land, in welchem das Phishing-Awareness-Training durchgeführt wird, beurteilt werden (Sutter et al., 2022, S. 6). Neben markenrechtlichen sind auch arbeitsrechtliche Bestimmungen zu beachten (Volkamer et al., 2020, S. 519–520). Abhängig von der Organisation und ihren arbeitsrechtlichen Bestimmungen ist zu ermitteln, ob die Auswertungen und Daten in Zusammenhang mit dem Phishing-Awareness-Training anonymisiert oder pseudonymisiert werden müssen (Volkamer et al., 2020, S. 519–520).

Rechtliche Aspekte bieten keine direkte Chance für die Durchführung von Phishing-Awareness-Trainings. Hingegen können rechtliche Risiken entstehen, welche von Organisationen bei der Durchführung eines Phishing-Awareness-Trainings beachtet werden sollten, um rechtliche Konsequenzen zu vermeiden.

3.4 Ergebniszusammenfassung

In den Unterkapiteln 3.1, 3.2 und 3.3 wurden die Erkenntnisse aus Sicht des TOE-Frameworks, die sich aus der Literatur ergaben, beschrieben. In diesem Kapitel werden die Ergebnisse nochmals kurz zusammengefasst und es wird eine Übersicht über die gesamte verwendete Literatur gegeben.

Aus organisatorischer Sicht wurden viele Einflussfaktoren im Bereich der Eigenschaften und des Verhaltens der Geschulten sowie der Art und des Aufbaus eines Schulungstrainings festgestellt. Die vielen Möglichkeiten, die Schulung auf die Mitarbeitenden auszurichten und zu gestalten, gestatten es, eine effektives und effizientes Phishing-Awareness-Training durchzuführen. Hingegen können die vielen Möglichkeiten des Schulungsaufbaus und dessen Gestaltung bei einem Phishing-Awareness-Training komplex werden. Hinzu kommen die Chancen von Normen und Richtlinien, die in Kombination eine effektive Cybersicherheitskultur schaffen können, wohingegen diese ebenfalls komplex und aufwendig in der Implementierung sein können. Ebenfalls gilt es aus organisatorischer Sicht, ethische und interne Rechtfertigungsrisiken zu beachten, welche bei der Durchführung eines Phishing-Awareness-Trainings entstehen können.

Technische Sicherheitsmassnahmen bieten die Chance, Phishing-Angriffe bereits vor der Zustellung an den Endbenutzenden abzuwehren. Ergänzende technische Sicherheitsmassnahmen wie Warnhinweise und Meldeplattformen helfen zusätzlich, den Schutz vor Cyberangriffen zu verbessern. Zugleich können technische Sicherheitsmassnahmen weitere Risiken schaffen, indem beispielsweise Whitelistings mittels E-Mail-Spoofing ausgenutzt oder echte Phishing-Angriffe übersehen werden aufgrund der durch das Phishing-Awareness-Training geschaffenen Falschmeldungen.

Als Umfeldfaktoren wurden hauptsächlich externe Partner sowie rechtliche Aspekte identifiziert. Externe Partner bieten aufgrund ihrer Expertise die Chance, Phishing-Awareness-Trainings effektiver und effizienter zu gestalten. Zugleich können bei der Zusammenarbeit mit externen Partnern Sicherheitsrisiken entstehen, indem im Fall eines Daten-Leaks sensitive Daten an potenzielle Angreifende gelangen. Im rechtlichen Umfeld ergeben sich keine direkten Chancen, hingegen kann die Beachtung rechtlicher Risiken das Risiko vermindern, rechtliche Konsequenzen zu erhalten.

In Anhang B befindet sich eine tabelarische Übersicht der gesamten verwendeten Literatur. Die Tabelle ist gemäss dem TOE-Framework gegliedert, wobei sie wiederum weiter in die einzelnen Aspekte anhand der Erkenntnisse unterteilt ist. Ebenfalls wird die Kernuntersuchung jeder verwendeten Literatur aufgezeigt.

4 Auswertung der Experten:inneninterviews

Die Überprüfung der in der Praxis vorhandenen Chancen und Risiken, welche durch Phishing-Awareness-Trainings entstehen, erfolgt mithilfe von Experten:inneninterviews. Das verwendete Vorgehen, die verwendete Methode und die interviewten Experten wurden in Kapitel 2.2 beschrieben. Die aus der deduktiven Inhaltsanalyse ermittelten Kategorien sind in Abbildung 3 dargestellt. In diesem Kapitel wird auf die Erkenntnisse aus den Experten:inneninterviews genauer eingegangen. Die Erkenntnisse werden anhand der Kategorien gegliedert und detailliert beschrieben. In Kapitel 6.1 werden diese Erkenntnisse dann mit den Erkenntnissen aus der Literatur sowie den Erkenntnissen aus dem Datensatz verglichen und beurteilt.

Abbildung 3: Übersicht der Erkenntnisse aus den Experten:inneninterviews

4.1 Organisatorisch

Im Folgenden werden die organisatorischen Chancen und Risiken, welche in den Experten:inneninterviews identifiziert wurden, erläutert. Dies erfolgt auf Basis der identifizierten Kategorien. Innerhalb der Kategorien werden die Expertenmeinungen zusammengetragen und verglichen.

4.1.1 Risikominimierung

Die Auswertung der Experten:inneninterviews führte zu zwei allgemeinen Chancen, die sich aus der Durchführung von Phishing-Awareness-Trainings ergeben können und von vielen Experten benannt werden. Zum einen ist dies die Risikominimierung gegenüber einem Cybersicherheitsvorfall (E3, 00:02:58-8; E2, 00:10:44-5; E4, 00:02:34-4). Zum anderen werden die Sensibilisierung und das aufmerksam Machen der Mitarbeitenden angeführt, um ebenfalls das Risiko, Opfer eines Phishing-Angriffs zu werden, zu minimieren (E5, 00:00:27-5; E1, 00:02:15-5; E8, 00:05:06-1; E4, 00:02:34-4). Experte 2 weist darauf hin, dass Untersuchungen teilweise gezeigt haben, dass Phishing-Awareness-Trainings sogar das Risiko eines Cybersicherheitsvorfalls erhöhen können (E2, 00.23:37-4). Er betont jedoch, dass dies aus seiner Sicht nur entsteht, wenn das Phishing-Awareness-Training falsch durchgeführt wird (E2, 00.23:37-4). Neben der Risikominimierung und der Sensibilisierung nennt Experte 6 noch zwei weitere Chancen, welche durch das Phishing-Awareness-Training entstehen können. Zum einen ist dies, das Thema «Sicherheit» näher an die Mitarbeitenden zu bringen und ihr Interesse an Sicherheit zu steigen (E6, 00:01:03-9). Zum anderen kann sich Experte 6, sowie auch Experte 7, vorstellen, dass die geschulten Mitarbeitenden neben der Risikominimierung im Unternehmen auch im privaten Leben von dem Awareness-Training profitieren können (E6, 00:01:03-9; E7, 00:08:32-4).

4.1.2 Repräsentation des Security-Teams

Viele Mitarbeidende kommen selten bis nie mit Sicherheitsvorkehrungen der IT in Berührung (E2, 01:16:53-6). Der einzige Aspekt im Bereich der Sicherheit, mit welchem Mitarbeitende in Berührung kommen, ist das Security-Awareness-Programm (E2, 01:16:53-6). Experte 2 sieht dies als Chance und Risiko zugleich. Das Cyber-Security-Team wie auch der CISO haben mit dem Phishing-Awareness-Training die Möglichkeit, sich selbst und ihre Sicherheitsvorkehrungen den Mitarbeitenden zu präsentieren (E2,

00:10:44-5). Wird das Phishing-Awareness-Training falsch oder unzureichend durchgeführt, kann dies im Umkehrschluss die Arbeit des Cyber-Security-Teams und des CISOs als unzureichend darstellen (E2, 01:16:53-6).

4.1.3 Kosten und Aufwand

Weitere Aspekte, die sich aus den Experten:inneninterviews ergeben, sind die Kosten sowie der Aufwand, welche durch eine Phishing-Awareness-Kampagne generiert werden. Bei diesen Aspekten überwiegen die Risiken. Die Durchführung eines Phishing-Awareness-Trainings generiert hohe Aufwendungen (E3, 00:03:42-8; E4, 00:10:52-0; E1, 00:03:49-1; E7, 00:03:06-1; E3, 00:49:21-2). Insbesondere der Aufwand nach einer Phishing-Awareness-Kampagne mit der Beantwortung von Fragen sollte nicht vernachlässigt werden (E1, 00:03:49-1). Hinzu kommt der Aufwand für die Mitarbeitenden, welchen das Phishing-Training und simulierte Phishing-E-Mails generieren. Dieser Aufwand kann in der Praxis von den Mitarbeitenden als Zeitverschwendung und sinnlos angesehen werden (E2, 00:10:44-5; E1, 00:02:54-5). Aufwendungen bedeuten in der Praxis immer auch Kosten, der Kostenaspekt kann aber noch verstärkt werden, indem Phishing-Awareness-Training-Tools mehrheitlich teuer sein können (E2, 00:15:21-9). Gleichzeitig entsteht durch das Phishing-Awareness-Training kein direkt sichtbarer Vorteil, was die Rechtfertigung der Kosten und die Durchführung eines Phishing-Awareness-Trainings erschwert (E7, 00:56:22-6). Gemäss Experte 3 stellt sich daher immer die Frage: «Wie viel investiert man, um wie viel Risiko zu reduzieren?» (E3, 00:02:58-8).

4.1.4 Eigenschaften und Verhalten der geschulten Mitarbeitenden

Die Eigenschaften und das Verhalten der geschulten Mitarbeitenden haben gemäss den Experten einen Einfluss auf die Durchführung eines Phishing-Awareness-Trainings. Experte 4 beschreibt beispielsweise, dass Mitarbeitende teilweise auch auf ein simuliertes Phishing-E-Mail klicken, obwohl sie wissen, dass es sich um Phishing handelt (E4, 00:17:30-0). Dies geschieht aufgrund der Tatsache, dass diese Mitarbeitenden schlichtweg neugierig sind (E4, 00:17:30-0). Die Berücksichtigung der Eigenschaften und des Verhaltens bietet aber die Chance, ein Phishing-Awareness-Training besser zu personalisieren und dadurch die Resistenz gegenüber echten Phishing-Angriffen zu verbessern (E4, 00:15:37-7). Das Risiko beziehungsweise die Problematik besteht dabei darin, dass solche eigenschafts- und verhaltensbezogenen Informationen nicht leicht zugänglich sind (E4, 00:12:30-0). Zudem kann die Berücksichtigung der Eigenschaften und des Verhaltens schnell relativ komplex werden (E4, 00:12:30-0). Deswegen sehen die Experten in

der Praxis die Unterteilung eher auf funktionaler Ebene, wie HR, Finanzabteilung etc. (E4, 00:12:30-0; E7, 00:06:38-2)

4.1.5 Art und Aufbau einer Schulung

Die Art und der Aufbau der Schulung können in der Praxis variieren. Es gibt viele Möglichkeiten, ein Phishing-Awareness-Training zu gestalten, von der Schulungsmethode und Schulungsmedium bis zu den Bestimmungen einer Schulung, mir dem Intervall oder dem Personalisierungsgrad. Diese Gestaltungsmöglichkeiten sorgen auch in der Praxis für Chancen und Risiken.

Schulungsmethode und Schulungsmedium

Die Art und der Aufbau der Schulung sind gemäss den Experten abhängig von der Zielgruppe. Die Lernfähigkeiten unterscheiden sich bei Mitarbeitenden, gewisse Mitarbeitende lernen zuverlässiger visuell, andere besser mit Text etc. (E4, 00:17:30-0). Das Risiko besteht darin, dass die Lernmethoden der Mitarbeitenden nicht bekannt sind und dadurch der Aufwand für die Eruierung der richtigen Lernmethoden hoch sein kann. Besonders bei grösseren Zielgruppen kann der Aufwand, für das Bestimmen der richtigen Trainingsart oder dem richtigen Schulungsmedium, deutlich zunehmen (E1, 00:12:31-4). Die Experten empfehlen daher, möglichst alle Aufbauarten und Medien zu verwenden (E4, 00:17:30-0; E3, 00:13:35-4; E8, 00:27:25-4). Entscheidend ist gemäss den Experten, dass das Training interessant ist und dass es den Mitarbeitenden Spass macht (E7, 00:14:56-0; E6, 00:16:45-4; E5, 00:17:46-8). Durch die Verwendung unterschiedlicher Methoden und Medien sowie die interessante Gestaltung ergibt sich die Chance, dass die Schulung besser bei der Zielgruppe angenommen wird und die Mitarbeitenden das Training auch tatsächlich durchführen (E4, 00:17:30-0; E1 00:12:31-4; E6, 00:16:45-4; E5, 00:20:17-1).

Schulungsbestimmungen

Wie bei den Schulungsmethoden und den Schulungsmedien gibt es eine Vielzahl an Möglichkeiten, den Aufbau einer Schulung zu bestimmen. Dazu gehören unter anderem das Informieren der Mitarbeitenden, der Inhalt oder die Bestimmung, an wen zu welchem Zeitpunkt welche E-Mails gesendet werden. Experte 2 erwähnt bei den Bestimmungen die Chance, dass mittels Phishing-Awareness-Training die IT-Richtlinien kommuniziert

werden können und so sichergestellt werden kann, dass diese auch tatsächlich gelesen werden (E2, 00:10:44-5).

Ebenfalls ist es gemäss Experte 2 von Bedeutung, den Schulungszeitpunkt zu bestimmen (E2, 00:30:45-7). Besonders bei Phishing-Simulationen und der anschliessenden Aufforderung zur Schulung aufgrund eines Fehlverhaltens kann ein unpassender Moment sein, wenn das E-Mail beispielsweise während eines Meetings geöffnet wurde (E2, 00:30:45-7). Das kann zu dem Risiko führen, dass unpassende Zeitpunkte bewirken, dass Schulungen nicht absolviert werden (E2, 00:30:45-7). Der Zeitpunkt von Phishing-Simulationen ist auch für die Experten 4 und 5 eine entscheidende Thematik. Sie betonen, dass Mitarbeitende miteinander reden und dabei das Risiko generieren, den Effekt von Phishing-Simulationen zu reduzieren, indem sie sich gegenseitig warnen (E4, 00:07:52-0; E5, 00:04:26-2). Dieses Verhalten ist bei einem echten Angriff zwar wünschenswert, sollte aber für eine effektive Schulung mittels randomisierter Zustellung verhindert werden.

Experte 3 erwähnt zudem noch zwei weitere Aspekte, welche bei den Bestimmungen beachtet werden sollten. Zum einen ist dies das Rückschlussverfahren auf sensitive Daten, wie das Passwort (E3, 00:08:38-3). Diese sollten gemäss dem Experten chiffriertwerden, da die Speicherung des Passwortes kritisch sein kann (E3, 00:08:38-3). Hingegen kann dann nicht nachvollzogen werden, ob ein eingegebenes Passwort tatsächlich dem echten Passwort entspricht oder ob der Mitarbeitende, aus Interesse, was passiert, zufällige Daten eingegeben hat. Zum anderen ist die Kommunikation innerhalb der Organisation genau zu definieren. Auch wenn ein Phishing-Awareness-Training von den Führungskräften genehmigt wurde, kann es dennoch zu dem Risiko kommen, dass Abteilungen oder Gruppen die Durchführung als Problem ansehen (E3, 00:05:30-6). Ebenfalls kann gemäss Experte 7 das Rückschlussverfahren aus Sicht der Mitarbeitenden ein Risiko darstellen (E7, 00:08:21-4), sofern Rückschlüsse auf die Mitarbeitenden gezogen werden und sich die Mitarbeitenden dadurch blossgestellt fühlen (E7, 00:08:21-4). Hingegen bietet es auch die Chance, die Mitarbeitenden noch spezifischer zu schulen und die Qualität des Trainings zu steigern (E7, 00:08:21-4).

Ein ebenfalls diskutierter Aspekt ist das Informieren der Mitarbeitenden und des IT-Personals über die Durchführung eines Phishing-Awareness-Trainings. Hierbei sind die Experten ebenfalls unterschiedlicher Meinung. Experte 2 vertritt die Ansicht, dass alle Mitarbeitenden inklusive des IT-Personals über die Durchführung informiert werden sollten (E2, 00:29:55-9). Er argumentiert, dass das Wissen über das Stattfinden einer Phishing-

Kampagne den Mitarbeitenden nicht hilft, diese zu erkennen (E2, 00:35:52-4). Im Gegenteil soll es sogar dazu beitragen, die Sensibilisierung zu steigern, auch wenn gerade keine Phishing-Simulation versendet wurde (E2, 00:35:52-4). Experte 7 hingegen ist überzeugt, dass weder die Mitarbeitenden noch das IT-Personal über die Durchführung informiert werden sollten (E7, 00:16:46-3). Er argumentiert, dass das IT-Personal aufgrund seiner erhöhten Rechte zur Hochrisikogruppe gehört und daher ebenfalls gleich geschult werden sollte (E7, 00:16:46-3). Die weiteren Experten vertreten die Meinung, dass Schlüsselpersonen oder -abteilungen, wie der Helpdesk oder die Security-Operations-Center-Mitarbeitenden kurz SOC-Mitarbeitenden, informiert werden sollten (E4, 00:21:06-7; E3, 00:17:50-7; E1, 00:14:16-9; E5, 00:20:46-7; E6, 00:21:16-9). Das Informieren begründet Experte 1 insbesondere damit, dass keine Eskalation ausgelöst wird und allenfalls rechtliche Konsequenzen entstehen (E1, 00:15:25-0). Experte 6 argumentiert, dass durch das Informieren der Schlüsselstellen das Risiko verhindert wird, dass das Phishing-Training durch die IT gestoppt wird (E6, 00:21:16-9).

Aktualität des Schulungsmaterials

Pishende nutzen aktuelle Themen und Trends, um Phishing-Angriffe erfolgreich durchzuführen. Demzufolge sind die Experten einer Meinung dahingehen, dass der Inhalt einer Phishing-Kampagne mit aktuellen Themen und Trends auf dem neusten Stand gehalten werden soll, um eine effektive Schulung zu gewährleisten (E7, 00:01:55-4; E4, 00:02:34-4; E2, 01:07:47-6; E3 00:08:38-3). Ebenfalls sollten gemäss Experte 5 und 6 Phishing-Simulationen den Mitarbeitenden so präsentiert werden wie echte Phishing-Angriffe (E5, 00:07:21-2; E6, 00:07:52-6). Dies beinhaltet auch Warnungen wie beispielsweise «Dieses Mail kommt von Extern» (E5, 00:07:21-2). Gleichzeitig betont Experte 5, dass aktuellen Themen wie Krieg, Pandemie und andere mit Bedacht definiert werden sollten, da Mitarbeitende einen emotionalen Bezug zu diesen besitzen können und dadurch das Risiko eines emotionalen Angriffs geschaffen wird (E5, 00:49:22-0).

Personalisierung der Schulung

Wie in Kapitel 4.1.4 und in den Bereichen «Schulungsmethode und Schulungsmedium» und «Schulungsbestimmungen» bereits erläutert, ist die Personalisierung des Phishing-Awareness-Trainings ein bedeutender Faktor. Aber auch bei der Personalisierung gibt es Chancen und Risiken, die beachtet werden sollten. Generell sind die Experten der Meinung, dass es diverse Faktoren gibt, die für eine Personalisierung sprechen (E7, 00:06:38-

2; E4, 00:12:30-0; E3, 00:08:38-3; E5, 00:10:05-3; E6, 00:10:22-3; E1, 00:08:40-0). Personenbezogene Faktoren sind jedoch komplex zu eruieren, daher sollte eine Personalisierung auf Ebene der Funktion erfolgen (E7, 00:06:38-2; E4, 00:12:30-0; E3, 00:08:38-3; E5, 00:10:05-3; E6, 00:10:22-3; E1, 00:08:40-0). Experten 2, 3 und 8 sind jedoch der Meinung, dass vor einer Personalisierung eine Grundschulung stattfinden sollte, bei welcher die Mitarbeitenden auf generelle Phishing-Angriffe trainiert werden (E2, 00:35:52-4; E8, 00:21:17-1; E3, 00:08:38-3). Eine weitere Möglichkeit, Phishing-Simulationen zu personalisieren, beschreiben die Experten 2 und 3, indem sie vorschlagen, Phishing auf Basis des Schwierigkeitsgrads zu erstellen (E2, 00:30:45-7; E3, 00:08:38-3).

Weiter weist Experte 2 darauf hin, dass es auch bedeutsam ist, nicht nur Phishing-Simulationen, sondern auch die Trainings selbst zu personalisieren (E2, 00:25:36-5). Damit diese ebenfalls auf die Mitarbeitenden und die Industrie abgestimmt sind und einen besseren Effekt zeigen (E2, 00:25:36-5).

Durch die Personalisierung entsteht die Chance, eine bessere Qualität der Schulung zu erreichen und besser auf die Mitarbeitenden einzugehen (E7, 00:12:03-4; E6, 00:10:34-6). Dies hilft wiederum, echte Phishing-Angriffe zu erkennen und auch Spear-Phishing-Angriffe besser abzuwehren (E4, 00:15:37-7; E8, 00:15:53-6; E1, 00:07:30-0; E5, 00:11:22-1).

Die Personalisierung eines Phishing-Awareness-Trainings kann jedoch gemäss den Experten auch Risiken haben. Durch die Personalisierung können spezifische Angriffe durchgeführt werden, die die Mitarbeitenden dann auch bei regulären E-Mails verunsichern (E8, 00:07:45-1). Ebenfalls besteht gemäss Experte 8 das Risiko, dass mit einer zu hohen Personalisierung die Klickraten künstlich erhöht werden (E8, 00:23:29-3). Wie bereits zu Beginn dieses Abschnitts erwähnt, ist eine Personalisierung auch nicht immer leicht, aufgrund der fehlenden Informationen über die Mitarbeitenden (E1, 00:07:30-0). Zuletzt kann durch eine Personalisierung auch das Risiko entstehen, dass die Mitarbeitenden das Training als unzulässig, unpassend oder ethisch verwerflich empfinden, aufgrund des persönlichen direkten Angriffs (E1, 00:09:52-6; E5, 00:12:11-2).

Intervall der Schulungen

Der letzte Aspekt, welcher in Bezug auf die Art und den Aufbau der Schulung genannt wird, ist das Intervall eines Phishing-Awareness-Trainings, insbesondere das Intervall einer Phishing-Simulation. Auch hier überwiegt bei den Experten mehrheitlich die gleiche

Meinung und sie betonen, dass ein Phishing-Awareness-Training ein ständiges Thema ist und kontinuierlich durchegeführt werden muss (E2, 00:10:44-5; E3, 00:10:35-4; E4, 00:17:30-0; E7, 00:29:34-9; E8, 00:05:06-1). Jedoch sollte das Intervall genau definiert werden, denn eine zu häufige Durchführung kann zu dem Risiko führen, dass die Mitarbeitenden genervt sind und sich beim Training nur noch durchklicken (E3, 00:13:35-4; E4, 00:04:18-9; E5, 00:01:48-0; E6, 00:16:45-4; E8, 00:07:45-1). Das Intervall kann gemäss Experte 3 aber nicht nur durch Kontinuität, sondern auch durch Variation helfen, die Sensibilisierung zu stärken (E3, 00:16:27-7). Indem zum Beispiel mehrere Phishing-Simulationen in einem Monat gesendet werden und anschliessend zwei bis drei Monate keine, sodass die Mitarbeitenden nicht wissen, wann eine Phishing-Simulation versendet wird, und so stets vorsichtig agieren (E3, 00:16:27-7).

4.1.6 Normen, Richtlinien und kulturelle Aspekte

Normen, Richtlinien und Kultur sind ebenfalls Aspekte im Phishing-Awareness-Training. Die Experten sehen diese Aspekte als Teil der Phishing-Awareness (E1, 00:16:44-4; E2, 00:38:51-2; E3, 00:20:10-9; E4, 00:23:00-9; E6, 00:24:15-7; E7, 00:19:49-3). Das Phishing-Awareness-Training kann beispielsweise helfen, eine Cybersicherheitskultur aufzubauen, gleichzeitig kann die Cybersicherheitskultur helfen, eine bessere Phishing Awareness zu schaffen (E1, 00:16:44-4; E2, 00:38:51-2; E3, 00:20:10-9; E4, 00:23:00-9; E6, 00:24:15-7; E7, 00:19:49-3). Experte 4 betont jedoch, dass die Durchführung eines Phishing-Awareness-Trainings auf Basis der aktuellen Kultur aufgebaut sein muss (E4, 00:56-1). Experte 5 nennt zudem das Risiko, dass eine schlechte Cybersicherheitskultur dazu führen kann, dass es zu Problemen beim Phishing-Awareness-Training kommt (E5, 00:23:51-7). Zuletzt kann durch die Cybersichheitskultur die Chance entstehen, den Mitarbeitenden klarzumachen, dass jeder für die Sicherheit verantwortlich ist, und nicht nur die IT oder der CISO (E8, 00:32:42-0).

4.1.7 Ethische Aspekte

Phishing-Awareness-Trainings bilden eine ethische Grauzone, da die Mitarbeitenden üblicherweise nicht über die Teilnahme bestimmen können (E1, 00:19:23-7). Ethische Handlungsansätze bieten dabei keine direkten Chancen, sondern helfen, Risiken zu minimieren. Aus den Interviews gehen drei Aspekte hervor, welche aus Sicht der Ethik beachtet werden sollten. Der erste Aspekt beinhaltet die adressierten Mitarbeitenden. Hierbei sollte darauf geachtet werden, dass diese korrekt adressiert werden und es nicht zu ethischen Missverständnissen kommt (E1, 00:09:52-6; E2, 00:45:16-4; E4, 00:25:33-1;

E5, 00:25:45-5; E7, 00:23:24-8). Der zweite Aspekt ist der Inhalt des Trainings, auch hier sollte darauf geachtet werden, dass keine ethisch falschen oder missverständlichen Inhalte aufgegriffen werden (E1, 00:09:52-6; E2, 00:45:16-4; E3, 00:11:57-3; E6 00:26:14-3; E8, 00:36:25-1). Beispielweise sollten Phishing-Simulationen mit Bonusankündigungen vermieden werden, da in diesem Fall die Gefühle der Mitarbeitenden angegriffen werden (E2, 00:45:16-4; E3, 00:11:57-3). Der dritte Aspekt beinhaltet die Verwendung externer Firmennamen oder Logos bei Phishing-Simulationen. Die Verwendung externer Firmennamen und Logos kann rechtlich, aber auch ethisch das Problem hervorrufen, dass die verwendete Firma als Auslöser der Phishing-E-Mails dargestellt wird (E7, 00:23:24-8).

4.1.8 Aspekte der internen Rechtfertigung

Klickraten bei den Phishing-Simulationen werden häufig in der Praxis verwendet, um einen Basiswert zu erhalten (E1, 00:20:49-2). Die Klickraten werden anschliessend vom Management als Argumentationsbasis genutzt (E4, 00:29:26-7; E7, 00:28:11-1). Alle Experten sind aber der gleichen Meinung, dass die Verwendung von Klickraten als Argumentationsbasis ein Risiko darstellen kann, wenn die Zahlen nicht im Kontext zu dem Schwierigkeitsgrad beurteilt werden (E1, 00:20:49-2; E2, 00:53:19-5; E3, 00:23:58-3; E4, 00:26:53-7; E5, 00:01:48-0; E6, 00:28:36-7; E7, 00:25:12-2; E8, 00:23:29-3). Die Klickraten können auf unterschiedlichste Arten bewusst oder unbewusst manipuliert werden (E3 00:27:42-9; E5, 00:01:48-0). Es kann insbesondere vorkommen, dass Mitarbeitende klicken, obwohl sie wissen, dass es sich um ein Phishing handelt, oder es könnnen Klicks durch Systeme wie Antivirus verursacht werden (E1, 00:20:49-2; E3, 00:23:58-3; E5 00:29:22-5). Ebenfalls können Klickraten auf unterschiedliche Faktoren bezogen werden, wie der Klick auf einen Link oder die Preisgabe von Benutzername und Passwort (E1, 00:20:49-2). Werden diese Einflussfaktoren bei der Erhebung nicht berücksichtigt und die Klickraten ohne Kontext als Argumentationsbasis verwendet, kann dies zum Risiko von Fehlentscheidungen führen (E1, 00:20:49-2; E3, 00:20:10-9; E4, 00:29:55-4; E5, 00:01:48-0; E6, 00:28:36-7).

4.2 Technologisch

Im folgenden Abschnitt werden die technologischen Chancen und Risiken beschrieben, welche sich aus Sicht des TOE-Frameworks aus den Experten:inneninterviews ergaben. Der Abschnitt wird auf Basis der induktiv ermittelten Kategorien strukturiert.

4.2.1 Systemlösungen

In der Praxis gibt es unterschiedliche Systemlösungen, welche für ein Phishing-Awareness-Training verwendet werden können. Abhängig von der Lösung können unterschiedliche Chancen und Risiken generiert werden. Diese Lösungen bieten unterschiedliche Funktionen und Möglichkeiten zur Durchführung und Auswertung von Phishing-Awareness-Trainings (E1, 00:06:07-9; E2, 00:17:09-1). Entscheidend ist gemäss Experte 1, dass ein System verwendet wird, mit dem man auch entsprechend umgehen kann (E1, 00:04:35-4). Ansonsten kann das Risiko einer Fehlkonfiguration entstehen und beispielsweise können Phishing-Simulation-E-Mails an die falschen Personen versendet werden (E1, 00:04:35-4). Software as a Service Lösungen kurz SaaS-Lösungen können zusätzlich die Chance eines kostengünstigeren Betriebs gegenüber On-Premise-Anwendungen, also dem eigenen betreiben der Anwendung, bieten, da Wartungen, Konfigurationen etc. entfallen (E1, 00:27:08-3). Jedoch darf nicht davon ausgegangen werden, dass bei SaaS-Lösungen der Aufwand komplett entfällt (E3, 00:41:05-2). Das Bedeutendste an der Systemlösung ist gemäss Experte 3 jedoch, dass die Anwendung für den Mitarbeitenden möglichst unkompliziert ist und so das Training weitestgehend ohne Umstände zur Verfügung stellt (E3, 00:13:35-4).

4.2.2 Technische Abwehrmassnahmen

In der Praxis werden für die Durchführung von Phishing-Awareness-Trainings teilweise Konfigurationsanpassungen an Spamfiltern und Maigateways vorgenommen. Diese Massnahmen bieten die Möglichkeit, dass die Schulungs-E-Mails auch tatsächlich bei den Mitarbeitenden ankommen und nicht vorgängig herausgefiltert werden (E1, 00:24:09-2; E7, 00:03:06-1). Gleichzeitig können die Massnahmen das Risiko bieten, dass diese Konfigurationen von echten Phishenden ausgenutzt und so echte Phishing-E-Mails zugestellt werden können (E1, 00:24:09-2; E2, 00:17:09-1; E3, 00:28:07-4; E7, 00:32:13-1). Dieses Risiko wird zusätzlich verstärkt, da es bei Konfigurationsanpassungen immer auch zur Fehlkonfiguration kommen kann (E1, 00:25:51-7). Gemäss den meisten Experten sind diese Risiken jedoch gering. Zusätzlich weist Experte 6 darauf hin, dass dieses Risiko stark reduziert werden kann, wenn weitere E-Mail-Prüfungsmechanismen wie SPF-Check, DKIM und DMARK aktiv bleiben (E6, 00:31:47-0). Um das Risiko weiter zu reduzieren, sollten gemäss Experte 3 diese freigeschalteten Kanäle auch weiterhin über-

wacht werden, um Unstimmigkeiten festzustellen (E3, 00:28:07-4). Ebenfalls können gemäss Experte 4 diese Massnahmen zum Risiko führen, dass Mitarbeitende solche Freischaltungen erkennen und dadurch der Trainingseffekt vermindert wird (E4, 00:30:26-3).

4.2.3 Vertrauen in die Technik

Die im vorangegangenen Kapitel erwähnten Massnahmen wie Spamfilter, SPF-Check usw. helfen im Normalfall echte Phishing-Angriffe abzuwehren. Experte 4 nannte zur Veranschaulichung dieser Massnahmen, dass an der ZHAW monatlich etwa vier Millionen E-Mails zugestellt und davon rund drei Millionen E-Mails als bösartig herausgefiltert werden (E4, 00:32:07-8). Diese Abwehrmassnahmen können in der Praxis bei den Mitarbeitenden aber auch zu einem falschen Vertrauen in die Technik führen (E1, 00:29:06-3; E2 00:15:21-9; E4, 00:32:07-8; E5, 00:32:33-9; E6, 00:33:16-1; E7, 00:34:57-9). Das Phishing-Awareness-Training bietet hierbei die Chance, dieses falsche Vertrauen anzugehen und den Mitarbeitenden die Grenzen der technischen Möglichkeiten aufzuzeigen (E1, 00:29:06-3; E2, 00:57:19-7; E4, 00:32:07-8; E5, 00:32:33-9; E6, 00:33:16-1; E7, 00:34:57-9). Denn trotz technischer Massnahmen stellt Phishing weiterhin ein Problem dar und die Mitarbeitenden müssen sich dessen bewusst sein (E1, 00:29:06-3; E3 00:30:20-1;E5, 00:32:33-9; E6, 00:33:16-1; E7, 00:34:57-9).

4.2.4 Technische Warnhinweise

Neben technischen Abwehrmassnahmen, wie in Kapitel 4.2.2 beschrieben, besteht die Möglichkeit technischer Warnhinweise für den Mitarbeitenden, wie Banners bei externen E-Mails oder Warnungen bei Webseiten, zu implementieren. Die Meinungen der Experten unterscheiden sich hierbei deutlich. Während ein Teil der Experten Warnhinweise als sinnvoll erachtet (E2, 01:00:57-4; E3 00:31:52-3; E5 00:36:11-7; E7, 00:37:27-5; E8, 00:44:06-1), sind andere Experten eher kritisch gegenüber Warnhinweisen (E1, 00:31:08-7; E4 00:34:43-4; E6 00:36:49-8;E8, 00:44:06-1). Zudem stellt sich die Frage, ob Mitarbeitende mit den Warnhinweisen umgehen können und diese verstehen (E1, 00:31:08-7). Warnhinweise können zwar die Chancen bieten, die Mitarbeitenden besser auf Bedrohungen aufmerksam zu machen, jedoch nur, wenn sie richtig implementiert sind und lediglich sporadisch angezeigt werden (E2, 01:01:37-1; E6, 00:40:58-7; E7, 00:37:27-5). Eine zu häufige Anzeige kann dazu führen, dass die Mitarbeitenden blind gegenüber diesen Meldungen werden (E1, 00:33:23-4; E5, 00:39:43-4; E8, 00:44:06-1).

Ebenfalls kann die Anzeige von Warnhinweisen, wie auch die technischen Abwehrmassnahmen, zu einem falschen Vertrauen führen und dafür sogen, dass sich Mitarbeitende zu stark darauf verlassen (E3, 00:32:54-5).

4.2.5 Unterschiedliche Plattformen

Die Arbeitswelt wird immer mobiler und es werden stets mehr E-Mails auf mobilen Endgeräten wie Smartphone, Tablet, Smartwatches usw. abgerufen. Aus dem Experten:inneninterviews ergaben sich zwei Aspekte in Bezug auf die unterschiedlichen Plattformen. Zum einen ergibt sich, dass das Schulungsmaterial auf mobilen Endgeräten durchführbar ist (E2, 01:02:29-4; E7, 00:40:22-0), zum anderen die Integration dieser Plattformen im Schulungsmaterial selbst (E1, 00:35:39-4; E4, 00:37:22-4; E3, 00:33:38-6; E5, 00:44:09-9; E8, 00:48:59-7). Die Durchführbarkeit des Schulungsmaterials auf mobilen Endgeräten bietet die Chance, ein für den Benutzenden freundlicheres Schulungsdesign anzubieten und dadurch die Durchführungsrate zu steigern (E2, 01:02:29-4; E7, 00:40:22-0). Die Integration der mobilen Plattformen innerhalb des Schulungsmaterials hat die Chance, die Mitarbeitenden besser und umfangreicher zu schulen (E1, 00:41:20-0; E3, 00:33:38-6; E5, 00:44:09-9; E7, 00:43:21-2). Diese Chance ist auf die Tatsache zurückzuführen, dass sich das Prüfen von E-Mails auf mobilen Plattformen technisch vom Prüfen auf herkömmlichen Desktops unterscheidet und Angreifende vermehrt mobile Plattformen anvisieren (E1, 00:35:39-4; E5, 00:42:15-9; E6, 00:43:04-4). Die Integration im Schulungsmaterial kann aber auch das Risiko der Komplexität erhöhen aufgrund der Tatsache, dass es viele unterschiedliche E-Mail-Clients und Geräte gibt (E1, 00:42:27-2; E4, 00:37:22-4; E5, 00:42:15-9; E6, 00:43:04-4). Deswegen empfiehlt Experte 4, die gängigsten Endgeräte und E-Mail-Clients zu verwenden und zu prüfen, wer welches Endgerät oder welchen Client nutzt, um anschliessend das Schulungsmaterial spezifisch anhand der meistgenutzten Plattform zuzuweisen (E4, 00:36:32-0).

4.2.6 Interne Meldeplattform

Im Rahmen von Phishing-Awareness-Trainings werden vermehrt auch Meldefunktionen wie ein Button im E-Mail-Client oder eine Melde-Webseite eingeführt. Diese Funktion bietet gemäss den Experten diverse Chancen und Risiken. Eine Chance, die aus der Meldefunktion resultiert, ist die Möglichkeit, dadurch einen echten Phishing-Angriff zu erkennen und so die Reaktionszeit der IT zu verkürzen (E1, 00:38:10-3; E2, 01:04:40-9; E6, 00:46:11-7; E7, 00:45:06-7). Ebenfalls ist eine Meldefunktion für die Mitarbeitenden unkompliziert anzuwenden und steigert dadurch die Benutzerfreundlichkeit (E1,

00:38:10-3; E3, 00:36:09-4). Der Button im E-Mail-Client bietet zusätzlich die Chance, den Benutzenden immer wieder zu sensibilisieren, da der Button stetig präsent ist (E2, 01:04:40-9). Für das Phishing-Awareness-Training selbst kann mit der Meldefunktion ein Punktesystem verwendet werden, bei dem Mitarbeitende Punkte erhalten für das korrekte Erkennen eines Phishing-E-Mails (E2, 01:04:40-9). Dieses Punktesystem bietet wiederum die Chance, spezifischere Schulungen durchzuführen (E2, 01:04:40-9). Eine Meldefunktion kann hingegen auch das Risiko darstellen, den Aufwand der IT stark zu erhöhen, denn Mitarbeitende werden mit grosser Wahrscheinlichkeit auch häufig Spam-E-Mails oder andere, nicht gefährliche Mails melden, die dann bearbeitet werden müssen (E1, 00:38:10-3; E2, 01:04:40-9; E4, 00:39-35-6; E6, 00:46:11-7). Die Bearbeitung der gemeldeten Mails führt zum nächsten Risiko. Wird für die gemeldeten Mails keine Rückmeldefunktion implementiert, mit der die Mitarbeitenden über die Korrektheit der Meldung informiert werden, können sie das Interesse am Melden verlieren (E4, 00:39-35-6; E6, 00:02:52-4). Zuletzt kann mit einer Meldefunktion auch das Risiko entstehen, dass dieses gar nicht genutzt wird, aus Angst, etwas Falsches zu melden, oder aus Furcht vor Konsequenzen (E5, 00:45:26-0; E7, 00:45:06-7).

4.3 Umfeld

Im Folgenden werden die Erkenntnisse aus den Experten:inneninterviews im letzten Bereich des TOE-Frameworks, dem Umfeld, beschrieben. Auf Basis der induktiven Kategorienbildung wurden die drei Aspekte «Einbindung externer Firmen», «Meldungen an Externe» sowie «Rechtliches» identifiziert. Die Strukturierung erfolgt anhand dieser Kategorien.

4.3.1 Einbindung externer Firmen

Auf dem Markt gibt es diverse Anbieter und Partner, die Phishing-Awareness-Trainings vertreiben. Die Zusammenarbeit mit solchen externen Partnern kann Chancen und Risiken beinhalten. Die grösste Chance besteht bei der Zusammenarbeit mit externen Partnern darin, dass vom Know-how dieser Partner profitiert werden kann, aufgrund ihrer Spezialisierung im Bereich des Phishing-Awareness-Trainings (E2, 01:14:21-2; E5, 00:52:59-9; E8, 00:49:48-5). Zusätzlich bieten solche Partner mehrheitlich Vorlagen und Unterstützung bei der Erstellung des Schulungsmaterials oder von Phishing-Simulation, was die Chance beinhaltet, den Aufwand in diesem Bereich zu reduzieren (E2, 01:14:21-2;

E4, 00:43:17-5; E5 01:02:33-9). Die Tatsache, dass besonders im Bereich von Security ein Fachkräftemangel herrscht, verstärkt die Chance der Aufwandsreduzierung durch die Auslagerung des Phishing-Awareness-Trainings (E1, 00:27:08-3). Ebenfalls kann es die Chance bieten, ein echtes Szenario darzustellen, und dem CISO ermöglichen, auch die Reaktion der IT zu testen (E4, 00:43:17-5; E6, 00:51:54-6). Die Zusammenarbeit mit externen Partnern kann jedoch auch zu Risiken führen. Externe Partner kennen das zu schulende Unternehmen mehrheitlich nur oberflächlich, was Problemen bei der Durchführung hervorrufen kann (E2, 01:16:17-0; E3, 00:41:05-2; E4, 00:43:17-5). Ebenfalls kann es vorkommen, dass die Partner im Ausland ansässig sind und dadurch andere Regelungen und Rechtslagen gelten (E1, 00:45:54-2; E2, 00:55:32-2; E7, 00:50:55-6). Die unterschiedlichen Rechtslagen sind ebenfalls aufgrund des Datenaustauschs zu beachten (E1, 00:25:51-7; E3, 00:43:44-4; E5, 00:51:34-8; E6, 00:55:16-1). Experte 4 empfiehlt daher, nur mit Partnern zusammenzuarbeiten, welche über ein ähnliches rechtliches Niveau wie das Zielland besitzen (E4, 00:45:58-9). Zusätzlich kann durch den Datenaustausch das Risiko entstehen, dass Daten durch Daten-Leaks abwandern und diese dann von echten Angreifenden genutzt werden (E1, 00:25:51-7; E2, 00:17:09-1; E7, 00:49:35-1). Dieses Risiko wird jedoch von den meisten Experten als gering eingestuft (E4, 00:44:37-5; E5, 00:55:04-0). Neben dem Datenaustausch werden externen Partnern teilweise auch Zugriffe wie beispielsweise auf das Active Directory gewährt (E2, 00:55:32-2). Hier muss gemäss Experte 2 sichergestellt werden, dass die Zugriffsrechte auf ein Minimum beschränkt werden (E2, 01:11:49-8).

4.3.2 Meldungen an Externe

Meldungen an externe Stellen wie Regierungsinstitutionen, Registrar, Hoster usw. bieten in der Praxis keine direkten Chancen. Externe Stellen über die Durchführung einer Phishing-Awareness-Kampagne zu informieren, hilft jedoch, Risiken zu minimieren (E1, 00:43:42-5; E4, 00:41:17-1). Die Experten empfehlen insbesondere die Institutionen NCSC früher MELANI beziehungsweise das nationale Cybersicherheitsdepartement, den Domain Registrar sowie die SWITCH den nationalen Domain-Verwalter, zu informieren (E1, 00:43:42-5; E2, 10:24:36-2; E3, 00:06:38-2; E4, 00:47:31-4; E5, 00:57:05-3). Ebenfalls kann es empfehlenswert sein, den Hoster der Phishing-Awareness-Plattform über die Durchführung des Phishing-Awareness-Trainings in Kenntnis zu setzen (E4, 00:48:23-1). Das Informieren externer Stellen hilft dabei, das Risiko zu minimieren, dass die Phishing-Awareness-Kampagne blockiert wird (E1, 00:43:42-5; E3, 00:45:57-0; E4,

00:48:23-1). Ebenfalls können dadurch Aufwendungen reduziert werden, die durch Meldungen einer Phishing-Simulation entstehen (E1, 00:52:29-5; E5, 00:57:05-3). Weiter sollten externe Firmen, deren Namen oder Logos in Phishing-Simulationen verwendet werden, vorgängig informiert und um Erlaubnis gefragt werden (E2, 10:24:36-2). Dadurch sollen rechtliche Konsequenzen vermieden werden.

4.3.3 Rechtliche Aspekte

Wie bereits in Kapitel 4.3.2, ergeben sich auch bei den rechtlichen Aspekten keine direkten Chancen. Die Berücksichtigung rechtlicher Aspekte hilft jedoch, Risiken zu minimieren. Aus den Experten:inneninterviews gehen diverse rechtliche Aspekte hervor, welche beachtet werden sollten. Zum einen sind dies landes- oder industriespezifische Regulierungen (E1, 00:03:49-1; E2, 00:25:36-5; E8, 00:52:27-5). Je nachdem, in welchem Land ein Phishing-Awareness-Training durchgeführt wird, müssen die Regulierungen des entsprechenden Landes, beachtet werden (E1, 00:03:49-1; E2, 00:25:36-5). Dies beinhaltet insbesondere Markenschutz-, Urheber- und Datenschutzrechte (E1, 00:47:00-5; E2, 01:18:56-8; E3, 00:05:30-6; E4, 00:41:17-1; E6, 00:05:52-2; E7, 00:05:17-4). Hinzu kommt, dass sich diese Regulierungen aufgrund von Ereignissen, wie beispielsweise Sanktionen, ändern können (E2, 01:07:47-6). Daher müssen diese Regulatoren auch immer wieder geprüft und das Verhalten entsprechend angepasst werden (E2, 01:07:47-6; E7, 00:47:24-5). Ebenfalls müssen rechtliche Aspekte beachtet werden, wenn, wie in Kapitel 4.3.1 beschrieben, mit externen Partnern zusammengearbeitet wird (E1, 00:45:54-2; E7, 00:50:55-6). Meldungen an externe Stellen, wie in Kapitel 4.3.2 beschrieben, oder Meldungen an externe Firmen können dabei helfen, rechtliche Risiken zu verringern (E1, 00:48:35-2; E3, 00:42:35-2; E4, 00:09:18-4). Zusätzlich empfiehlt Experte 7 bei Unsicherheit Abklärungen mit dem Datenschutzbeauftragten oder einem Rechtsdienst, um das Risiko rechtlicher Konsequenzen zu minimieren (E7, 00:52:16-2).

5 Auswertung OptiPhish

Im Rahmen des OptiPhish-Projekts wurde eine abschliessende Umfrage zur Studie durchgeführt. Aus der Umfrage resultierten 438 gültige Rückmeldungen, die noch nicht weiter untersucht wurden. Im nun folgenden Kapitel wird dieser Datensatz ausgewertet und die Resultate werden beschrieben.

Im OptiPhish-Projekt wurden über einen Zeitraum von zwölf Monaten 144 Kampagnen durchgeführt und insgesamt 288'000 Phishing-Simulations-E-Mails versendet. Die Umfrage zeigt, dass diese Anzahl an Phishing-Simulationen bei den Umfrageteilnehmern mehrheitlich negativ aufgenommen wird. Abbildung 4 zeigt, dass 62,1 % der Umfrageteilnehmenden diese Anzahl als zu hoch oder auch als deutlich zu hoch empfunden haben. Die gleiche Tendenz ergibt sich auch aus der Auswertung der individuellen Rückmeldungen in Abbildung 7. Von den 80 negativen Rückmeldungen bemängeln 32 Umfrageteilnehmende das Intervall und die Häufigkeit der durchgeführten Phishing-Simulationen. Die Empfindung gegenüber einer akzeptablen Anzahl an simulierten Phishing-E-Mails pro Jahr variiert hingegen zwischen null und 365. Von den 438 Umfrageteilnehmenden geben 416 Teilnehmende die für sie akzeptable Anzahl an Simulations-E-Mails pro Jahr an. Wie Abbildung 5 zeigt, empfinden 42,1 % null bis fünf E-Mails pro Jahr akzeptabel. Aber auch sechs bis zehn und elf bis 20 Simulations-E-Mails sind für je 20 % der Umfrageteilnehmenden angemessen. Weitere Punkte, die in der Umfrage befragt wurden, sind der Schwierigkeitsgrad und der Inhalt. Der Schwierigkeitsgrad wurde, wie Abbildung 4 zeigt, von mehr als 70 % der Umfrageteilnehmenden als zu einfach bewertet. Diese Bewertung ergibt sich auch aus der Auswertung der individuellen Rückmeldungen. Wie Abbildung 7 verdeutlicht, wird der Inhalt als zweithäufigster Grund für die negative Bewertung angegeben. Die Themen des Inhalts hingegen werden von fast 75 % als angemessen beurteilt. Das OptiPhish-Projekt erwies sich auch für mehr als die Hälfte der Umfrageteilnehmenden mit 58,2 % als hilfreich, wie in Abbildung 4 deutlich wird. Zuletzt werden die Phishing-Simulationen von 72,4 % der Umfrageteilnehmenden als akzeptables Mittel für ein Phishing-Awareness-Training empfunden, wie dies ebenfalls in Abbildung 4 dargelegt wird.

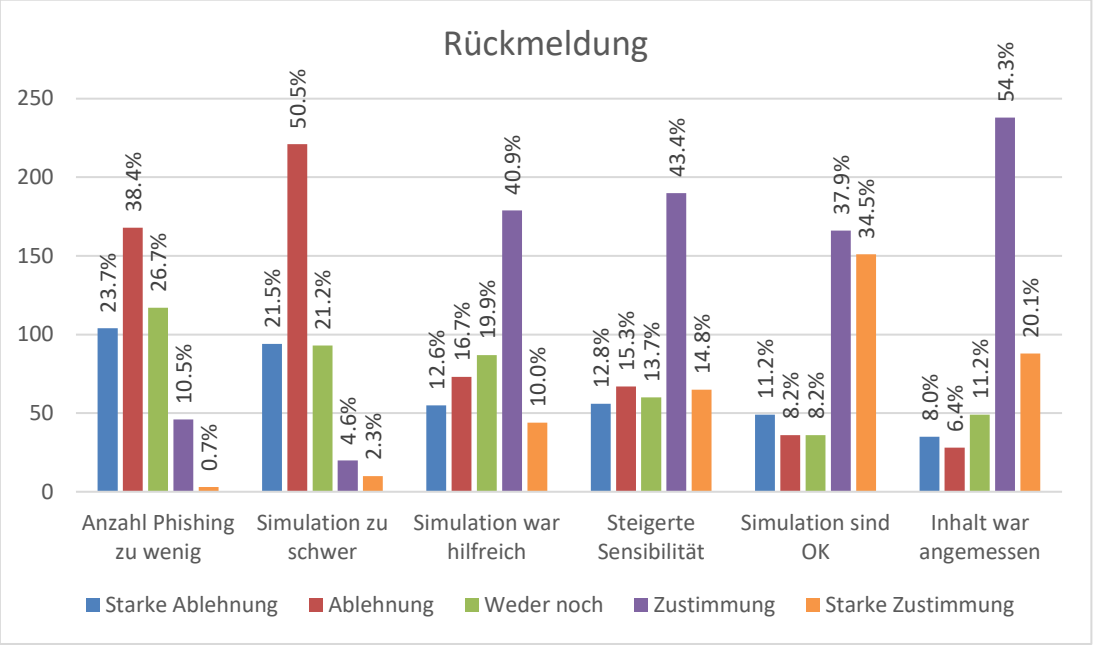

Abbildung 4: Übersicht aller Rückmeldungen

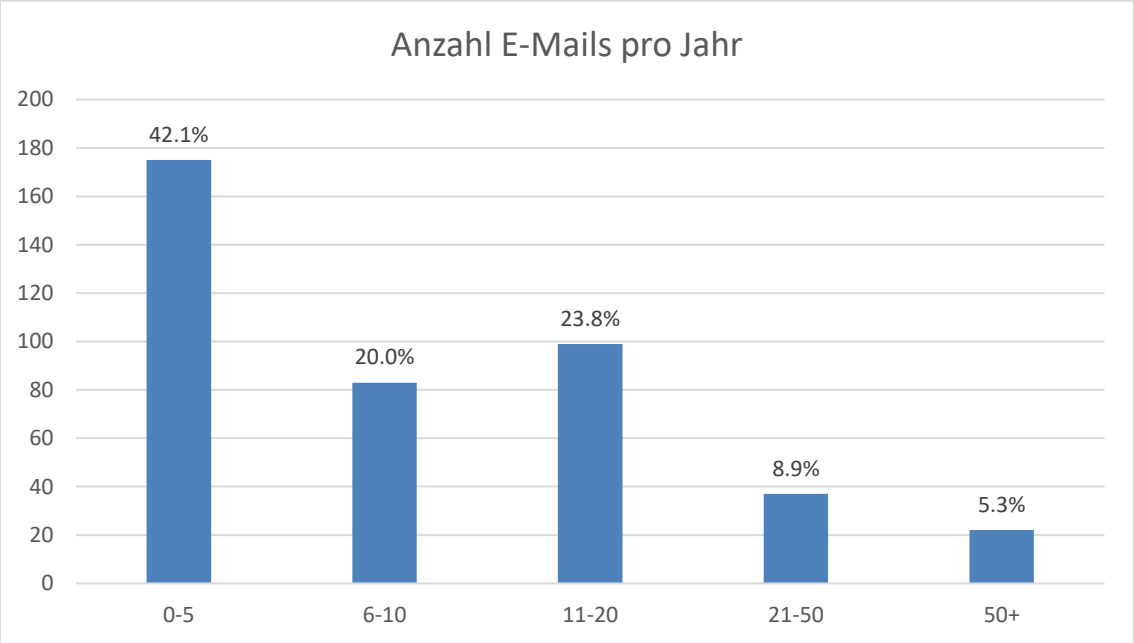

Abbildung 5: Anzahl akzeptabler E-Mails pro Jahr

Ebenfalls wird untersucht, ob die Anfälligkeit gegenüber einer den Phishing-Simulationen einen Einfluss auf die Akzeptanz der Umfrageteilnehmenden hatte. Hierbei hat sich kein signifikanter Unterschied gezeigt. Wie Abbildung 6 verdeutlicht, sind sowohl die positive als auch die negative Empfindung in etwa gleich, unabhängig davon, ob die Teilnehmenden auf eine Simulation hereingefallen sind oder nicht.

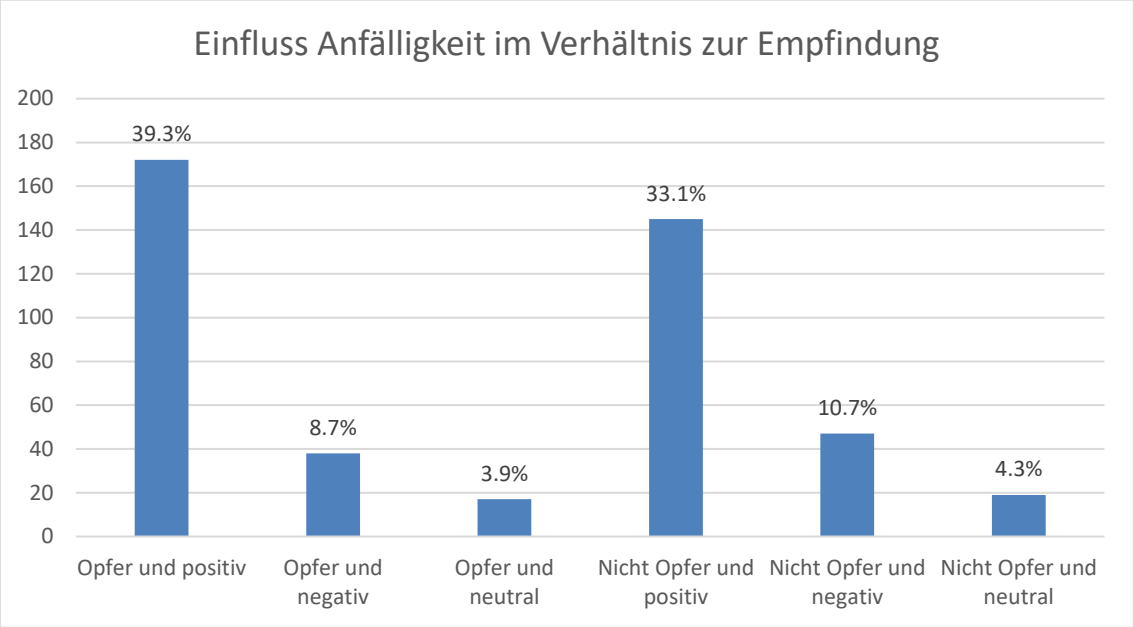

Abbildung 6: Empfindung im Verhältnis zur Anfälligkeit

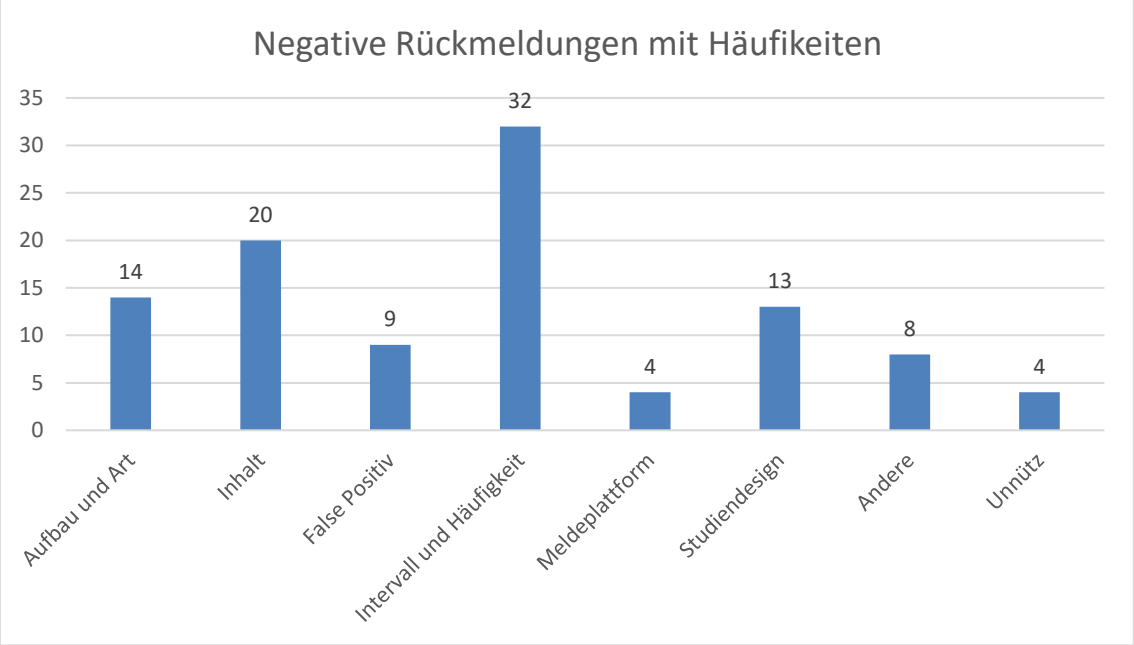

Abbildung 7: Kategorien der negativen Rückmeldungen

Als letzter Punkt wurden die individuellen Rückmeldungen untersucht. Diese wurden in «positiv» und «negativ» unterteilt und es wurden die entsprechenden Gründe ermittelt. Bei den positiven Rückmeldungen sind 23 von 54 Rückmeldungen nicht direkt einem Grund zuzuorden. Weiter werden, wie Abbildung 8 zeigt, der Inhalt und die Hilfestellung durch das Training als positiv bewertet. Die negativen Rückmeldungen variieren stärker. Wie im ersten Abschnitt dieses Kapitels beschrieben, sind die am häufigsten genannten

Gründe für die negativen Rückmeldungen der «Intervall und Häufigkeit» sowie der «Inhalt» der Phishing-Simulationen. Weiter stellt Abbildung 7 dar, dass der Aufbau und die Art sowie das Design der Studie als negativ empfunden wurden. Die restlichen Rückmeldungen kritisieren «False Positiv», die «Meldeplattform», die «Nützlichkeit» sowie Anderes am OptiPhish-Projekt.

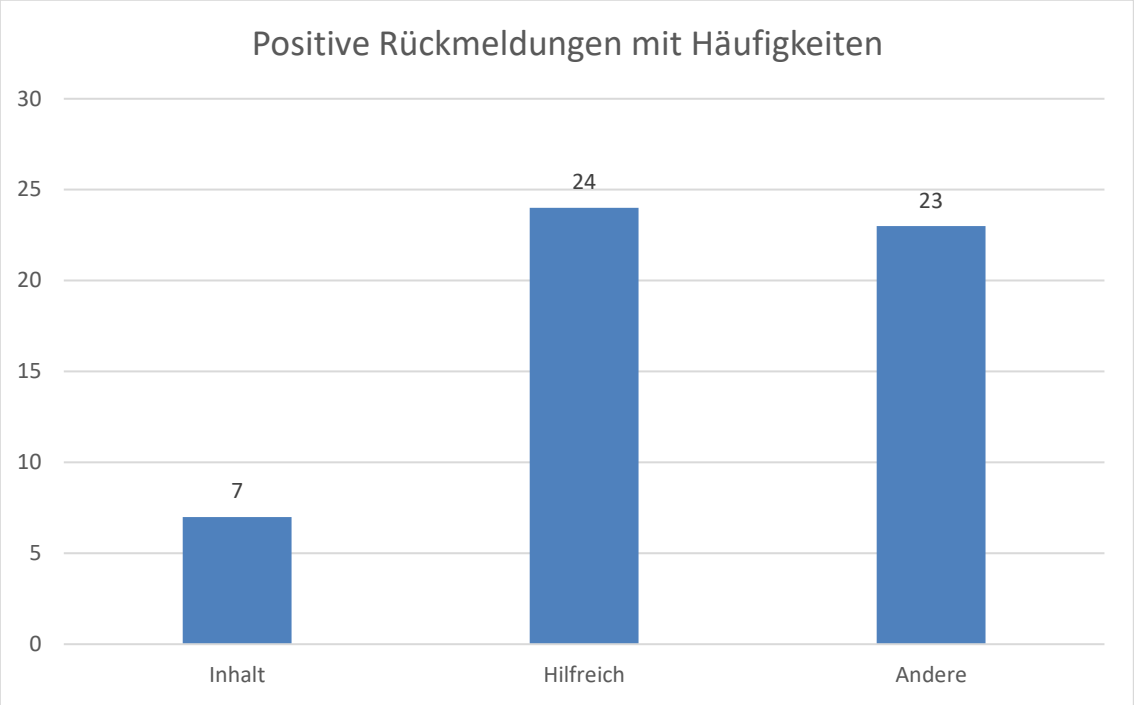

Abbildung 8: Kategorien der positiven Rückmeldungen

6 Schlussteil

In diesem Kapitel werden die Erkenntnisse aus dem Hauptteil nochmals aufgegriffen und verglichen. Ebenfalls folgt in diesem Kapitel die Beantwortung der Forschungfrage und der Arbeitsfragen. Ausserdem wird auf Basis der Resultate eine Schlussfolgerung gezogen und eine Handlungsempfehlung abgegeben. Zum Schluss erfolgen die Beschreibung der Limitationen dieser Arbeit sowie die Erörterung möglicher weiterführender Forschungen.

6.1 Diskussion

Im Folgenden werden die Ergebnisse aus der systematischen Literaturrecherche, den Experten:inneninterviews sowie dem Datensatz zusammengeführt. Die Erkenntnisse werden miteinander verglichen und kritisch hinterfragt. Ebenfalls wird auf die Beantwortung der Forschungsfrage sowie der Arbeitsfragen eingegangen. Für die Beantwortung der Arbeitsfragen werden die Chancen und Risiken, anhand der TOE-Bereiche tabellarisch dargestellt.

6.1.1 Organisatorisch

Eigenschaften und Verhalten der geschulten Mitarbeitenden

In den Kapiteln 3.1.1 und 4.1.4 wurden die eigenschafts- und verhaltensbezogen Einflussfaktoren in Bezug auf die Anfälligkeit auf Phishing-Angriffe beschrieben. Dass diese Eigenschaften und das Verhalten von Mitarbeitenden einen Einfluss auf die Anfälligkeit auf Phishing-Angriffe haben, konnte sowohl in der Literatur wie in Kapitel 3.1.1 beschrieben als auch in den Experten:inneninterviews identifiziert werden (E4, 00:17:30-0). Ebenfalls konnte in beiden Bereichen festgestellt werden, dass ein Risiko der Komplexität entstehen kann, wenn das Phishing-Awareness-Training auf diese Eigenschaften eingehen soll (Alseadoon et al., 2013, S. 6; E4, 00:12:30-0). Dennoch sollten gemäss den Autoren in der Literatur eigenschafts- und verhaltensbezogene Faktoren bei einem Phishing-Awareness-Training berücksichtigt werden (Abroshan et al., 2021b, S. 44939; Frank et al., 2022, S. 6). Dieser Meinung sind auch die Experten, jedoch empfehlen sie eine Unterscheidung anhand der Funktion, um das Komplexitätsrisiko zu reduzieren (E4, 00:12:30-0; E7, 00:06:38-2).

Art und Aufbau einer Schulung

Sowohl in der Literatur als auch in den Experten:inneninterviews zeigte sich, dass es im Bereich «Art und Aufbau» eines Phishing-Awareness-Trainings viele Aspekte und Möglichkeiten gibt, eine Schulung zu gestalten. In Kapitel 3.1.2 wurden Möglichkeiten der Schulungsmethode, wie die eingebettete oder die direkte Schulung, aufgezeigt (Alhashmi et al., 2021, S. 30; Kumaraguru et al., 2007, S. 72). In der Literatur gilt dabei die eingebettete Schulung als die effektivste (Jaeger & Eckhardt, 2021, S. 429–449; Jampen et al., 2020, S. 34; William et al., 2022, S. 813). Ebenfalls wurden unterschiedliche Schulungsmedien wie die Face-to-Face-Schulung oder die Online-Schulung aufgezeigt (Alhashmi et al., 2021, S. 30; Darem, 2021, S. 7948). Der Inhalt kann wiederum mit unterschiedlichen Varianten vermittelt werden. Bekannt sind die Medien «Video», «Game», «Text» oder «webbasiert» (Alhashmi et al., 2021, S. 30). Die in den Kapiteln 3.1.1 und 4.1.4 beschriebenen unterschiedlichen Eigenschaften und Verhaltensweisen zeigen auch, dass Mitarbeitende unterschiedliche Lerntypen aufweisen (E4, 00:17:30-0). Daher sollten die Schulungsmethoden und die Schulungsmedien auf die Zielgruppe abgestimmt sein (E4, 00:17:30-0). Sowohl aus der Literatur als auch aus den Experten:inneninterviews ging jedoch hervor, dass das Abstimmen auf die Zielgruppe ein Risiko der Komplexität hervorrufen kann (E1, 00:12:31-4). Daher empfehlen die Experten, möglichst alle unterschiedlichen Schulungsmethoden und -medien anzuwenden (E4, 00:17:30-0; E3, 00:13:35-4; E8, 00:27:25-4). Damit kann das Phishing-Awareness-Training für die Mitarbeitenden interessant gestaltet und die Motivation der Mitarbeitenden hochgehalten werden (E7, 00:14:56-0; E6, 00:16:45-4; E5, 00:17:46-8). Die Berücksichtigung unterschiedlicher Schulungsmethoden und -medien kann somit gemäss der Literatur, wie in Kapitel 3.1.2 beschrieben, und gemäss den Experten:inneninterviews, wie in Kapitel 4.1.5 beschrieben, die Chance bieten, die Schulung effektiv und effizient zu gestalten und gleichzeitig die Motivation für das Training bei den Mitarbeitenden hochzuhalten. Im Gegenzug kann diese Berücksichtigung aufgrund der vielen Varianten und der unterschiedlichen Eigenschaften das Risiko der Komplexität bilden und dadurch den Aufwand stark steigern.

Bei der Durchführung eines Phishing-Awareness-Trainings ergeben sich diverse Bestimmungen, welche getroffen werden sollten. Diese Bestimmungen bieten sowohl Chancen als auch Risiken. Alshaikh et al. (2018, S. 5091–5092) nennt unter anderem das Risiko

von einer nicht ausreichenden Betrachtung unterschiedlicher Aspekte bei einer zu schnellen Implementierung. Eine weitere Bestimmung betrifft das Informieren der Mitarbeitenden sowie des IT-Personals. Diese Bestimmung ist sowohl in der Literatur als auch in der Praxis umstritten. Ein Teil der Autoren und Experten ist überzeugt davon, dass Mitarbeitende und das IT-Personal über die Durchführung des Phishing-Awareness-Trainings informiert werden sollten (Kumaraguru et al., 2009; Miranda, 2018, S. 9–10; E7, 00:16:46-3). Andere Autoren und Experten sind hingegen der Meinung, dass keine Information über die Durchführung eines Phishing-Awareness-Trainings erfolgen sollte (Miranda, 2018, S. 9–10; E2, 00:29:55-9). Grund für die Diskussion ist die Erkenntnis, dass alle Mitarbeitenden unabhängig von ihrem technischen Wissen gleich anfällig auf Phishing-Angriffe reagieren (Alwanain, 2019, S. 327; Ebner, 2018, S. 46; Jampen et al., 2020, S. 22; E7, 00:16:46-3). Im Gegenzug kann das Informieren der Mitarbeitenden und des IT-Personals den Schulungseffekt mindern oder ein falsches Handeln des IT-Personals auslösen (Miranda, 2018, S. 9–10; E1, 00:15:25-0). Ein Grossteil der Experten empfiehlt daher, Schlüsselstellen zu informieren, um die Risiken zu minimieren und dennoch von den Chancen zu profitieren (E4, 00:21:06-7; E3, 00:17:50-7; E1, 00:14:16-9; E5, 00:20:46-7; E6, 00:21:16-9). Unabhängig von einer vorgängigen Information über das Phishing-Awareness-Training sind aber die Forschenden in der Literatur wie auch die Experten der gleichen Auffassung, dass alle Mitarbeitenden geschult werden sollten (William et al., 2022, S. 813; E1, 00:14:16-9; E2, 00:29:55-9; E4, 00:21:06-7; E3, 00:17:50-7; E5, 00:20:46-7; E6, 00:21:16-9; E7, 00:16:46-3). Sowohl das Informieren als auch das Nichtinformieren der Mitarbeitenden und des IT-Personals bringen jeweils Chancen und Risiken. Das Informieren der Mitarbeitenden direkt nach einem Fehlverhalten kann die Chance nutzen, den Schulungseffekt zu steigern (Singh et al., 2023, S. 1–2; Volkamer et al., 2020, S. 519–520; E6, 00:21:16-9). Jedoch wird das Risiko geschaffen, dass die Mitarbeitenden miteinander kommunizieren und dadurch der Schulungseffekt gemindert wird (Miranda, 2018, S. 9–10). Das Nichtinformieren kann die Chance bieten, einen besseren Trainingseffekt zu erzielen, indem alle geschult werden, und auch die Chance bieten die Reaktion des IT-Personals zu prüfen (Alwanain, 2019, S. 327; Anawar et al., 2019, S. 327; Ebner, 2018, S. 46; Jampen et al., 2020, S. 22; E6, 00:21:16-9). Als Risiko können jedoch falsche Reaktion durch das IT-Personal ausgelöst oder das Training kann durch die IT gestoppt werden (Kumaraguru et al., 2009; Miranda, 2018, S. 9–10; E6, 00:21:16-9). Im Bereich der Bestimmungen wurden jedoch noch weitere Aspekte in der Literatur oder von den Experten genannt, welche zu Chancen und Risiken führen können. In der

Literatur werden die Bestimmung einer Durchführungspflicht oder Belohnungen und Bestrafungen genannt. Belohnungen und Bestrafungen können die Chance bieten, dass die Durchführung des Trainings sichergestellt werden kann (Alwanain, 2019, S. 323; Bora et al., 2020, S. 1165). Gleichzeitig bieten Belohnungen und Bestrafungen das Risiko, dass die Motivation der Mitarbeitenden und der Lerneffekt des Trainings gesenkt werde (Alwanain, 2019, S. 323; Bora et al., 2020, S. 1165). Aus den Experten:inneninterviews ging zusätzlich die Chance hervor, dass die IT-Richtlinien den Mitarbeitenden kommuniziert werden können und sichergestellt wird, dass diese auch gelesen werden (E2, 00:10:44-5). Ebenfalls kann das Risiko entstehen, dass Mitarbeitende sich gegen das Phishing-Awareness-Training äussern, wenn bei Auswertung des Trainings, Rückschlüsse auf einzelne Mitarbeitende gezogen werden (E3, 00:08:38-3; E7, 00:08:21-4).

Ein weiterer Faktor ist der Inhalt einer Schulung und deren Aktualität. Angreifende passen ihre Angriffsmethoden laufend an und verwenden aktuelle Ereignisse (Zainab et al., 2021, S. 17). Damit die Effektivität eines Phishing-Awareness-Trainings gewährleistet werden kann, sollte daher das Schulungsmaterial sowohl gemäss der Literatur als auch gemäss den Experten aktuell gehalten und es sollten auch aktuelle Ereignisse einbezogen werden (Rosser et al., 2022, S. 133; E7, 00:01:55-4; E4, 00:02:34-4; E2, 01:07:47-6; E3 00:08:38-3). Jedoch müssen gemäss Experte 5 aktuelle Themen mit Vorsicht gewählt werden, da sonst das Risiko entstehen kann, dass sich Mitarbeitende persönlich betroffen fühlen (E5, 00:49:22-0).

Ein zentraler Faktor, welcher sich indirekt aus den Eigenschaften und dem Verhalten der Mitarbeitenden sowie den Schulungsmethoden und den Schulungsmedien ergab, ist die Personalisierung des Phishing-Awareness-Trainings. Sowohl die Literatur, wie in Kapitel 3.2.1 beschrieben, als auch die Experten, wie in Kapitel 4.1.5 beschrieben, vertreteten den gleichen Standpunkt, dass eine Personalisierung der Schulung sinnvoll ist. Eine Personalisierung ermöglicht es, Schulungen besser auf die Realität abzustimmen und beispielsweise die Abwehr gegen Spear-Phishing-Angriffe zu schulen (Alshaikh et al., 2021, S. 1; Rizzoni et al., 2022, S. 11; Roepke et al., 2020, S. 65). Zudem bietet es die Chance, eine effektivere und qualitativ bessere Schulung zu gewährleisten, indem etwa Schwierigkeitsgrade verwendet werden (Alshaikh et al., 2021, S. 1; Jaeger & Eckhardt, 2021, S. 449; Rizzoni et al., 2022, S. 11; Roepke et al., 2020, S. 65). Zusätzlich kann dadurch die Motivation der Mitarbeitenden gesteigert werden, indem besser auf diese eingegangen wird (Alshaikh et al., 2021, S. 1; Rizzoni et al., 2022, S. 11; Roepke et al., 2020, S. 65). Die

Personalisierung kann jedoch, wie im Bereich «Eigenschaften und Verhalten der geschulten Mitarbeitenden» beschrieben, das Risiko der Komplexität schaffen. Diesem Risiko kann allerdings entgegengewirkt werden, indem die Schulung die Funktion beziehungsweise den Aufgabenbereich berücksichtigt (Rizzoni et al., 2022, S. 11; Roepke et al., 2020, S. 65; William et al., 2022, S. 812–813; E7, 00:06:38-2; E4, 00:12:30-0; E3, 00:08:38-3; E5, 00:10:05-3; E6, 00:10:22-3; E1, 00:08:40-0). Gemäss den Experten können aber durch zu starke Personalisierung auch Risiken entstehen, wie das Verfälschen von Klickraten, die Angst vor Phishing bei regulären E-Mails oder die Ablehnung bei den Mitarbeitenden (E8, 00:23:29-3; E1, 00:09:52-6; E5, 00:12:11-2; E8, 00:23:29-3).

Als letzter Aspekt innerhalb der Bestimmung gilt es, das Intervall zu betrachten. Sowohl die Literatur als auch die Experten befinden, dass ein Phishing-Awareness-Training kontinuierlich durchgeführt werden muss (Volkamer et al., 2018, S. 123; E2, 00:10:44-5; E3, 00:10:35-4; E4, 00:17:30-0; E7, 00:29:34-9; E8, 00:05:06-1). Durch die Kontinuität kann die Chance genutzt werden, dass das Gelernte Präsent bleibt (Volkamer et al., 2018, S. 123). Ein zu kurzes Intervall kann jedoch aufgrund der Zeitintensität das Risiko schaffen, die Mitarbeitenden zu verärgern und die Motivation zu senken (Desolda et al., 2022, S. 26; Jampen et al., 2020, S. 38; Rizzoni et al., 2022, S. 11; (E3, 00:13:35-4; E4, 00:04:18-9; E5, 00:01:48-0; E6, 00:16:45-4; E8, 00:07:45-1). Dies zeigt sich auch in der Auswertung des OptiPhish-Datensatzes in Abbildung 4, bei dem die Mehrheit der Umfrageteilnehmenden das Intervall bemängelte. Zusätzlich kann gemäss Experte 3 eine Variation des Intervalls den Trainingseffekt steigern, da die Mitarbeitenden nicht wissen, wann simulierte Phishing-Angriffe durchgeführt werden, und dadurch dauerhaft vorsichtig reagieren (E3, 00:16:27-7).

Normen, Richtlinien und kulturelle Aspekte

Die Meinung in Bezug auf Normen, Richtlinien und Kultur differiert in Literatur und Expertenaussagen. Die Forschenden sehen Normen und Richtlinien zur Schaffung einer Cybersicherheitskultur als wirksamer und effektiver, anstelle eines Phishing-Awareness-Trainings, an (Alshaikh, 2020, S. 7–8; Corradini & Nardelli, 2019, S. 194; Petrič & Roer, 2022; Shahbaznezhad et al., 2021, S. 545). Die Experten hingegen vertreten die Meinung, dass Phishing-Awareness-Trainings einen Teil der Cybersicherheitskultur darstellen und daher keine Unterscheidung zwischen Cybersicherheitskultur und Phishing-Awareness-Trainings gemacht werden kann (E1, 00:16:44-4; E2, 00:38:51-2; E3, 00:20:10-9; E4,

00:23:00-9; E6, 00:24:15-7; E7, 00:19:49-3). Als Risiko wird in der Literatur die Schwierigkeit und Langwierigkeit für den Aufbau einer Cybersicherheitskultur genannt (Leidner & Kayworth, 2006, S. 357). Die Experten hingegen sehen die Chance einer gegenseitigen Unterstützung von der Cybersicherheitskultur und dem Phishing-Awareness-Training (E1, 00:16:44-4; E2, 00:38:51-2; E3, 00:20:10-9; E4, 00:23:00-9; E6, 00:24:15-7; E7, 00:19:49-3).

Ethische Aspekte

Phishing-Awareness-Trainings werden sowohl in der Literatur als auch von den Experten als ethische Grauzone beschrieben (Sutter et al., 2022, S. 2; E1, 00:19:23-7). In der Literatur wird die Möglichkeit erwähnt, Phishing-Kampagnen von ethischen Kommissionen prüfen zu lassen, um die ethische Korrektheit sicherzustellen(Sutter et al., 2022, S. 5). Eine solche Prüfung kann jedoch das Risiko eines erhöhten Aufwands sowie einer Verzögerung aufzeigen, da sie viel Zeit in Anspruch nehmen kann (Nijland, 2022, S. 7). Die Experten hingegen empfehlen, dass Phishing-Kampagnen mit der nötigen Vorsicht und der Berücksichtigung der Zielgruppen ethisch korrekt gestaltet werden (E1, 00:09:52-6; E2, 00:45:16-4; E3, 00:11:57-3; E6 00:26:14-3; E8, 00:36:25-1). Dadurch soll das Risiko minimiert werden, Mitarbeitende auf ethischer Ebene zu beeinträchtigen.

Aspekte der internen Rechtfertigung

Klickraten werden im Zusammenhang mit Phishing-Awareness-Trainings als Messinstrument und anschliessend als Argumentationsgrundlage verwendet (Steves et al., 2020, S. 1–12; E1, 00:20:49-2; E4, 00:29:26-7; E7, 00:28:11-1). Sowohl, die Literatur als auch die Experten weisen im Zusammenhang mit Klickraten auf das Risiko der Verfälschung und die daraus folgenden Fehlentscheidungen hin (Steves et al., 2020, S. 1–12; E1, 00:20:49-2; E3, 00:20:10-9; E4, 00:29:55-4; E5, 00:01:48-0; E6, 00:28:36-7). Klickraten sollten daher immer im Kontext mit anderen Variablen wie Schwierigkeitsgrad oder Korrektheit der Daten betrachtet werden (Steves et al., 2020, S. 1–12; E1, 00:20:49-2; E2, 00:53:19-5; E3, 00:23:58-3; E4, 00:26:53-7; E5, 00:01:48-0; E6, 00:28:36-7; E7, 00:25:12-2; E8, 00:23:29-3).

Risikominimierung

Die generelle Chance, welche sich aus einem Phishing-Awareness-Training ergibt und sich sowohl in den Experten:inneninterviews als auch indirekt im gesamten Kapitel 3 zeigt, ist die Risikominimierung gegenüber einem Cybervorfall (E3, 00:02:58-8; E2, 00:10:44-5; E4, 00:02:34-4). Diese Risikominimierung entsteht durch die Sensibilisierung der Mitarbeitenden auf das Thema «Phishing». Ebenfalls soll Phishing-Awareness, gemäss den Experten 6 und 7, zusätzlich die Chance bieten, den Mitarbeitenden das Thema «Sicherheit» näherzubringen und ihnen dieses auch für ihren privaten Alltag zugänglich machen (E6, 00:01:03-9; E7, 00:08:32-4). Dies wird zudem im OptiPhish-Datensatz, wie in Abbildung 8 dargestellt, bestätigt, indem die Mehrheit angab, dass die Trainings hilfreich waren. Zusätzlich wurde in den individuellen Rückmeldungen bestätigt, dass das erlernte Wissen auch im privaten Alltag hilfreich sei.

Repräsentation des Security-Teams

Experte 2 nennt neben den bereits identifizierten Chancen eine weitere Chance, welche sich durch das Phishing-Awareness-Training ergibt. Security-Teams arbeiten aus Sicht der Mitarbeitenden mehrheitlich im Hintergrund (E2, 01:16:53-6). Phishing-Awareness-Trainings ermöglichen es dem Security-Team, sich gegenüber den Mitarbeitenden zu präsentieren (E2, 00:10:44-5). Das Phishing-Awareness-Training ist hierbei eine geeignete Methode, da es sich um ein Thema handelt, welches für die Mitarbeitenden sichtbar und greifbar ist (E2, 01:16:53-6).

Kosten und Aufwand

Kosten und Aufwand sind weitere Risikoaspekte, welche sich aus Kapitel 3 und den Experten:inneninterviews ergeben. Phishing-Awareness-Trainings können hohe Aufwendungen und Kosten verursachen (Zainab et al., 2021, S. 17; E3, 00:03:42-8; E4, 00:10:52-0; E1, 00:03:49-1; E7, 00:03:06-1; E3, 00:49:21-2). Die Aufwendungen entstehen sowohl seitens der Mitarbeitenden als auch auf der Seite der Durchführung und Auswertung eines Phishing-Awareness-Trainings (Volkamer et al., 2018, S. 120; E1, 00:03:49-1; E2, 00:10:44-5; E1, 00:02:54-5).

Schlussfolgerung

Im organisatorischen Bereich ergeben sich diverse Chancen und Risiken, welche aus dem Phishing-Awareness-Training resultieren können. Viele der Chancen und Risiken betreffen einzelne Aspekte der Gestaltung eines Trainings, wie etwa das Intervall oder die Personalisierung des Trainings. Es zeigen sich auch Chancen und Risiken, wie in Tabelle 8 dargestellt, welche unabhängig von der Gestaltung des Trainings entstehen. Die Arbeitsfrage AF2 «Welche organisatorischen Aspekte ergeben sich bei der Durchführung eines Phishing-Awareness-Trainings?» lässt sich anhand der bedeutendsten organisatorischen Chancen, wie der «Risikominimierung gegenüber Cyberangriffen» und «Sensibilisierung der Mitarbeitenden» sowie anhand der bedeutendsten organisatorischen Risiken, «den hohen Aufwand und Kosten» sowie die «Zeitverschwendung der Mitarbeitenden», beantworten. Generell kann die Arbeitsfrage AF2 jedoch anhand allen generellen organisatorischen Aspekten in der Tabelle 8 sowie den in Tabelle 9 aufgelisteten organisatorischen Aspekten der Gestaltung des Trainings beantwortet werden.

Tabelle 8: Generelle organisatorische Chancen und Risiken

Organisatorisch			
Erkenntnisse	E	L	D
Chancen			
Risikominimierung gegenüber Cyberangriffen	✓	✓	×
Sensibilisierung der Mitarbeitenden	✓	✓	×
Securuity-Thema und Security-Team den Mitarbeitenden näher bringen	✓	×	✓
Sensibilisierung der Mitarbeitenden auch im Privatleben	✓	×	✓
Risiken			
Hohe Aufwendungen und Kosten	✓	✓	×
Zeitverschwendung der Mitarbeitenden bei falscher Durchführung	✓	✓	×
Verärgerung der Mitarbeitenden	✓	✓	×
Legende: E = Experten, L = Literatur, D = Datensatz			

Je nach Gestaltung des Trainings sind die Chancen und Risiken in Tabelle 9 relevant.

Tabelle 9: Organisatorische Chancen und Risiken anhand der Gestaltung des Trainings

Organisatorisch				
Gestaltungsart	**Erkenntnisse**	E	L	D
Chancen				
Personalisierung des Inhaltes anhand der Eigenschaften und Verhalten der Mitarbeitenden	Steigerung der Effektivität und Qualität der Schulung	✓	✓	×
Personalisierung der Schulungsart und des Aufbaus anhand der Eigenschaften und Verhalten der Mitarbeitenden	Steigerung der Effektivität und Qualität der Schulung	✓	✓	×
Informieren der Mitarbeitenden und IT	Vermeidung von Aufwendungen sowie Vermeidung falscher Reaktion durch das IT-Personal	✓	✓	×
Nichtinformieren der Mitarbeitenden und IT	Steigerung des Trainingseffekts und Möglichkeit zum Testen der Reaktion der IT	✓	✓	×
Durchführungspflicht	Sicherstellen der Durchführung des Trainings und dadurch höhere Effektivität	×	✓	×
Kommunikation der IT-Richtlinien innerhalb des Trainings	Sicherstellung, dass die IT-Richtlinie gelesen wird	✓	×	×
Rückschlüsse auf einzelne Mitarbeiter und Ihre Ergebnisse ziehen	Verbesserung des Schulungseffekts durch spezifische Schulungen	✓	×	×
Schulungsinhalt anhand von aktuellen Ereignissen aktuell halten	Steigerung der Effektivität durch Schaffung realitätsnaher Trainings	✓	✓	×
Verwendung eines angemessenen oder unangemessenen Intervall	Steigerung der Effektivität durch Kontinuität	✓	✓	×
Verwendung von Normen, Richtlinien und Kultur als Phishing-Awareness-Training	Normen, Richtlinien und Kultur können das Phishing-Awarness-Training unterstützen und versa versa	✓	×	×
Risiken				
Personalisierung des Inhaltes anhand der Eigenschaften und Verhalten der Mitarbeitenden	Steigerung der Komplexität und des Aufwandes, Verfälschung von Klickraten, Inakzeptanz der Mitarbeitenden und Angst vor legitimen E-Mails	✓	✓	×
Personalisierung der Schulungsart und des Aufbaus anhand der Eigenschaften und Verhalten der Mitarbeitenden	Steigerung der Komplexität und des Aufwandes	✓	✓	×
Implementierungszeit	Nicht ausreichenden Betrachtung unterschiedlicher Aspekte bei einer zu schnellen Implementierung	×	✓	×

Informieren der Mitarbeitenden und IT	Minderung des Schulungseffekts durch Wachsamkeit und Warnungen unter den Mitarbeitenden	✓	✓	×
Nichtinformieren der Mitarbeitenden und IT	Generierung von Aufwendungen sowie hervorrufen von falscher Reaktionen durch die IT	✓	✓	×
Durchführungspflicht	Senkung der Motivation der Mitarbeitenden	×	✓	×
Rückschlüsse auf einzelne Mitarbeiter und Ihre Ergebnisse ziehen	Generierung von Ängsten und Widerstand	✓	×	×
Schulungsinhalt anhand von aktuellen Ereignissen aktuell halten	Gefühl eines persönlichen Angriffes bei den Mitarbeitenden schaffen	✓	×	×
Verwendung eines angemessenen oder unangemessenen Intervall	Verärgerung der Mitarbeitenden	✓	✓	×
Verwendung von Normen, Richtlinien und Kultur als Phishing-Awareness-Training	Schwer und lang zu implementieren	×	✓	×
Interne Argumentation mit Klickraten	Gefahr falsche Entscheidungen zu treffen aufgrund falscher Beurteilung der Klickraten	✓	✓	×
Beachtung und Nichtbeachtung ethischer Normen	Verzögerungen bei Implementation, wenn ethische Korrektheit durch Kommission geprüft wird und ethische Angriffe der Mitarbeitenden, wenn ethische Aspekte nicht berücksichtigt werden	✓	✓	×
Legende: E = Experten, L = Literatur, D = Datensatz				

Nicht alle Chancen und Risiken, welche sich aus den Experten:inneninterviews ergaben, konnten durch die Literatur bzw. die Auswertung des Datensatzes bestätigt werden oder vice versa. Erkenntnisse, welche bestätigt werden konnten, werden als relevanter angesehen. Dennoch sind Ergebnisse, welche ausschliesslich in der Literatur oder ausschliesslich aus den Experten:inneninterviews gewonnen wurden, nicht zu vernachlässigen. Es empfiehlt sich aber, diese Erkenntnisse mit Vorsicht zu betrachten.

6.1.2 Technologisch

Systemlösungen

Für die Implementation von Phishing-Awareness-Trainings werden üblicherweise Systemlösungen verwendet, welche On-Premise oder als SaaS-Lösung betrieben werden können. In der Literatur ergeben sich unterschiedliche Chancen und Risiken in Bezug auf

diese Systemlösungen. Je nach Lösung kann das Risiko entstehen, dass Anbieter die Schulungsinhalte nicht aktuell gestalten oder nicht ausreichend Individualisierungsmöglichkeiten bestehen (Burita et al., 2022, S. 12; Higashino et al., 2019, S. 82). Die Experten erwähnen die Chance, dass bei einer SaaS-Lösung die Möglichkeit einer effizienten und kostengünstigeren Lösung entsteht (E1, 00:27:08-3). Sie weisen jedoch auch auf das Risiko hin, dass mit einer Systemlösung nicht davon ausgegangen werden darf, dass keine Aufwendungen entstehen (E3, 00:41:05-2). Ebenfalls kann das Risiko einer falschen Zustellung der Inhalte oder Sicherheitslücken durch Fehlkonfiguration entstehen, welches sich jedoch unabhängig von der Systemlösung ergeben kann (E1, 00:04:35-4).

Technische Abwehrmassnahmen

Technische Abwehrmassnahmen wie Spamfilter, SPF-Filter, DKIM und DMARK werden in der Praxis eingesetzt, um echte Phishing-Angriffe abzuwehren (Alabdan, 2020, S. 24; Althobaiti et al., 2021, S. 11–12; Kumaraguru et al., 2009). Diese Massnahmen können im Zusammenhang mit Phishing-Awareness-Trainings das Risiko schaffen, dass auch Trainings und die simulierten Phishing-E-Mails blockiert werden (Kumaraguru et al., 2009; E1, 00:24:09-2; E7, 00:03:06-1). In der Praxis werden gemäss der Literatur und gemäss den Experten daher sogenannte Whitelistings eingerichtet, um diese Filter zu umgehen und das Risiko einer fälschlichen Blockierung der Trainings zu minimieren (Volkamer et al., 2020, S. 519–520; E1, 00:24:09-2; E7, 00:03:06-1). Diese Massnahme kann wiederum das Risiko schaffen, dass die Whitelistings von Phishenden mittels E-Mail-Spoofing ausgenutzt werden (Volkamer et al., 2020, S. 519–520; E1, 00:24:09-2; E2, 00:17:09-1; E3, 00:28:07-4; E7, 00:32:13-1). Hingegen sehen die Experten dieses Risiko als gering an und es kann mit einer korrekten Konfiguration ebenfalls noch mehr minimiert werden (E6, 00:31:47-0; E3, 00:28:07-4).

Vertrauen in die Technik

Die zuvor beschriebenen technischen Abwehrmassnahmen sorgen sowohl gemäss der Literatur als auch gemäss den Experten für ein falsches Vertrauen in die Technik (Butavicius et al., 2020, S. 2; Jampen et al., 2020, S. 19–29; E1, 00:29:06-3; E2 00:15:21-9; E4. 00:32:07-8; E5, 00:32:33-9; E6. 00:33:16-1; E7, 00:34:57-9). Sowohl in der Literatur als auch bei den Experten findet sich die Einstellung, dass Phishing-Awareness die Chance bietet, dieses falsche Vertrauen zu reduzieren, indem den Mitarbeitenden die Grenzen der technischen Abwehrmassnahmen aufgezeigt werden (Butavicius et al., 2020, S. 8; E1,

00:29:06-3; E2, 00:57:19-7; E4, 00:32:07-8; E5, 00:32:33-9; E6, 00:33:16-1; E7. 00:34:57-9). Durch das Aufzeigen der Grenzen können das Fehlverhalten und dadurch das Risiko eines Cybervorfalls reduziert werden (Butavicius et al., 2020, S. 8). Ebenfalls kann den Mitarbeiten aufgezeigt werden, dass sie einen Teil der Sichheit darstellen (E1, 00:29:06-3; E3, 00:30:20-1; E5, 00:32:33-9; E6, 00:33:16-1; E7, 00:34:57-9).

Technische Warnhinweise

Neben den technischen Abwehrmassnahmen besteht auch die Möglichkeit, technische Warnhinweise als zusätzlichen Faktor für die Mitarbeitenden zu implementieren. Die Verwendung von Warnhinweisen ist sowohl in der Literatur als auch bei den Experten umstritten. Mehrere Autoren sowie Experten sehen Warnhinweise als Chance, um einen weiteren Schutzmechanismus einzubinden (Kävrestad et al., 2022, S. 2; Yang et al., 2017; E2, 01:00:57-4; E3 00:31:52-3; E5 00:36:11-7; E7, 00:37:27-5; E8, 00:44:06-1). Andere Autoren und Experten sehen Risiken, indem sie den Effekt dieser Warnhinweise anzweifeln, oder zusätzliche Risiken, wie die Warnung von Mitarbeitenden vor simulierten Phishing-E-Mails (Desolda et al., 2022, S. 144; Jampen et al., 2020, S. 35–36; E1, 00:31:08-7; E4 00:34:43-4; E6 00:36:49-8;E8, 00:44:06-1). Gleicher Meinung sind sich die Forschenden und die Experten hingegen dabei, dass, wenn die Warnhinweise zu häufig oder zu unauffällig auftreten, das Risiko der Blindheit gegenüber diesen Warnungen entsteht (Desolda et al., 2022, S. 144; Jampen et al., 2020, S. 35–36; E2, 01:01:37-1; E6, 00:40:58-7; E7, 00:37:27-5; E1, 00:33:23-4; E5, 00:39:43-4; E8, 00:44:06-1).

Unterschiedliche Plattformen

Mobiles Arbeiten ist mittlerweile Teil des Alltags eines Unternehmens. Dazu gehört es, auch E-Mails auf mobilen Endgeräten wie Mobiltelefonen, Tablets, Smartwatches usw. zu prüfen. Die technischen Voraussetzungen, um E-Mails auf Phishing zu prüfen, unterscheiden sich bei mobilen Plattformen gegenüber dem Desktop-E-Mail-Client (Dixon et al., 2022, S. 2; Rizzoni et al., 2022, S. 11; E1, 00:35:39-4; E4, 00:37:22-4; E3, 00:33:38-6; E5, 00:44:09-9; E8, 00:48:59-7). Diese Tatsache zu berücksichtigen und mobile Plattformen im Schulungsmaterial zu integrieren, bietet die Chance eines effektiveren Schutzes, indem den Mitarbeitenden der sichere Umgang auch mit mobilen Plattformen gezeigt wird (Dixon et al., 2022, S. 2; Rizzoni et al., 2022, S. 11; E1, 00:41:20-0; E3, 00:33:38-6; E5, 00:44:09-9; E7, 00:43:21-2). Die Vielzahl an Tools und Plattformen schaffen das

Risiko der Komplexität und des Aufwands, um die Mitarbeitenden auf den unterschiedlichen Plattformen zu schulen (E1, 00:42:27-2; E4, 00:37:22-4; E5, 00:42:15-9; E6, 00:43:04-4). Experte 4 empfiehlt, dieses Risiko zu umgehen, indem analysiert wird, welche Plattform am häufigsten genutzt wird, um diese anschliessend spezifisch zu schulen (E4, 00:36:32-0). Ebenfalls nennen die Experten 2 und 7 eine weitere Chance, wenn die Durchführung der Schulung auch auf mobilen Endgeräten angeboten wird. Dadurch kann die Chance geschaffen werden, dass Mitarbeitende die Schulung jederzeit absolvieren können und derart die Durchführungsrate steigt (E2, 01:02:29-4; E7, 00:40:22-0).

Interne Meldeplattform

Interne Meldeplattformen für das Melden von Phishing-Angriffen werden in der Praxis vermehrt im Zusammenhang mit Phishing-Awareness-Trainings eingeführt. Diese Meldeplattformen bieten die Chance, echte Phishing-Angriffe zu erkennen und frühzeitig zu stoppen (Jaeger & Eckhardt, 2021, S. 450; Protasova & Mazko, 2021, S. 130; Zainab et al., 2021, S. 17; E1, 00:38:10-3; E2, 01:04:40-9; E6, 00:46:11-7; E7, 00:45:06-7). Weiter entstehen gemäss den Experten die Chancen, den Benutzenden eine benutzerfreundliche Methode für das Melden verdächtiger E-Mails zu bieten und durch die Präsenz eines Meldebuttons für die Mitarbeitenden einen stetigen Erinnerungsfaktor zu gewährleisten (E1, 00:38:10-3; E3, 00:36:09-4; E2, 01:04:40-9). Wird mit dem Meldeprozess eine Wertung der einzelnen Mitarbeitenden eingeführt, kann zudem die Chance generiert werden, Mitarbeitende spezifisch anhand ihres Erfahrungsniveaus zu schulen, um dadurch einen besseren und interessanteren Schulungseffekt zu erzielen. Hingegen kann eine Meldefunktion bei einem unzureichenden Meldeprozess auch Risiken darstellen. Die Vielzahl an E-Mails, welche durch das Phishing-Awareness-Training entstehen, und die damit verbundenen Meldungen können das Risiko eines hohen Aufwands in der IT darstellen (Althobaiti et al., 2021, S. 9–11; E1, 00:38:10-3; E2, 01:04:40-9; E4, 00:39-35-6; E6, 00:46:11-7). Aufgrund der Vielzahl an Meldungen kann zusätzlich das Risiko entstehen, dass auch echte Phishing-Angriffe übersehen werden (Althobaiti et al., 2021, S. 11; Mihelic et al., 2019, S. 1471–1472; E1, 00:38:10-3; E2, 01:04:40-9; E4, 00:39-35-6; E6, 00:46:11-7). Ein schlechter Rückmeldeprozess, wie in Kapitel 4.2.6 beschrieben, kann zusätzlich das Risiko schaffen, dass Mitarbeitende das Interesse am Melden verlieren oder bei den Mitarbeiten die Angst entsteht, falsch zu melden (E4, 00:39-35-6; E6, 00:02:52-4; E5, 00:45:26-0; E7, 00:45:06-7).

Schlussfolgerung

Auch im technischen Bereich ergeben sich Chancen und Risiken, welche generell das Phishing-Awareness-Training betreffen, und Chancen und Risiken, welche sich auf gestaltungs spezifische Aspekte beziehen. Die Arbeitsfrage AF4 «Welche technischen Aspekte ergeben sich bei der Durchführung eines Phishing-Awareness-Trainings??» kann anhand der bedeutendsten technischen Chancen, wie dem «Aufzeigen der technischen Grenzen» und «Nutzen von Kosteneffizienten Lösungen» sowie anhand der bedeutendsten technischen Risiken, «Blockierung der Trainings oder Simulations-E-Mails» sowie «Sicherheitslücken durch Freischaltungen», beantwortet werden. Allgemein kann die Arbeitsfrage AF4 anhand allen generellen technologischen Aspekten in der Tabelle 10 sowie den in Tabelle 11 aufgelisteten gestalterischen technologischen Aspekten beantwortet werden.

Tabelle 10: Generelle Technologische Chancen und Risiken

Technologisch			
Erkenntnisse	E	L	D
Chancen			
Aufzeigen der technischen Grenzen und Minimierung des falschen Vertrauens	✓	✓	×
Möglichkeit für effiziente und kostengünstige Lösung für Phishing-Awareness-Trainings bei Nutzung einer SaaS-Lösung	✓	×	×
Risiken			
Falscher Zustellung der Inhalte oder Sicherheitslücken durch Fehlkonfiguration	✓	×	×
Blockierung der Trainings oder Simulations-E-Mails oder Sicherheitslücken durch Freischaltungen	✓	✓	×
Ineffektivität bei nicht aktuellen Inhalten der Systemlösungen oder unzureichender Individualisierungsmöglichkeiten	✓	✓	×
Legende: E = Experten, L = Literatur, D = Datensatz			

Die Aspekte der Gestaltung, wie mobile Plattformen oder interne Meldeplattformen sind die in Tabelle 11 dargestellten.

Tabelle 11: Technologische Chancen und Risiken anhand der Gestaltung des Trainings

Technologisch				
Gestaltungsart	**Erkenntnisse**	E	L	D
Chancen				
Technische Abwehrmassnahmen durch Konfiguration der Systeme	Risikominimierung vor echten Angriffen bei richtiger Konfiguration	✓	×	×
Zusätzliche Warnhinweise den Mitarbeitenden Anzeigen	Zusätzlicher Schutz vor echten Phishing Angriffen	✓	✓	×
Integration unterschiedlicher Plattformen im Schulungsmaterial	Steigerung der Effektivität der Schulung, da die Mitarbeitenden auf unterschiedlicher Plattformen geschult werden	✓	✓	×
Zur Verfügung Stellen des Schulungsinhaltes auf unterschiedliche Plattformen	Steigerung der Durchführungsrate und Motivation der Mitarbeitenden, da das Training einfacher zugänglich ist	✓	×	×
Verwendung einer internen Meldeplattform	Benutzerfreundlicher Meldeprozess Gestaltung, Zusätzliche Sensibilisierung durch die Präsenz des Meldebuttons und Schulungsoptimierung durch Messungen der Meldungen	✓	×	×
Risiken				
Verwendung von fertigen Systemlösungen	Es kann das falsche Gefühl vermitteln werden, dass bei Verwendung von Systemlösungen keine Aufwendungen anfallen.	✓	✓	×
Zusätzliche Warnhinweise den Mitarbeitenden Anzeigen	Dass Mitarbeiter vor Phishing Simulationen gewarnt werden und Aufwand für die Implementierung ohne grossen zusätzlichen Nutzen	✓	✓	×
Integration unterschiedlicher Plattformen im Schulungsmaterial	Steigerung der Komplexität und des Aufwandes, durch die grosse Anzahl an möglichen Plattformen	✓	✓	×
Verwendung einer internen Meldeplattform	Überlastung des IT-Personals und Gefahr, dass echte Phishing Angriffe übersehen werden, aufgrund der vielen Meldungen während Phishing-Simulationen	✓	✓	×
Legende: E = Experten, L = Literatur, D = Datensatz				

Auch im technischen Bereich konnten nicht alle Chancen und Risiken aus den Experten:inneninterviews oder der Literatur gegenseitig bestätigt werden. Jene Erkenntnisse,

die sowohl in der Literatur als auch aus den Experten:inneninterviews identifiziert wurden, werden als relevant angesehen. Dennoch sollten Erkenntnisse, welche nur einseitig gewonnen wurden, nicht vernachlässigt werden. Es empfiehlt sich aber, diese Erkenntnisse mit Vorsicht zu betrachten.

6.1.3 Umfeld

Einbindung externer Firmen

Der Bereich «Security» wird in der Praxis immer mehr ausgelagert, entsprechend bietet es sich auch an, das Phishing-Awareness-Training mit externen Partnern durchzuführen. Das Auslagern des Security-Themas kann gemäss den Experten und der Literatur eine Chance sein, indem auf das umfangreiche Wissen dieser Anbieter zurückgegriffen werden kann (Kweon et al., 2021, S. 370; E2, 01:14:21-2; E5, 00:52:59-9; E8, 00:49:48-5). Zusätzlich kann es gemäss den Experten die Chance bringen, dem Fachkräftemangel im Security-Bereich entgegenzuwirken, wenn Arbeitsstunden ausgelagert und eingespart werden (E1, 00:27:08-3; E2, 01:14:21-2; E4, 00:43:17-5; E5 01:02:33-9). Gemäss den Experten 4 und 6 bietet die Zusammenarbeit mit externen Partnern ausserdem die Chance, auch die Reaktion der IT zu prüfen, indem sie nicht über eine laufende Phishing-Simulation informiert wird (E4, 00:43:17-5; E6, 00:51:54-6). Neben den Chancen gilt bei den Experten und in der Literatur auch die Ansicht, dass durch die Auslagerung Risiken entstehen können. Je nach Sitz des Partners können unterschiedliche rechtliche Situationen gelten (Burita et al., 2022, S. 12; Innab et al., 2018, S. 4; E1, 00:45:54-2; E2, 00:55:32-2; E7, 00:50:55-6). Zusätzlich kann das Risiko eines Daten-Leaks, bei der Zusammenarbeit mit externen Partnern, verstärkt werden, indem Daten an potenzielle Angreifende gelangen können. Dieses Risiko wird zwar sowohl von der Literatur als auch von den Experten als Gefahr angesehen, jedoch von mehreren Experten als gering eingeschätzt (Burita et al., 2022, S. 12; Higashino et al., 2019, S. 82; E1, 00:25:51-7; E2, 00:17:09-1; E7, 00:49:35-1; E4, 00:44:37-5; E5, 00:55:04-0).

Meldungen an Externe

Die Information über die Durchführung eines Phishing-Awareness-Trainings ist ein bedeutender Punkt in der Praxis. Meldungen an Externe beziehen sich mehrheitlich auf landesspezifische Gegebenheiten, weshalb in der Literatur keine Angaben gefunden wurden. Aus den Experten:inneninterviews ergaben sich jedoch für die Schweiz spezifische Chan-

cen und beziehungsweise risikomindernde Massnahmen. Das Informieren von Institutionen wie das NCSC, den Registrar, den Hoster oder weitere extern Betroffene, kann die Risiken minimieren, geblockt zu werden, rechtliche Konsequenzen zu erhalten und Aufwand bei Externen zu generieren (E1, 00:43:42-5; E2, 10:24:36-2; E3, 00:45:57-0; E4, 00:48:23-1; E5, 00:57:05-3). Ebenfalls empfehlenswert ist es, bei der Verwendung von Namen und Logos externer Parteien, diese zu informieren und um Erlaubnis zu fragen, um ebenfalls rechtliche Konsequenzen zu vermeiden (E2, 10:24:36-2).

Rechtliche Aspekte

Phishing-Awareness-Trainings können bei Nichtbeachtung rechtlicher Aspekte zu rechtlichen Konsequenzen führen. Die Forschenden und die Experten sind der Meinung, dass bei der Verwendung von Namen und Logos Markenschutz und Urheberrecht beachtet werden sollten, um rechtliche Konsequenzen zu vermeiden (Sutter et al., 2022, S. 6; Volkamer et al., 2020, S. 519–520; E2, 01:18:56-8; E3, 00:05:30-6; E4, 00:41:17-1; E6, 00:05:52-2; E7, 00:05:17-4). Rechtliche Regelungen können jedoch von Land zu Land variieren und sollten daher für das spezifische Land sowie bei der Zusammenarbeit mit externen Partnern jeweils betrachtet werden (Sutter et al., 2022, S. 6; E1, 00:03:49-1; E2, 00:25:36-5; E7, 00:50:55-6; E8, 00:52:27-5). Gemäss Artikel 11 im Markenschutzgesetz ist die Verwendung von Marken allerdings nur dann unzulässig, wenn die Marke mit gleicher oder ähnlicher Ware oder Dienstleistung verwendet wird (MSchG, 1992). Dennoch ist es empfehlenswert, Marken und Namen nur mit dem Einverständnis des Inhabers zu verwenden, da im Bedarfsfall beispielsweise auch mit Rufschädigung argumentiert werden könnte. Ebenfalls gilt es gemäss Experte 2, Regelungen immer wieder zu prüfen, da sich diese ereignisbasiert auch ändern können (E2, 01:07:47-6).

Schlussfolgerung

Die Chancen und Risiken im Umfeld sind mehrheitlich landesspezifisch. Dennoch konnten generelle Chancen und Risiken ermittelt werden, welche für das jeweilige Land betrachtet werden sollten. Die Arbeitsfrage AF3 «Welche Aspekte im Umfeld ergeben sich bei der Durchführung eines Phishing-Awareness-Trainings?» kann anhand der bedeutendsten Chancen im Umfeld, wie die «Risikominimierung vor rechtlichen Konsequenzen» und «Risikominimierung von Blockierungen durch den Provider» sowie anhand dem bedeutendsten Risiko im Umfeld «Änderungen von rechtlichen Regulierungen», beantwortet werden. Auch im Umfeld konnten relevante gestalterische Aspekte identifiziert

werden, welche für die Beantwortung der AF3 relevant sind, diese sind in in Tabelle 13 dargestellt. Allgemein kann die Arbeitsfrage AF3 anhand allen generellen Aspekten aus dem Umfeld in der Tabelle 12 sowie den in Tabelle 13 aufgelisteten Aspekten der Gestaltung aus dem Umfeld beantwortet werden.

Tabelle 12: Generelle umfeldbezogene Chancen und Risiken

Umfeld			
Erkenntnisse	E	L	D
Chancen			
Risikominimierung von Blockierungen und rechtlichen Konsequenzen, wenn externe Stellen informiert werden	✓	×	×
Risikominimierung von rechlichen Konsequenzen bei Beachtung landesspezifischer Regulierungen	✓	✓	×
Risiken			
Rechtliche Widerhandlungen zu begehen durch ändernde rechtlicher Regulierungen, oder Aufwendungen für die Aktualisierung der Inhalte	✓	×	×
Legende: E = Experten, L = Literatur, D = Datensatz			

Tabelle 13: Umfeldbezogene Chancen und Risiken anhand der Gestaltung des Trainings

Umfeld				
Gestaltungsart	**Erkenntnisse**	E	L	D
Chancen				
Zusammenarbeit mit externen Partnern als Unterstützung	Profitieren vom Wissen der externen Partner	✓	✓	×
	Entlastung der IT durch Auslagerung der Arbeitsstunden	✓	×	×
	Es kann die Reaktion des IT-Personals bei Phishing-Angriffen geprüft werden	✓	×	×
Risiken				
Zusammenarbeit mit externen Partnern als Unterstützung	Externe Partner kennen nicht zwingend die Rechtslage und Regulatoren des Ziel-Unternehmens und können dadurch unter Umständen, rechtswidrige Kampagnen anbieten	✓	✓	×
	Externe Partner können ein Ziel von Cyberkriminellen sein und dadurch das Risiko eines Daten-Leaks schaffen	✓	✓	×
Legende: E = Experten, L = Literatur, D = Datensatz				

Nicht alle Chancen und Risiken konnten sowohl von der Literatur als auch von den Experten bestätigt werden. Die Herkunft der Erkenntnis ist in Tabelle 12 und Tabelle 13 entsprechend vermerkt. Erkenntnisse, welche von der Literatur und den Experten genannt wurden, werden als relevant angesehen. Dennoch sollten bei der Implementierung eines Phishing-Awareness-Trainings auch die einseitig gewonnenen Erkenntnisse betrachtet werden. Es empfiehlt sich, diese Erkenntnisse mit Vorsicht zu betrachten.

6.1.4 Auswertung Datensatz

Die Resultate des OptiPhish-Datensatzes wurden in Kapitel 5 beschrieben. Folglich werden die Resultate aus dem Datensatz beurteilt. Abbildung 4 zeigt unterschiedliche Faktoren, die von den Umfrageteilnehmenden bewertet wurden. Es zeigt sich, dass für mehr als die Hälfte der Umfrageteilnehmenden die Anzahl an Simulationen zu hoch war. Dies bestätigt sich auch in Abbildung 7, bei der ersichtlich wird, dass die am häufigst genannten Kritikpunkte, das Intervall und die Häufigkeit der Simulationen sind. Dies bestätigt auch die Relevanz der in Kapitel 6.1.1 beschriebenen Chancen und Risiken zum Intervall. Ein weiterer Faktor, den Abbildung 4 aufzeigt, ist, dass knapp über die Hälfte das Training als hilfreich empfanden und weitere ca. 20 % das Training neutral bewerteten. Ebenfalls gaben ca. 57 % an, dass das Training die Sensibilisierung gesteigert hat. Wird bedacht, dass die Bewertung auf den eigenen Meinungen der Umfrageteilnehmenden basiert, sind diese Werte überwiegend positiv. Dies wird auch anhand der positiven individuellen Rückmeldungen bestätigt, bei denen als häufigster Grund, die Tatsache genannt wurde, dass das Training hilfreich war. Ebenfalls als positiv erweist sich die Auswertung, ob die Simulationen sowie deren Inhalte angemessen waren. Sowohl die Simulation an sich als auch ihre Inhalte wurden von mehr als 70 % als angemessen betrachtet. Umso erstaunlicher ist es, dass, obwohl der Inhalt von mehr als 70 % als angemessen empfunden wurde, der Inhalt der am zweitmeisten genannte Aspekt in den negativen individuellen Rückmeldungen war. Dies ist jedoch sowohl anhand der Rückmeldungen als auch anhand der Bewertung der Schwierigkeit in Abbildung 7 auf zu leichte Simulationen zurückzuführen. Ebenfalls wurde ausgewertet, inwiefern ein Fehlverhalten bei einer Phishing-Simulation Einfluss auf die Wahrnehmung gegenüber dem Training hatte. Wie Abbildung 6 zeigt, verhält sich die Wahrnehmung unabhängig von einem Fehlverhalten oder einem richtigen Verhalten in etwa gleich.

Schlussfolgerung

Mehr als 70 % empfanden die Simulation als angemessen. Ebenfalls empfanden mehr als 50 % das Training als hilfreich und mehr als 57 %, dass das Training die Sensibilisierung gesteigert hat. Die negativen Rückmeldungen sind dabei mehrheitlich auf ein zu kurzes Intervall oder auf zu leichte Simulationen zurückzuführen und nicht auf das eigentliche Training. Entsprechend kann die Arbeitsfrage AF1 «Wie wird ein Phishing-Awareness-Training von den Teilnehmenden aufgenommen?» damit beantwortet werden, dass das Phishing-Awareness-Training bei den Geschulten überwiegend positiv aufgenommen wird und auch eine Mehrheit von der Schulung profitieren kann. Aufgrund der Anzahl an negativen Rückmeldungen sollten aber besonders das Intervall und der Inhalt von Schulungen stärker berücksichtigt werden.

6.1.5 Schlussfolgerung

In dieser Arbeit wurde anhand des TOE-Frameworks untersucht, welche Chancen und Risiken bei der Durchführung eines Phishing-Awareness-Trainings entstehen können. Mittels Literatur und Experten:inneninterviews konnten diverse Chancen und Risiken in den TOE-Bereichen identifiziert werden. Eine Vielzahl konnte dabei sowohl von der Literatur als auch von den Experten bestätigt werden. Einzelne Chancen und Risiken konnten jedoch nur einseitig belegt werden. In der Arbeit zeigte sich auch, dass Chancen und Risiken generell oder anhand der Gestaltung des Trainings, entstehen können. Die Forschungsfrage «Welche Chancen und Risiken ergeben sich entsprechend den TOE-Blickwinkeln bei der Durchführung eines Phishing-Awareness-Trainings?» kann entsprechend den bedeutendsten Chancen, wie der «Risikominimierung gegenüber Cyberangriffen», «Sensibilisierung der Mitarbeitenden», «Aufzeigen der technischen Grenzen», «Nutzen von Kosteneffizienten Lösungen», «Risikominimierung vor rechtlichen Konsequenzen» und «Risikominimierung von Blockierungen durch den Provider» sowie den bedeutendsten Risiken, «den hohen Aufwand und Kosten», «Zeitverschwendung der Mitarbeitenden bei falscher Durchführung», «Blockierung der Trainings oder Simulations-E-Mails», «Sicherheitslücken durch Freischaltungen» und «Änderungen von rechtlichen Regulierungen», beantwortet werden. Allgemein sind für die Beantwortung der Forschungsfrage jedoch alle Chancen und Risiken der generellen Aspekten in Tabelle 14, sowie den gestalterischen Aspekte in Tabelle 9, Tabelle 11 und Tabelle 13, relevant.

Tabelle 14: Übersicht aller generellen Chancen und Risiken bei der Durchführung eines Phishing-Awareness-Trainings

TOE-Bereich	Erkenntnisse	E	L	D
	Chancen			
Organisatorisch	Risikominimierung gegenüber Cyberangriffen	✓	✓	×
	Sensibilisierung der Mitarbeitenden	✓	✓	×
	Securuity-Thema und Security-Team den Mitarbeitenden näher bringen	✓	×	✓
	Sensibilisierung der Mitarbeitenden auch im Privatleben	✓	×	✓
Technologisch	Aufzeigen der technischen Grenzen und Minimierung des falschen Vertrauens	✓	✓	×
	Möglichkeit für effiziente und kostengünstige Lösung für Phishing-Awareness-Trainings bei Nutzung einer SaaS-Lösung	✓	×	×
Umfeld	Risikominimierung von Blockierungen und rechtlichen Konsequenzen, wenn externe Stellen informiert werden	✓	×	×
	Risikominimierung von rechlichen Konsequenzen bei der Beachtung von landesspezifischer Regulierungen	✓	✓	×
	Risiken			
Organisatorisch	Hohe Aufwendungen und Kosten	✓	✓	×
	Zeitverschwendung der Mitarbeitenden bei falscher Durchführung	✓	✓	×
	Verärgerung der Mitarbeitenden	✓	✓	×
Technologisch	Falscher Zustellung der Inhalte oder Sicherheitslücken durch Fehlkonfiguration	✓	×	×
	Blockierung der Trainings oder Simulations-E-Mails oder Sicherheitslücken durch Freischaltungen	✓	✓	×
	Ineffektivität bei nicht aktuellen Inhalten der Systemlösungen oder unzureichender Individualisierungsmöglichkeiten	✓	✓	×
Umfeld	Rechtliche Widerhandlungen zu begehen durch ändernde rechtlicher Regulierungen, oder Aufwendungen für die Aktualisierung der Inhalte	✓	×	×
	Legende: E = Experten, L = Literatur, D = Datensatz			

Ebenfalls wurde anhand des OptiPhish-Datensatzes untersucht, wie ein Phishing-Awareness-Training von Mitarbeitenden aufgenommen wird. Die Resultate zeigten, dass ein Phishing-Awareness-Training von der Mehrheit akzeptiert und als hilfreich befunden wird.

Die Arbeit liefert einen Überblick über mögliche Chancen und Risiken bei der Durchführung eines Phishing-Awareness-Trainings. Mit der Arbeit wird zudem die bestehende Literatur ergänzt, die sich mehrheitlich mit der Effektivität sowie bestimmten Methoden

und Tools befasst, indem diese Arbeit die Durchführung von Phishing-Awareness-Trainings aus der organisatorischen Sicht betrachtet. Es sollte jedoch beachtet werden, dass zum einen nicht alle Chancen und Risiken mehrfach belegt werden. Zum anderen wurden sowohl bei den Experten:inneninterviews als auch beim OptiPhish-Datensatz subjektive Meinungen befragt, was zu Diskrepanzen in der Implikation führen kann. Spezifische Limitationen werden in Kapitel 6.3 genauer ausgeführt. Dennoch zeigt sich, dass die Vielzahl an Chancen und Risiken unterschiedliche Auswirkungen haben können und auch dass dies nicht immer gelten müssen. So wurde beispielsweise festgestellt, dass die Forschenden und die Experten nicht immer einer Meinung sind oder sogar gegensätzliche Meinungen besitzen. Daher sollte die Gestaltung und Durchführung von Phishing-Awareness-Trainings, sorgfältig geplant werden und die Auswirkungen anhand der Chancen und Risiken für das eigene Unternehmen abgewägt werden. Generell zeigt sich aber ein Phishing-Awareness-Training als eine effektive Methode, um sich vor Cyberangriffen zu schützen, und sollte daher in den Unternehmen auch durchgeführt werden. Wichtig ist dabei die kontinuierliche Durchführung, damit das Training sich als effektiv erweist.

6.2 Handlungsempfehlung

Phishing-Angriffe haben immer mehr zugenommen und die Tendenz zeigt aktuell keine Abflachung dieses Trends. Ebenfalls sind immer noch die meisten Cybersicherheitsvorfälle auf ein falsches Verhalten bei einem Phishing-Angriff zurückzuführen. Deswegen ist es empfehlenswert, dass sich Unternehmen mithilfe von Phishing-Awareness-Trainings schützen. Ebenfalls sollte ein Phishing-Awareness-Training kontinuierlich durchgeführt werden, damit ein konstanter Schutz gewährleistet werden kann. Phishing-Awareness-Trainings liefern dabei diverse Chancen, aber auch Risiken, welche in dieser Arbeit aufgezeigt wurden. Für die Praxis wird daher empfohlen, dass die in Tabelle 14 dargestellten Chancen und Risiken bei der Implementierung berücksichtigt werden. Ebenfalls wird angeraten, die in Tabelle 9, Tabelle 11 und Tabelle 13 dargestellten Gestaltungsspezifischen Chancen und Risiken, bei der Verwendung dieses gestalterischen Aspekts, zu berücksichtigen. Die ermittelten Chancen und Risiken können dabei helfen, Phishing-Awareness-Trainings möglichst optimal zu nutzen. Es wird aber auch empfohlen, die Chancen und Risiken individuell zu beurteilen, da sich diese industriespezifisch oder länderspezifisch ändern können.

6.3 Limitationen

Die Ergebnisse dieser Bachelorarbeit ergeben sich aus der Literaturrecherche, den Experten:inneninterviews und der Auswertung des OptiPhish-Datensatzes. Es gilt zu beachten, dass in jedem Bereich Limitationen bestehen und die Repräsentativität kritisch betrachtet werden muss. In diesem Kapitel werden die Limitationen genauer beschrieben.

6.3.1 Limitation der Literaturrecherche

Bei der Literaturrecherche wurde versucht, mittels einer systematischen Literaturrecherche ein möglichst breites Spektrum abzudecken. Dennoch kann es aufgrund der begrenzten Anzahl an Abfragen und der gewählten Einschränkungen zu Lücken in der relevanten Literatur kommen. Ebenfalls basiert die systematische Literaturrecherche auf der Bewertung der Titel und der Abstracts. Dieses Vorgehen bewirkt eine gewisse Subjektivität bei der Bewertung der Relevanz. Diese Subjektivität kann ebenfalls zu Lücken in der relevanten Literatur führen. Dennoch wurde mittels der systematischen Literaturrecherche ein breites Spektrum abgedeckt und sie sollte einen Grossteil der relevanten Literatur beinhalten.

6.3.2 Limitation der Experten:inneninterviews

Bei den Experten:inneninterviews wurde eine kleine Gruppe an Experten interviewt. Diese Tatsache weist eine Limitation im Bereich der Repräsentativität auf. Hinzu kommt, dass mehr als die Hälfte der Experten aus der ZHAW stammen und sich dadurch die Erkenntnisse aus den Experten:inneninterviews überwiegend auf die Erfahrungen innerhalb der ZHAW stützen. Die Limitation der Repräsentativität wird hingegen durch den Vergleich mit der aktuellen Literatur relativiert.

6.3.3 Limitation Datensatzanalyse

Der verwendete Datensatz stammt aus dem OptiPhish-Projekt. Daher zeigt sich auch beim Datensatz eine Limitation im Bereich der Repräsentativität, da sich alle Rückmeldungen auf das OptiPhish-Projekt stützen. Zusätzlich handelt es sich beim Datensatz um anonymisierte Daten, die eine Plausibilitätsprüfung erschwerten. Die Daten aus dem Datensatz stammen ausserdem aus den subjektiven Meinungen der Umfrageteilnehmer und wurde nicht systematisch gemessen oder geprüft. Bei der Untersuchung des Datensatzes war es das Ziel, die Wahrnehmung der Teilnehmenden zu identifizieren. Demzufolge ist

in der Auswertung des Datensatzes auch eine Subjektivität gewünscht und dies relativiert die Limitation im Bereich der Repräsentativität.

6.4 Weiterführende Forschung

In der Arbeit zeigten sich verschiedene Chancen und Risiken, welche sich entweder ausschliesslich anhand der Literatur oder ausschliesslich anhand der Experten identifizieren liessen. Für die Forschung bietet es sich an, diese einseitig belegten Chancen und Risiken weiter zu untersuchen. Erkenntnisse, welche sich nur in der Literatur zeigten, könnten auf deren Relevanz in der Praxis geprüft werden und mittels Studie belegt werden. Für jene Erkenntnisse, welche sich ausschliesslich aus den Experten:inneninterviews ergaben, empfiehlt es sich, diese durch spezifische Literaturrecherchen zu analysieren oder ebenfalls mittels Studie zu belegen. Die Auswertung, wie Phishing-Awareness-Trainings bei Mitarbeitenden angenommen werden, wurde in dieser Arbeit anhand eines Datensatzes durchgeführt. Aufgrund der Tatsache, dass dieser Datensatz sich auf eine spezifische Studie beschränkt, wäre auch hier die Verifizierung anhand anderer Datensätze sinnvoll. Zuletzt wurde in der Arbeit festgestellt, dass weder in der Literatur noch in der Praxis die rechtliche Lange von Phishing-Awareness-Trainings klar zu sein scheint. Daher wäre eine genaue Untersuchung der Rechtslage ein wertvoller Beitrag für die Literatur und Praxis.

7 Literaturverzeichnis

Abroshan, H., Devos, J., Poels, G. & Laermans, E. (2021a). COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic. *IEEE Access*, *9*, 121916–121929. https://doi.org/10.1109/ACCESS.2021.3109091

Abroshan, H., Devos, J., Poels, G. & Laermans, E. (2021b). Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access*, *9*, 44928–44949. https://doi.org/10.1109/ACCESS.2021.3066383

Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, *12*(10), 168. https://doi.org/10.3390/fi12100168

Alhashmi, A. A., Darem, A [Abdulbasit] & Abawajy, J. (2021). Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats.

Alseadoon, I. M., Othman, M. F. I., Foo, E. & Chan, T. (2013). *Typology of phishing email victims based on their behavioural response*. https://scholar.archive.org/work/56ip2es4sjbitmpxisriroeloi/access/wayback/https://aisel.aisnet.org/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1084&context=amcis2013

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Alshaikh, M., Maynard, S. & Ahmad, A. (2019). TOWARD SUSTAINABLE BEHAVIOUR CHANGE: AN APPROACH FOR CYBER SECURITY EDUCATION TRAINING AND AWARENESS. In.

Alshaikh, M., Maynard, S. B. & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & Security*, *100*, 102090. https://doi.org/10.1016/j.cose.2020.102090

Alshaikh, M., Maynard, S. B., Ahmad, A. & Chang, S. (2018). *An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations*. https://scholarspace.manoa.hawaii.edu/items/a97d1684-992b-4697-a72e-a659d8206a40

Althobaiti, K., Jenkins, A. D. G. & Vaniea, K. (2021). A Case Study of Phishing Incident Response in an Educational Organization. *Proc. ACM Hum.-Comput. Interact.*, *5*(CSCW2). https://doi.org/10.1145/3476079

Alwanain, M. I. (2019). An Evaluation of User Awareness for the Detection of Phishing Emails. *International Journal of Advanced Computer Science and Applications*, *10*(10). https://doi.org/10.14569/IJACSA.2019.0101046

Anawar, S., Kunasegaran, D. L., Mas'ud, M. Z. & Zakaria, N. A. (2019). Analysis of phishing susceptibility in a workplace: a big-five personality perspectives. *J Eng Sci Technol*, *14*(5), 2865–2882.

APWG. (2022). *PHISHING ACTIVITY TRENDS REPORT 3rd Quarter 2022*. https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf?_ga=2.134803189.580041249.1675526412-1263615438.1675526412&_gl=1*1jw6m0d*_ga*MTI2MzYxNTQzOC4xNjc1NTI2NDEy*_ga_55RF0RHXSR*MTY3NTUyNjQxMi4xLjEuMTY3NTUyNjQyNS4wLjAuMA.

Bardsley-Marcial, B. (2022). COMMON FACTORS IN SUSCEPTIBILITY TO PHISHING. *International Journal of Information, Business and Management*, *14*(4), 97–104. https://www.proquest.com/scholarly-journals/common-factors-susceptibility-phishing/docview/2717341204/se-2?accountid=143299

Bayl-Smith, P., Taib, R., Yu, K. & Wiggins, M. (2022). Response to a phishing attack: persuasion and protection motivation in an organizational context. *Information & Computer Security*, *30*(1), 63–78. https://doi.org/10.1108/ICS-02-2021-0021

Bona, M. de & Paci, F. (2020). A real world study on employees' susceptibility to phishing attacks. In M. Volkamer & C. Wressnegger (Hrsg.), *ACM Digital Library, ARES 2020: 15th International Conference on Availability, Reliability and Security : August 25-August 28, 2020, all-digital conference* (S. 1–10). The

Association for Computing Machinery. https://doi.org/10.1145/3407023.3409179

Bora, K., Do-Yeon, L. & Beomsoo, K. (2020). Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks. *Behaviour & Information Technology*, *39*(11), 1156–1175. https://doi.org/10.1080/0144929X.2019.1653992

Markenschutzgesetz, Art. 11 (1992).

Burita, L., Klaban, I. & Racil, T. (2022). Education and Training Against Threat of Phishing Emails. *International Conference on Cyber Warfare and Security*, *17*(1), 7–18. https://doi.org/10.34190/iccws.17.1.28

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M. & Calic, D. (2020). When believing in technology leads to poor cyber security: Development of a trust in technical controls scale. *Computers & Security*, *98*, 102020. https://doi.org/10.1016/j.cose.2020.102020

Chen, R., Gaia, J. & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, *133*, 113287. https://doi.org/10.1016/j.dss.2020.113287

Corradini, I. & Nardelli, E. (2019). Building Organizational Risk Culture in Cyber Security: The Role of Human Factors. In T. Z. Ahram & D. Nicholson (Hrsg.), *Advances in Human Factors in Cybersecurity* (S. 193–202). Springer International Publishing.

Darem, A [A.] (2021). Anti-Phishing Awareness Delivery Methods. *Engineering, Technology & Applied Science Research*, *11*(6), 7944–7949. https://doi.org/10.48084/etasr.4600

DBIR. (2020). *Data Breach Investigations Report 2020.* DBIR. https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf

Desolda, G., Di Nocera, F., Ferro, L., Lanzilotti, R., Maggi, P. & Marrella, A. (2019). Alerting Users About Phishing Attacks. In A. Moallem (Hrsg.), *HCI for Cybersecurity, Privacy and Trust* (S. 134–148). Springer International Publishing.

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T. & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys*, *54*(8), 1–35. https://doi.org/10.1145/3469886

Dixon, M., Nicholson, J., Branley-Bell, D., Briggs, P. & Coventry, L. (2022). Holding Your Hand on the Danger Button: Observing User Phish Detection Strategies Across Mobile and Desktop. *Proc. ACM Hum.-Comput. Interact.*, *6*(MHCI). https://doi.org/10.1145/3546730

Döring, N. (2023). *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften* (6., vollst. überarb., akt. u. erw. Auflage 2023). Springer Berlin; Springer.

Dresing, T. & Pehl, T. (2020). Transkription. In G. Mey & K. Mruck (Hrsg.), *Handbuch Qualitative Forschung in der Psychologie* (S. 835–854). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-26887-9_56#ESM

Ebner, T. (2018). 3 Steps to Better Cybersecurity. *Associations Now*, *14*(3), 44–47. https://www.proquest.com/trade-journals/3-steps-better-cybersecurity/docview/2266294739/se-2?accountid=143299

Federal Bureau of Investigations Public Service Announcements. (Apr. 2020). *Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion*. https://www.ic3.gov/Media/Y2020/PSA200406

Frank, M., Jaeger, L. & Ranft, L. M. (2022). Contextual drivers of employees' phishing susceptibility: Insights from a field study. *Decision Support Systems*, *160*, 113818. https://doi.org/10.1016/j.dss.2022.113818

Higashino, M., Kawato, T., Ohmori, M. & Kawamura, T. (2019). An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Information Leakage. In *2019 5th International Conference on Information Management (ICIM)*.

Huang, K. & Pearlson, K. (2019). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. In T. Bui (Hrsg.), *Proceedings of the Annual Hawaii International Conference on System Sciences, Proceedings of the*

52nd Hawaii International Conference on System Sciences. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2019.769

Hurt, J. (2018). 5 strategies to avoid phishing attacks in today's medical practices. *Ophthalmology Times*, *43*(8), 48. https://www.proquest.com/trade-journals/5-strategies-avoid-phishing-attacks-todays/docview/2056026183/se-2?accountid=143299

Innab, N., Al-Rashoud, H., Al-Mahawes, R. & Al-Shehri, W. (2018). Evaluation of the Effective Anti-Phishing Awareness and Training in Governmental and Private Organizations in Riyadh. In *2018 21st Saudi Computer Society National Computer Conference (NCC)*.

Jaeger, L. & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, *31*(3), 429–472. https://doi.org/10.1111/isj.12317

Jampen, D., Gür, G., Sutter, T. & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences*, *10*(1). https://doi.org/10.1186/s13673-020-00237-7

Jensen, M. L., Dinger, M., Wright, R. T. & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems*, *34*(2), 597–626. https://doi.org/10.1080/07421222.2017.1334499

Kävrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., Roos, R. & Furnell, S. (2022). Evaluation of Contextual and Game-Based Training for Phishing Detection. *Future Internet*, *14*(4), 104. https://doi.org/10.3390/fi14040104

Kearney, W. D. & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, *61*, 46–58. https://doi.org/10.1016/j.cose.2016.05.006

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A. & Pham, T. (2009). School of Phish: A Real-World Evaluation of Anti-Phishing Training. In *SOUPS '09, Proceedings of the 5th Symposium on Usable Privacy*

and Security. Association for Computing Machinery. https://doi.org/10.1145/1572532.1572536

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F. & Hong, J. (2007). Getting users to pay attention to anti-phishing education. In L. F. Cranor (Hrsg.), *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (S. 70–81). ACM. https://doi.org/10.1145/1299015.1299022

Kweon, E., Lee, H., Chai, S. & Yoo, K. (2021). The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. *Information Systems Frontiers*, *23*(2), 361–373. https://doi.org/10.1007/s10796-019-09977-z

Lambat, Y., Ayres, N., Maglaras, L. & Ferrag, M. A. (2021). A Mamdani Type Fuzzy Inference System to Calculate Employee Susceptibility to Phishing Attacks. *Applied Sciences*, *11*(19), 9083. https://doi.org/10.3390/app11199083

Leidner, D. E. & Kayworth, T. (2006). Review: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict. *MIS Quarterly*, *30*(2), 357. https://doi.org/10.2307/25148735

Mayring, P. & Fenzl, T. (2019). Qualitative Inhaltsanalyse. In N. Baur & J. Blasius (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung* (S. 633–648). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-21308-4_42

Merz, T. R., Fallon, C. & Scalco, A. (2019). A Context-Centred Research Approach to Phishing and Operational Technology in Industrial Control Systems. *Journal of Information Warfare*, *18*(4), 24–36. https://www.jstor.org/stable/26894692

Mihelic, A., Jevscek, M., Vrhovec, S. & Bernik, I. (2019). Testing the Human Backdoor: Organizational Response to a Phishing Campaign. *JOURNAL OF UNIVERSAL COMPUTER SCIENCE*, *25*(11), 1458–1477.

Mims, C. (2016). How to Improve Cybersecurity? Just Eliminate the Human Factor. *Wall Street Journal (Online)*. https://www.proquest.com/newspapers/how-improve-cybersecurity-just-eliminate-human/docview/1757688729/se-2?accountid=143299

Miranda, M. J. A. (2018). Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach. *International Management Review*, *14*(2), 5-10,56. https://www.proquest.com/scholarly-journals/enhancing-cybersecurity-awareness-training/docview/2127156399/se-2?accountid=143299

Nijland, J. G. W. (2022). *Gamification of cyber security awareness training for phishing against university students*. http://essay.utwente.nl/89424/

NIST. *phishing: Definition(s):*. https://csrc.nist.gov/glossary/term/phishing

Petrič, G. & Roer, K. (2022). The impact of formal and informal organizational norms on susceptibility to phishing: Combining survey and field experiment data. *Telematics and Informatics*, *67*, 101766. https://doi.org/10.1016/j.tele.2021.101766

Proctor, R. W. & Chen, J. (2015). The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. *Human factors*, *57*(5), 721–727.

Protasova, D. & Mazko, E. (2021). How to protect your organization against phishing attacks?

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., Landesberger, T. von & Volkamer, M. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (S. 259–284). USENIX Association. https://www.usenix.org/conference/soups2020/presentation/reinheimer

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M. & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. *DIGITAL HEALTH*, *8*, 20552076221081716. https://doi.org/10.1177/20552076221081716

Roepke, R., Koehler, K., Drury, V., Schroeder, U., Wolf, M. R. & Meyer, U. (2020). A Pond Full of Phishing Games - Analysis of Learning Games for Anti-Phishing Education. In G. Hatzivasilis & S. Ioannidis (Hrsg.), *Model-driven Simulation and Training Environments for Cybersecurity* (S. 41–60). Springer International Publishing.

Röpke, R., Schroeder, U., Drury, V. & Meyer, U. (2020). Towards Personalized Game-Based Learning in Anti-Phishing Education. In *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)*.

Rosser, H., Mayor, M., Stemmler, A., Ahuja, V., Grover, A. & Hale, M. (2022). Phish Finders: Crowd-powered RE for anti-phishing training tools. In *2022 IEEE 30th International Requirements Engineering Conference Workshops (REW)*.

Shahbaznezhad, H., Kolini, F. & Rashidirad, M. (2021). Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter? *Journal of Computer Information Systems*, *61*(6), 539–550. https://doi.org/10.1080/08874417.2020.1812134

Singh, K., Aggarwal, P., Rajivan, P. & Gonzalez, C. (2023). Cognitive elements of learning and discriminability in anti-phishing training. *Computers & Security*, *127*, 103105. https://doi.org/10.1016/j.cose.2023.103105

SoSafe (2023). CybercrimeTrends 2023: Aktuelle Bedrohungen und wie Sie IhreOrganisation schützen. https://lp.sosafe.de/hubfs/SoSafe%20-%20Cybercrime_Trends_23%20-%20DE.pdf?__hstc=106398849.43fc957fb69ce72ef9c26f9b42b86a85.1680434542524.1680434542524.1680434542524.1&__hssc=106398849.1.1680434542524&__hsfp=419906696

Steves, M., Greene, K. & Theofanos, M. (2020). Categorizing human phishing difficulty: a Phish Scale. *Journal of Cybersecurity*, *6*(1), tyaa009. https://doi.org/10.1093/cybsec/tyaa009

Sutter, T., Bozkir, A. S., Gehring, B. & Berlich, P. (2022). Avoiding the Hook: Influential Factors of Phishing Awareness Training on Click-Rates and a Data-Driven Approach to Predict Email Difficulty Perception. *IEEE Access*, *10*, 100540–100565. https://doi.org/10.1109/ACCESS.2022.3207272

Talley, K. (2018). Many employees know little about cybersecurity threats. *FierceCEO*. https://www.proquest.com/trade-journals/many-employees-know-little-about-cybersecurity/docview/2017017804/se-2?accountid=143299

Tornatzky, L. G., Fleischer, M. & Chakrabarti, A. K. (1990). *The processes of technological innovation*. *Issues in organization and management series*. Lexington.

Volkamer, M., Renaud, K., Reinheimer, B., Rack, P., Ghiglieri, M., Mayer, P., Kunz, A. & Gerber, N. (2018). Developing and Evaluating a Five Minute Phishing Awareness Video. In S. Furnell, H. Mouratidis & G. Pernul (Hrsg.), *Trust, Privacy and Security in Digital Business* (S. 119–134). Springer International Publishing.

Volkamer, M., Sasse, M. A. & Boehm, F. (2020). Phishing-Kampagnen zur Steigerung der Mitarbeiter-Awareness. *Datenschutz und Datensicherheit - DuD*, *44*(8), 518–521. https://doi.org/10.1007/s11623-020-1317-x

Wash, R. & Cooper, M. M. (2018). Who Provides Phishing Training? Facts, Stories, and People Like Me. In *CHI '18, Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (S. 1–12). Association for Computing Machinery. https://doi.org/10.1145/3173574.3174066

Wash, R. & Nthala, N. (Hrsg.) (2021). *Knowledge and capabilities that non-expert users bring to phishing detection.*

Webster, J. & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii. http://www.jstor.org/stable/4132319

Wilkinson, L. (2022). 4 tips to protect IT employees from phishing attacks. *Construction Dive*. https://www.proquest.com/trade-journals/4-tips-protect-employees-phishing-attacks/docview/2728795622/se-2?accountid=143299

William, Y., He, H., Wang-Sheng, L., Fadi, A. J. & Rachel, M. (2022). Simulated Phishing Attack and Embedded Training Campaign. *Journal of Computer Information Systems*, *62*(4), 802–821. https://doi.org/10.1080/08874417.2021.1919941

Yang, W., Xiong, A., Chen, J., Proctor, R. W. & Li, N. (2017). Use of Phishing Training to Improve Security Warning Compliance: Evidence from a Field Experi-

ment. In *HoTSoS, Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp* (S. 52–61). Association for Computing Machinery. https://doi.org/10.1145/3055305.3055310

Younis, Y. A. & Musbah, M. (2020). A Framework to Protect Against Phishing Attacks. In *ICEMIS'20, Proceedings of the 6th International Conference on Engineering & MIS 2020.* Association for Computing Machinery. https://doi.org/10.1145/3410352.3410825

Zainab, A., Chaminda, H., Liqaa, N. & Imtiaz, K. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

Anhang

A Übersicht der Abfragen in der Literaturrecherche

Abfrage Nr	Abfragedatum	Datenbank	Query	Jahr	Literatur Art
1	18.03.2023	Proquest	title(phishing) AND ((title(organizational) OR title(organization) OR title(organisation) OR title(organisations)) AND (summary(campaign) OR summary(education) OR summary(training)))	2018-2023	Fachmagazine, Wissenschaftliche Zeitschriften
	18.03.2023	Web of Sience	(TI=(phishing) AND (TI=(organization) OR TI=(organizations) OR TI=(organizational)OR TI=(organisation) OR TI=(organisations)) AND (AB=(campaign)OR AB=(education) OR AB=(training)))	2018-2023	-
	18.03.2023	ACM Digital Libary	[Title: phishing] AND ([Title: organizational] OR [Title: organization] OR [Title: organisation] OR [Title: organisations]) AND ([Abstract: campaign] OR [Abstract: education] OR [Abstract: training]) AND [E-Publication Date: (01/01/2018 TO 03/31/2023)]	2018-2023	-
	18.03.2023	scholar	allintitle: phishing organizational OR organization OR organisation OR organisations	2018-2023	
2	18.03.2023	Proquest	title(phishing) AND title(awareness)	2018-2023	Fachmagazine, Wissenschaftliche Zeitschriften
	18.03.2023	Web of Sience	(TI=(phishing) AND TI=(awareness))	2018-2023	-
	18.03.2023	ACM Digital Libary	[Title: phishing] AND [Title: awareness]	2018-2023	-
	18.03.2023	scholar	allintitle: Phishing awareness	2018-2023	-
3	18.03.2023	Proquest	title(phishing) AND title(TOE)	2018-2023	Fachmagazine, Wissenschaftliche Zeitschriften
	18.03.2023	Web of Sience	(TI=(phishing) AND TI=(TOE))	2018-2023	-
	18.03.2023	ACM Digital Libary	[Title: phishing] AND [Title: TOE] AND [E-Publication Date: (01/01/2018 TO 03/31/2023)]	2018-2023	-
	18.03.2023	scholar	allintitle: Phishing TOE	2018-2023	

4	18.03.2023	Proqu-est	title(phishing) AND summary(TOE)	-	-
	18.03.2023	Web of Sience	(TI=(phishing) AND AB=(TOE))	-	-
	18.03.2023	ACM Digital Libary	[Title: phishing] AND [Abstract: TOE] AND [E-Publication Date: (01/01/2018 TO 03/31/2023)]	-	-
	18.03.2023	scholar	Abfrage nicht sinnvoll	-	-
5	19.03.2023	Proqu-est	title(phishing) AND ((title(organizational) OR title(organization) OR title(organisa-tion) OR title(organisations)) AND (sum-mary(chance) OR summary(risk)))	2018-2023	Fachmagazine, Wissenschaftli-che Zeitschrif-ten
	19.03.2023	Web of Sience	(TI=(phishing) AND (TI=(organization) OR TI=(organizations) OR TI=(organiza-tional)OR TI=(organisation) OR TI=(or-ganisations)) AND (AB=(chance)OR AB=(risk)))	2018-2023	-
	19.03.2023	ACM Digital Libary	[Title: phishing] AND ([Title: organiza-tional] OR [Title: organization] OR [Title: organisation] OR [Title: organisations]) AND ([Abstract: chance] OR [Abstract: risk]) AND [E-Publication Date: (01/01/2018 TO 03/31/2023)]	2018-2023	-
	19.03.2023	scholar	Abfrage bei 1 Durchgeführt	-	-
6	19.03.2023	Proqu-est	title(phishing) AND (summary(human) OR summary(user) OR summary(users) OR summary(participant) AND (sum-mary(behaviors) OR summary(behavior) OR summary(behaviours) summary(atti-tudes) summary(attitude) OR sum-mary(factors) OR summary(factor)))	2018-2023	Fachmagazine, Wissenschaftli-che Zeitschrif-ten
	19.03.2023	Web of Sience	(TI=(phishing) AND (AB=(human) OR AB=(user) OR AB=(users) OR AB=(partici-pant) AND (AB=(behaviors)OR AB=(be-havior) OR AB=(behaviours) OR AB=(atti-tudes) OR AB=(attitude) OR AB=(factors) OR AB=(factor))))	2018-2023	-
	19.03.2023	ACM Digital Libary	[Title: phishing] AND ([Abstract: human] OR [Abstract: user] OR [Abstract: users] OR [Abstract: participant] AND ([Ab-stract: behaviors] OR [Abstract: behav-ior] OR [Abstract: behaviours] OR [Ab-stract: attitudes] OR [Abstract: attitude] OR [Abstract: factors] OR [Abstract: fac-tor])) AND [E-Publication Date: (01/01/2018 TO 03/31/2023)]	2018-2023	-
	19.03.2023	scholar	Abfrage nicht sinnvoll	2018-2023	
7	19.03.2023	Proqu-est	(title(cybersecurity) OR title(cyber secu-rity) OR title(informationsecurity) OR ti-tle(information security)) AND sum-mary(phishing)	2018-2023	Fachmagazine, Wissenschaftli-che Zeitschrif-ten

	19.03.2023	Web of Sience	((TI=(cybersecurity) OR TI=(cyber security) OR TI=(informationsecurity) OR TI=(information security)) AND AB=(phishing))	2018-2023	-
	19.03.2023	ACM Digital Libary	([Title: cybersecurity] OR [Title: cyber security] OR [Title: informationsecurity] OR [Title: information security]) AND [Abstract: phishing] AND [E-Publication Date: (01/01/2018 TO 03/31/2023)]	2018-2023	-
	19.03.2023	scholar	Abfrage nicht sinnvoll	2018-2023	
8	19.03.2023	Proquest	title(phishing) AND (summary(organizational) OR summary(organization) OR summary(organisation) OR summary(organisations))	2018-2023	Fachmagazine, Wissenschaftliche Zeitschriften
	19.03.2023	Web of Sience	(TI=(phishing) AND (AB=(organization) OR AB=(organizations) OR AB=(organizational) OR AB=(organisation) OR AB=(organisations)))	2018-2023	-
	19.03.2023	ACM Digital Libary	[Title: phishing] AND ([Abstract: organizational] OR [Abstract: organization] OR [Abstract: organisation] OR [Abstract: organisations]) AND [E-Publication Date: (01/01/2018 TO 03/31/2023)]	2018-2023	-
	19.03.2023	scholar	Abfrage nicht sinnvoll	2018-2023	
9	19.03.2023	Proquest	title(anti-phishing) AND (summary(campaign) OR summary(education) OR summary(training))	2018-2023	Fachmagazine, Wissenschaftliche Zeitschriften
	19.03.2023	Web of Sience	(TI=(anti-phishing) AND (AB=(campaign) OR AB=(education) OR AB=(training)))	2018-2023	-
	19.03.2023	ACM Digital Libary	[Title: anti-phishing] AND ([Abstract: campaign] OR [Abstract: education] OR [Abstract: training]) AND [E-Publication Date: (01/01/2018 TO 03/31/2023)]	2018-2023	-
	19.03.2023	scholar	allintitle: anti-phishing training OR education OR campagne	2018-2023	
10	19.03.2023	Proquest	(title(cybersecurity) OR title(cyber security) OR title(informationsecurity) OR title(information security)) AND (title(organizational) OR title(organization) OR title(organisation) OR title(organisations))	2018-2023	Fachmagazine, Wissenschaftliche Zeitschriften
	19.03.2023	Web of Sience	((TI=(cybersecurity) OR TI=(cyber security) OR TI=(informationsecurity) OR TI=(information security)) AND (TI=(organizations) OR TI=(organizational)OR TI=(organisation) OR TI=(organisations)))	2018-2023	-

	19.03.2023	ACM Digital Libary	([Title: cybersecurity] OR [Title: cyber security] OR [Title: informationsecurity] OR [Title: information security]) AND ([Title: organizational] OR [Title: organization] OR [Title: organisation] OR [Title: organisations]) AND [E-Publication Date: (01/01/2018 TO 03/31/2023)]	2018-2023	-
	19.03.2023	scholar	Abfrage nicht sinnvoll	-	-

B Literatur Übersicht mit Kategorien

TOE-Bereich	Finding bereiche		Untersuchung der Quelle	Quelle
	Überkategorie	Subkategorie		
Organisational	Verhalten und Eigenschaften der Geschulten	Eigenschaften der Geschulten	Untersucht die Emotionale Einflussfaktoren für die Anfälligkeit von Phishing während COVID-19	(Abroshan et al., 2021a)
			Untersucht die Risikobereitschaft und den Entscheidungsfindungsstil von Personen gegenüber Phishing	(Abroshan et al., 2021b)
			Untersucht unterschiedliche Schulungsmethoden und deren Fähigkeiten	(Alseadoon et al., 2013)
			Untersucht das Phishing-Bewusstsein	(Alwanain, 2019)
			Untersucht Einflussfaktoren anhand Persönlichkeitseigenschaften gegenüber Phishing	(Anawar et al., 2019)
			Untersucht Einflussfaktoren für Anfälligkeit von Phishing	(Bardsley-Marcial, 2022)
			Untersucht Wirksamkeit von Phishing Simulationen	(Bora et al., 2020)
			Untersucht 3 Schritte zu einer bessere Cybersecurity Strategie	(Ebner, 2018)
			Untersucht verschiedene Anti-Phishing Schulungsprogramme und kategorisiert diese	(Jampen et al., 2020)
			Untersucht die Erstellung eines HICV ausgerichteter Risikobewertungsrahmen	(Merz et al., 2019)
			Untersucht Mögliche Phishing Abwehrmassnahmen für IT-Personal	(Wilkinson, 2022)
		Verhalten der Geschulten	Untersucht die Risikobereitschaft und den Entscheidungsfindungsstil von Personen gegenüber Phishing	(Abroshan et al., 2021b)
			Untersucht die wahrgenommene Anfälligkeit bei Phishing angriffen	(Chen et al., 2020)
			Untersucht den Einfluss von Kontextfaktoren auf die Anfälligkeit von Phishing	(Frank et al., 2022)
			Untersucht die Implementierung von Phishing Awareness Trainings in Krankenhäusern	(Hurt, 2018)
			Untersucht den langfristigen Trainingseffekt sowie demografische Einflussfaktoren	(Kumaraguru et al., 2009)
			Untersucht die Erstellung eines HICV ausgerichteter Risikobewertungsrahmen	(Merz et al., 2019)
			Untersucht unterschiedliche Anti Phishing Lernspiele	(Roepke et al., 2020)
			Untersucht den Wahrnehmungsunterschiede in Bezug auf Informationssicherheit	(Kearney & Kruger, 2016)
			Untersucht Mögliche Phishing Abwehrmassnahmen für IT-Personal	(Wilkinson, 2022)
		Schulungs-methoden	Untersucht Typen, Vektoren sowie Technische Ansätze von Phishing angriffen	(Alabdan, 2020)

	Art und Aufbau einer Schulung		Untersucht verschieden Schulungsmethoden für Phishing Awareness Training	(Alhashmi et al., 2021)
			Unteruscht die Aufmerkasamkeit von Geschulten bei Unterschiedlichen Schulungsmethoden	(Kumaraguru et al., 2007)
			Untersucht die Anfälligkeit gegenüber Phishing anhand situationsbasierter Variablen	(Jaeger & Eckhardt, 2021)
			Untersucht verschiedene Anti-Phishing Schulungsprogramme und kategorisiert diese	(Jampen et al., 2020)
			Untersucht die Wirksamkeit von Bestrafungen und Belohnung bei Phishing Awareness Trainings	(William et al., 2022)
		Schulungs - medium	Untersucht verschieden Schulungsmethoden für Phishing Awareness Training	(Alhashmi et al., 2021)
			Untersucht Effektivität von Schulungs-methoden	(Darem, 2021)
			Untersucht einen Trainingsansatz auf Basis der Achtsamkeitstheorie	(Jensen et al., 2017)
			Untersucht unterschiedliche Anti Phishing Lernspiele	(Roepke et al., 2020)
			Untersucht die Effektivität eines kurzen Videos als Phishing Awareness Training	(Volkamer et al., 2018)
			Untersucht Effektivität der Vermittlung unterschiedlicher Schulungsmaterial	(Wash & Cooper, 2018)
		Schulungs-bestimmungen	Untersucht Probleme bei der Implementierung von ISTA	(Alshaikh et al., 2018)
			Untersucht das Phishing-Bewusstsein	(Alwanain, 2019)
			Untersucht Einflussfaktoren anhand Persönlichkeitseigenschaften gegenüber Phishing	(Anawar et al., 2019)
			Untersucht 3 Schritte zu einer bessere Cybersecurity Strategie	(Ebner, 2018)
			Untersucht Kontext bezogene Einflussfaktoren für die Anfälligkeit gegenüber Phishing	(Bona & Paci, 2020)
			Untersucht Wirksamkeit von Phishing Simulationen	(Bora et al., 2020)
			Untersucht verschiedene Anti-Phishing Schulungsprogramme und kategorisiert diese	(Jampen et al., 2020)
			Untersucht den langfristigen Trainingseffekt sowie demografische Einflussfaktoren	(Kumaraguru et al., 2009)
			Untersucht die Implementierung eines Cybersicherheits Trainings	(Miranda, 2018)
			Untersucht Einflussfaktoren anhand Variablen für die Anfälligkeit von Phishing	(Singh et al., 2023)
			Untersucht aus verschiedenem Blickwinkel die Durchführung einer Anti Phishing Kampagne	(Volkamer et al., 2020)
			Untersucht die Wirksamkeit von Bestrafungen und Belohnung bei Phishing Awareness Trainings	(William et al., 2022)
		Aktualität der Trainings-inhalte	Untersucht die aktuellen Arten von Phishing und mögliche Abwehrmassnahmen	(Zainab et al., 2021)
			Untersucht ein Crowd Sourcing Modell zur Aktualisierung von Trainingsinhalten	(Rosser et al., 2022)

		Personali-sierung des Trainings	Untersucht einen Interventionsprozess zur Verhaltensänderung gegenüber SETA	(Alshaikh et al., 2019)
			Untersucht die Erstellung eines Prozesses zur Entwicklung von SETA-Programmen	(Alshaikh et al., 2021)
			Untersucht Probleme bei der Implementierung von ISTA	(Alshaikh et al., 2018)
			Untersucht die Risikobereitschaft und den Entscheidungsfindungsstil von Personen gegenüber Phishing	(Abroshan et al., 2021b)
			Untersucht die Anfälligkeit gegenüber Phishing anhand situationsbasierter Variablen	(Jaeger & Eckhardt, 2021)
			Untersucht verschiedene Anti-Phishing Schulungsprogramme und kategorisiert diese	(Jampen et al., 2020)
			Untersucht die Implementierung eines Phishing Awareness Training im Krankenhaus	(Rizzoni et al., 2022)
			Untersucht Personalisierungsmöglichkeiten in Spielbasierte Anti-Phishing-Tools	(Röpke et al., 2020)
			Untersucht System zur Bewertung des Schwierigkeitsgrades von Phishing Schulungen	(Steves et al., 2020)
			Untersucht die Wirksamkeit von Bestrafungen und Belohnung bei Phishing Awareness Trainings	(William et al., 2022)
			Untersucht die Entwicklung eines Frameworks für Benutzer Schulung in Arabischer Sprache	(Younis & Musbah, 2020)
		Intervall der Trainings-einheiten	Untersucht die Effektivität eines Phishing Awareness Training Programm	(Reinheimer et al., 2020)
			Untersucht Abwehrmassnahmen von Phishing-Angriffen anhand menschliche Faktoren	(Desolda et al., 2022)
			Untersucht verschiedene Anti-Phishing Schulungsprogramme und kategorisiert diese	(Jampen et al., 2020)
			Untersucht die Implementierung eines Phishing Awareness Training im Krankenhaus	(Rizzoni et al., 2022)
			Untersucht die Effektivität eines kurzen Videos als Phishing Awareness Training	(Volkamer et al., 2018)
	Kultur, Normen und Policies		Untersucht fünf Schlüsselinitiativen für die Verbesserung einer Cybersicherheitskulturen	(Alshaikh, 2020)
			Untersucht die Entwicklung einer Cybersicherheitskultur	(Corradini & Nardelli, 2019)
			Untersucht ein Modell für Faktoren, Entstehung und Messung von Cybersecurity-kultur in Unternehmen	(Huang & Pearlson, 2019)
			Untersucht die Implementierung einer Cybersicherheitskultur in Unternehmen	(Leidner & Kayworth, 2006)
			Untersucht die Faktoren für die Anfälligkeit auf Phishing	(Petrič & Roer, 2022)
			Untersucht die Erstellung eines Modells zur Schaffung von Cybersicherheitskultur	(Shahbaznezhad et al., 2021)
	Ethik		Untersucht den Einsatz eines Spiel basierten Phishing Trainings bei Studenten	(Nijland, 2022)
			Untersucht die Erstellung eines Modells zur Klassifizierung der wahrnehmung von Phishing Simulationen	(Sutter et al., 2022)

	Interne Rechtfertigung	Untersucht ein System zur Bewertung des Schwierigkeitsgrades von Schulungen	(Steves et al., 2020)
Technologie	Mögliche Systemlösungen	Untersucht die Evaluation eines eigenen Phishing Training Plattform	(Burita et al., 2022)
		Untersucht ein Phishing Awareness System, dass keine Sensitiven Daten speichert	(Higashino et al., 2019)
		Untersucht die Effektivität eines kurzen Videos als Phishing Awareness Training	(Volkamer et al., 2020)
	Vertrauen der Geschulten in die Technik	Untersucht das Vertrauen der Mitarbeiter in den technischen Schutz der Organisation	(Butavicius et al., 2020)
		Untersucht verschiedene Anti-Phishing Schulungsprogramme und kategorisiert diese	(Jampen et al., 2020)
	Warnhinweise als ergänzung	Untersucht die Gestaltung von Warnhinweisen	(Desolda et al., 2019)
		Untersucht verschiedene Anti-Phishing Schulungsprogramme und kategorisiert diese	(Jampen et al., 2020)
		Untersucht Die Effektivität von Spielbasiert und GBMT Lenkmechanismen	(Kävrestad et al., 2022)
		Untersucht die Effektivität von Warnhinweisen	(Yang et al., 2017)
	Einfluss unterschiedlicher Plattformen auf die Schulung	Untersucht die Interaktion mit Phishing E-Mails auf Desktop und Mobile	(Dixon et al., 2022)
		Untersucht die Implementierung eines Phishing Awareness Training im Krankenhaus	(Rizzoni et al., 2022)
	Meldeplattform als Ergänzung zur Schulung	Untersucht die aktuellen Arten von Phishing und mögliche Abwehrmassnahmen	(Zainab et al., 2021)
		Untersucht fünf Schlüsselinitiativen für die Verbesserung einer Cybersicherheitskulturen	(Alshaikh, 2020)
		Untersucht wie Mitarbeiter Phishing meldet und der Helpdesk damit umgeht	(Althobaiti et al., 2021)
		Untersucht Auswirkungen von Cyber-bedrohungen bei einem Phishing-Angriff	(Bayl-Smith et al., 2022)
		Untersucht die Anfälligkeit gegenüber Phishing anhand situationsbasierter Variablen	(Jaeger & Eckhardt, 2021)
		Untersucht verschiedene Anti-Phishing Schulungsprogramme und kategorisiert diese	(Jampen et al., 2020)
		Untersucht welche User mittels Phishing angegriffen werden und die Reaktion der IT	(Mihelic et al., 2019)
		Untersucht die Implementierung eines Cybersicherheits Trainings	(Miranda, 2018)
		Untersucht Tipps zum Schutz gegen Phishing	(Protasova & Mazko, 2021)
		Untersucht aus verschiedenem Blickwinkel die Durchführung einer Anti Phishing Kampagne	(Volkamer et al., 2020)
	Technische Abwehrmassnahmen	Untersucht die Risikobereitschaft und den Entscheidungsfindungsstil von Personen gegenüber Phishing	(Abroshan et al., 2021b)
		Untersucht Typen, Vektoren sowie Technische Ansätze von Phishing angriffen	(Alabdan, 2020)
		Untersucht wie Mitarbeiter Phishing meldet und der Helpdesk damit umgeht	(Althobaiti et al., 2021)
		Untersucht den langfristigen Trainingseffekt sowie demografische Einflussfaktoren	(Kumaraguru et al., 2009)

		Untersucht aus verschiedenem Blickwinkel die Durchführung einer Anti Phishing Kampagne	(Volkamer et al., 2020)
Umwelt	Zusammenarbeit mit Externen Unternehmen	Untersucht die Evaluation eines eigenen Phishing Training Plattform	(Burita et al., 2022)
		Untersucht ein Phishing Awareness System, dass keine Sensitiven Daten speichert	(Higashino et al., 2019)
		Untersucht Effektivität von Phishing Awaren-ess für Regierungseinrichtungen	(Innab et al., 2018)
		Untersucht die Wirksamkeit von Sicherheits-schulungen	(Kweon et al., 2021)
	Rechtliche Grundlagen	Untersucht aus verschiedenem Blickwinkel die Durchführung einer Anti Phishing Kampagne	(Volkamer et al., 2020)
		Untersucht die Erstellung eines Modells zur Klassifizierung der wahrnehmung von Phishing Simulationen	(Sutter et al., 2022)

C Interviewleitfaden

Ersteller:in	Severin Zimmermann
Version	4

Fragekategorie	
Allgemein	
Organisatorisch	
Technisch	
Umfeld	

Administratives	
Interview Datum	
Interview-Partner	
Arbeitgeber	
Aufnahme OK?	
Anonymisierung Daten?	

Nr.	Kategorie				Frage
Administratives [2-3 Min]					
					Vorstellung, Interviewer und Thema der Bachelorarbeit
					Hinweis: Wie angekündigt wird das Interview für die Auswertung aufzeichnen, Zugriff auf die Aufzeichnung haben mein Betreuer Tim Geppert und ich.
1					Darf in der Arbeit ihr Name und Funktion erwähnt werden?
					Alternativ: dürfen in der Arbeit Ihre Aussagen anonymisiert verwendet werden?
Hinweis: Aufzeichnung wird gestartet					
2					Darf ich Sie bitten kurz Ihre Position und Funktion zu nennen?
					Ergänzend: Wie lange arbeiten Sie schon in dieser Position/Funktion und in dieser Firma?
3					Hatten Sie bereits Erfahrungen mit Phishing?
4					Hatten Sie auch bereits Erfahrungen mit Phishing Awareness Training?
Hauptfragen [20 Min]					
5a					Was sind aus ihrer Sicht positive Aspekte, die im Rahmen eines Phishing Awareness Trainings resultieren können?
5b					Was sind aus ihrer Sicht negative Aspekte, die im Rahmen eines Phishing Awareness Trainings resultieren können oder die beachatet werden sollten?

					Hinweis: Abhängig von der Antwort folgen ergänzende Fragen:
5.1					Sind Ihnen weitere Aspekte bekannt, welche aus Organisatorischer sich tbeachtet werden sollten?
5.2					Sind Ihnen weitere Aspekte bekannt, welche aus Technischer sich tbeachtet werden sollten?
5.3					Sind Ihnen weitere Aspekte bekannt, welche aus Umfeld sich tbeachtet werden sollten?
6					Bleiben andere Aspekte aus Ihrer sich noch offen?
					Detailfragen [35 Min]
					Hinweis: Abhängig von den Antworten wird bei den Detailfragen nur nich nach ergänzugen gefragt
7					Sollte Ihrer Meinung nach die Durchführung von Phishing Awareness Trainings auf die Geschulten (Demografisch, verhalten, emotionale Lage, Risikobereitschaft etc.) abgestimmt/personalisiert werden?
					Ergänzend: Welche Chancen und Risiken sehen Sie bei der Personalisierung des Phishing Awareness Trainings?
					Ergänzend: Welche Chancen und Risiken sehen Sie bei einer nicht personalisierten Durchführung des Phishing Awareness Trainings?
8					Der Aufbau eines Phishing Awareness Trainings kann unterschiedlich gestaltet werden Bsp. Art (embedded, präventiv etc.), Inhaltsgestaltung (Game, Video, Fakten etc.), Zustellungsmethode (Klassenraum, Online, Flyer etc.), Informationsfluss (Mitarbeiter Informieren Ja/Nein). Welche Risiken und Chancen sehen Sie beim Aufbau beziehungsweise bei der Gestaltung des Trainings?
					Ergänzend: Sollte das IT-Personal informiert werden?
9					Spielt Ihrer Meinung nach die Cybersicherheitskultur eines Unternehmen eine grössere Rolle wie das Phishing Awareness Trainings?
					Ergänzend: Welche Chancen und Risiken sehen Sie in Bezug auf die Pflege einer Cybersicherheitskultur gegenüber einem Phishing Awareness Training?
					Alternativ: Sollten Ihrer Meinung die Schaffung einer Cybersicherheitskultur prioritär im Phishing Awareness Training gefördert werden?
10					Welche ethischen Aspekte müssen aus Ihrer Sicht bei der Durchführung eines Phishing Awareness Trainings beachtet werden?
11					Wie stehen Sie gegenüber Klickraten bei simulierten Phishings?
					Ergänzend: Sehen Sie Probleme bei der Rechtfertigung gegenüber höheren Instanzen bei einer geringen Klickrate?
12					Bei simulierten Phishings werden oft technische Vorkehrungen getroffen (SPAM filter, Absender Whitelisting etc.) sehen Sie dabei Risiken oder Chancen?

					Ergänzend: Erachten Sie solche Massnahmen als hilfreich beziehungsweise den Nutzen höher als potenzielle Gefahren?
13					Schaffen technische Sicherheitsmassnahmen Ihrer Meinung nach ein falsches Vertrauen bei den Mitarbeitern, was zu einer höheren Anfälligkeit führt?
14					Reichen Ihrer Meinung nach Schulungen für die Sensibilisierung der Mitarbeiter aus? Oder sollen ergänzend technische Warnhinweise angezeigt werden?
					Ergänzend: Sehen Sie Chancen und Risiken bei Warnhinweisen?
15					Sollten unterschiedliche Plattformen (Mobile, Desktop, Tablet etc.) bei der Durchführung eines Phishing Awareness Trainings berücksichtigt werden?
					Ergänzend: Sehen Sie Chancen und Risiken bei der Berücksichtigung unterschiedlicher Plattformen?
16					Welche Chancen und Risiken sehen Sie bei der Implementierung einer internen Meldeplattform?
					Hinweis: Erklärung Bsp. Button im Outlook
17					Sind Ihnen Externe Einflüsse bekannt, welche bei der Durchführung eines Phishing Awareness Trainings beachtet werden sollten?
17					Wie stehen Sie gegenüber externen Partnern bei der Implementierung eines Phishing Awareness Trainings?
					Ergänzend: Wie sehen Sie das mit ausländischen Partnern und Plattformen?
					Ergänzend: Denken Sie, es besteht ein erhöhtes Risiko gegenüber Phishing Angriffen bei Datenleaks des externen Anbieters?
17					Gibt es aus Ihrer Sicht rechtliche Aspekte bei der Durchführung eines Phishing Awareness Trainings zu beachten?
17					Sind Ihnen externe Parteien bekannt (Regierungsinstitutionen, Hoster, Regiestar etc.), die zwingend über die Durchführung eines Phishing Awareness Training informiert werden sollten?
					Ergänzend: Weshalb müssen aus Ihrer Sicht diese externen Parteien informiert werden?
17					Sind Ihnen Externe Meldepflichten bekannt?
Administratives [2 Min]					
18					Gibt es ihrer Sicht noch Punkte, die wir nicht oder nicht ausreichend behandelt haben und die wir jetzt noch ergänzen sollten?
19					Ich werde noch weitere Interviews durchführen, welche ggf. neue Aspekte liefern bei dem Ihre meinung ebenfalls intressant wäre, dürfte ich Sie in diesem Fall nochmals kontaktieren?
Hinweis: Aufzeichnung wird beendet					

					Hinweis: Gerne werde ich Ihnen die Arbeit nach Abschluss zur Verfügung stellen
					Bedankung
					Verabschiedung

D Transkript Experten-Interview Experte 1

Administratives	
Interview Datum	19.04.2023
Interview-Partner	Experte 1
Arbeitgeber	ZHAW
Aufnahme OK?	Ja
Anonymisierung Daten?	Nein

Severin Zimmermann: Sehr gut, schnell die Sprache des Transkripts ändern. #00:00:18-7#

Severin Zimmermann: Sehr gut, dann würde ich gerade mit der ersten Frage starten und zwar dürfte ich dich bitten deine Position und Funktion zu nennen? #00:00:27-5#

Experte 1: Ja, Ich bin wissenschaftlicher Mitarbeiter an der Zürcher Hochschule für Angewandte Wissenschaften und ich arbeite im Information Security Team als Researcher. #00:00:40-7#

Severin Zimmermann: Sehr gut, und wie lange arbeitest du schon im Information Security Team? #00:00:47-7#

Experte 1: Ich bin jetzt fünf Jahre hier im Team und zwei Jahre als wissenschaftlicher Mitarbeiter #00:00:54-1#

Severin Zimmermann: Sehr gut, dann hast du bereits Erfahrungen mit Phishing Angriffen? Wurdest du vielleicht selber einmal Opfer oder einer deiner Kollegen? #00:01:02-2#

Experte 1: Ja, natürlich im Information Security Bereich haben wir sehr viel /, Oder sind Sehr viel damit konfrontiert wir haben natürlich auch Erfahrungen damit

Wir haben diverse Leute, die auch schon gephished wurden und wir bearbeiten auch Fälle von Opfern, die gephished wurden Und natürlich über die Studie, die wir gemacht haben, haben wir sehr viel Know-how im Bereich Phishing #00:01:25-5#

Severin Zimmermann: Sehr gut, du sprichst die Studie an, da ging es ja um das OptiFish Projekt, wo ihr ein Phishing Awareness Training durchgeführt habt Hast du in dem Fall auch bereits Erfahrungen mit Phishing Awareness Training, ist das richtig? #00:01:40-6#

Experte 1: Ja, einfach durch die Studie habe ich natürlich bereits Erfahrungen mit Phishing Awareness wie du weißt, haben wir ja eine Studie dazu durchgeführt aber auf anderer Ebene habe ich bis jetzt auch noch nie Phishing Awareness gemacht Also rein wissenschaftlich wie sagt für ein wissenschaftliches Projekt. #00:01:57-9#

Severin Zimmermann: Okay, sehr gut, aber du konntest ja sicher Erfahrungen mit dem Thema Phishing Awareness erarbeiten. #00:02:04-2#

Experte 1: Ja, definitiv #00:02:06-0#

Severin Zimmermann: Sehr gut, dann sind dir positive Aspekte bekannt, die im Rahmen eines Phishing Awareness Trainings auftauchen können? #00:02:15-5#

Experte 1: Ja natürlich, sonst würden wir kein Training machen. Es ist natürlich klar, dass ein Phishing Awareness Training das Ziel hat, die Leute zu sensibilisieren. Das heißt, dass wir als Ziel immer haben sollten, dass wir Leute eigentlich schulen, richtig auf solche Phishing E-Mails zu reagieren und Phishing E-Mails auch zu erkennen und ich denke, Phishing Awareness Training kann da wirklich auch gewissen Leuten auch helfen, diese Sensibilisierung zu entwickeln. #00:02:44-0#

Severin Zimmermann: Sehr gut, sind dir aber auch negative Aspekte bekannt, die bei der Durchführung eines Phishing Awareness Trainings resultieren können? #00:02:54-5#

Experte 1: Ja klar, es gibt natürlich diverse Faktoren, die da mit reinspielen. Ich sage immer, Phishing Awareness ist nicht für jedermann geeignet Es gibt Leute,

die extrem positiv mit Phishing Awareness lernen können. Aber es gibt natürlich auch viele Leute, die das als Zeitverschwendung ansehen oder die dieses Training gar nicht benötigen aber trotzdem manchmal mit diesem Training konfrontiert werden durch ihre Firma oder eben wie jetzt bei uns durch eine Bildungsinstitution. Und für diese Leute ist es dann insofern negativ, dass sie sich ein bisschen vor den Kopf gestoßen fühlen Oder dass sie eben das Phishing Training als Zeitverschwendung ansehen, oftmals. #00:03:36-2#

Severin Zimmermann: Okay, also sehe ich das richtig, hauptsächlich die, ich sage jetzt mal in Anführungszeichen, Belästigung der Mitarbeiter und Zeitverschwendung, die als Risiko resultieren können? #00:03:49-1#

Experte 1: Das ist sicher einer der Aspekte, es gibt natürlich noch viele andere, auch organisatorische Aspekte Also man darf natürlich nicht unterschätzen den Aufwand, den so eine Phishing Kampagne generiert, was man auch negativ natürlich werten kann. Oder halte eben auch, dass solche Phishing Kampagnen je nach Land speziphishe Regulierungen haben, die dann relativ schwierig umzusetzen sind teilweise. Was auch einen negativen Effekt auf die Firma oder den Ruf der Firma haben kann, wenn das falsch ausgeführt wird. #00:04:20-3#

Severin Zimmermann: Sehr gut, du hast jetzt organisatorische und mit den rechtlichen Aspekten Umfeldaspekte genannt, sind dir auch Aspekte aus der technischen Sicht bekannt, die beachtet werden sollten? #00:04:35-4#

Experte 1: Ja, ist natürlich grad wenn man so eine Phishing Kampagne aufsetzt, muss man diese natürlich auch vorgängig testen. Also man sollte immer auch schauen, dass man sein System, das man dann verwendet testen /. Vorgängig testet und was natürlich wichtig ist, es gibt natürlich sehr viele verschiedene Produkte, die Phishing Awareness anbieten Aber nicht jedes Produkt ist gleich ausgereift oder hat die gleiche Funktionalität und daher ist es natürlich wichtig, auf technischer Seite ein Produkt zu haben, bei dem man sich auch wohlfühlt und mit dem man umgehen kann. Weil ein falsch konfiguriertes Produkt kann natürlich dann im schlimmsten Fall dazu führen, dass man E-Mails an Personen versendet, die diese E-Mails dann vielleicht nicht erhalten sollten. Oder dass die E-Mails gar nicht bei den End-Usern oder den geschulten oder zu schulenden Personen ankommen. Also man kann natürlich auch auf der technischen Ebene relativ viel falsch machen. #00:05:29-2#

Severin Zimmermann: Ok, sehr gut. Du sprichst jetzt bereits Themen an, auf die wir später noch detailliert eingehen werden. Für ein /. Oder Für den groben Überblick ist das sicher mal gut so aber trotzdem noch kurze Frage, sind dir jetzt als Überblick noch Aspekte bekannt, die ich jetzt noch nicht angesprochen habe? Oder du? #00:05:50-7#

Experte 1: Also du meinst mehr aus technischer Sicht, oder wie? #00:05:55-6#

Severin Zimmermann: Technisch, organisatorisch oder Umfeld, da kannst jetzt du entscheiden. Wir kommen sicher noch bei den Detailfragen intensiv auf diese Bereiche zu. #00:06:07-9#

Experte 1: Also was aus technischer Sicht sicherlich auch oftmals schief gehen kann, ist natürlich wenn man Statistiken erhebt. Also wenn man eigentlich versucht herauszufinden, wie gut das Training funktioniert. Da gibt es natürlich unterschiedliche Ansätze bei den Produkten, wie sie diese Zahlen erheben und wir haben zumindest festgestellt, dass es hier auch ein großes Fehlerpotenzial vorhanden ist, Das heißt, dass wenn man diese Tools nicht wirklich überprüft oder testet, wie schon angesprochen Dann kann es natürlich sein, dass man auch falsche Zahlen erhebt also das ist noch ein wichtiger Punkt, den man sich auf der technischen Seite zumindest immer auch vor Augen haben sollte, dass man auch Fehler machen kann bei der Datenerhebung oder. #00:06:50-6#

Severin Zimmermann: Sehr gut, also ich sehe das auch als technische, aber auch als organisatorische /. Oder als einen organisatorischen Aspekt, wenn dann vor allem auch diese Zahlen dann verwendet werden, um etwas zu argumentieren und diese gar nicht begründet sind oder mit dem richtigen Kontext hinterlegt. Dann würden wir zu den Detailfragen kommen. Sollte deiner Meinung nach das Phishing Awareness Training auf Personen, Personengruppen abgestimmt bzw. personalisiert werden? #00:07:30-0#

Experte 1: Grundsätzlich wäre es natürlich insofern wünschenswert, als dass diese Leute wahrscheinlich dann durch diese sogenannten SpearPhishing-E-Mails besser geschult werden könnten. Das Problem ist aber meistens, dass es technisch und organisatorisch nicht so einfach durchführbar ist. Also im kleinen Rahmen geht das relativ gut, vielleicht wenn man die Personen kennt aber wenn man dann eine große Firma hat, ist es sehr unwahrscheinlich, dass diese E-Mails personalisiert werden können einfach aufgrund dadurch, dass die Person, die diese Trainings durchführt, diese zu lernende Person gar nicht kennt. Und In diesem Umfeld ist es sehr schwierig, eine personalisierte Training anzubieten oder eine persönliche Training durchzuführen. Wäre aber natürlich insofern wünschenswert, als dass die Leute sicherlich davon profitieren könnten. #00:08:18-5#

Severin Zimmermann: Sehr gut, du sprichst jetzt die Personalisierung auf einzelne Benutzer an Ich habe jetzt in meinen Interviews, die ich schon gehabt habe,

vermehrt vernommen, dass es sinnvoll istn jedoch auf Funktions- bzw. Bereichsebene wie ist deine Meinung hierzu, wenn ich das auf z.B. die HR oder Finanzabteilung abstimme? #00:08:40-0#

Experte 1: Ja also, es macht sicherlich Sinn, weil man weiss heutzutage aus der Phishing-Studien, dass man, wenn man gezielt Content versendet der auch relevant für den alltäglichen Beruf einer Person ist oder für die allgemeinen Prozesse, die diese Person oftmals benutzt, dass diese dann tendenziell eher auf diese Phishing-E-Mails darauf einfallen. Das kann man natürlich gezielt auch für Phishing-Trainings einsetzen, für Phishing Awareness und das macht insofern auch Sinn, dass man das dann wirklich personalisiert. Man kann dazu auch einfache Beispiele geben, wenn man z.B. ein E-Mail schickt mit einem Dienst, wie z.B. Facebook an eine Geschäftsperson, die z.B. im HR arbeitet und Facebook im Geschäft gar nicht verwendet, dann ist es sehr unwahrscheinlich, dass diese Person diese E-Mail anklickt. Das heisst, das Alignment zwischen Content und der Person ist natürlich sehr wichtig und ich würde hier klar empfehlen, dass man in einer Phishing-E-Mails-Kampagne immer auf die Zielgruppe abstimmen sollte. #00:09:45-4#

Severin Zimmermann: Sehr gut, danke. Siehst du auch Risiken, die mit der Abstimmung auf Zielgruppen entstehen können? #00:09:52-6#

Experte 1: Ja, es ist natürlich klar, wenn man auf gewisse Zielgruppen E-Mails erstellt und diese dann sendet, dann kann es natürlich sein, dass das auch ethisch ein bisschen ein Problem ist Insofern, dass man vielleicht ein Thema aufgreift, das dann für diese Usergruppe wie sagt man /. Als unzulässiges Training angesehen wird. Das heisst, dass das Thema vielleicht nicht angemessen ist Ich kann dir z.B. ein Beispiel geben, es gab einmal ein Phishing-Awareness-Fall, bei dem hat man am Ende des Jahres, im Dezember, ein Bonus-E-Mail versendet Also man hat verschiedenen Mitarbeitern ein E-Mail gesendet, bei dem angepriesen wurde, sie kriegen einen Bonus auf das Ende des Jahres, aber Sie müssen sich für diesen Bonus registrieren. Das ist dan natürlich insofern für diese Leute ein schönes Erlebnis, wenn sie einen Bonus kriegen am Ende des Jahres, weil sie viel gearbeitet haben aber es kann natürlich auch dazu führen, dass die Leute, wenn sie dann diesen Bonus nicht kriegen, sich an den Kopf gestoßen fühlen oder. Oder dass das dann ethisch ein bisschen verwerflich ist oder viele Leute das dann als Beleidigung auffassen. Das ist das gleiche, wenn man gezielt E-Mails an gewisse Trainingsgruppen sendet, kann es natürlich immer vorkommen, dass diese das dann als beleidigend auffassen könnten. Man muss hier sehr gezielt oder sehr vorsichtig vorgehen #00:11:19-7#

Severin Zimmermann: Sehr gut, auf ethische Aspekte kommen wir sicher nachher auch noch zu sprechen. Jetzt aber erst einmal, Phishing-Awareness-Trainings können sehr unterschiedlich aufgebaut sein. Ihr habt soviel ich weiß in eurer Studie ein Embedded-Training verwendet, also sprich Phishing-Simulationen

und nur wenn die User geklickt haben, wurden sie oder wurde ihnen das Schulungsmaterial zugesendet. Es gibt aber sehr viele Möglichkeiten, dies zu gestalten, auch in der Variante, ob ich es als Game, Video oder mit einem Factsheet präsentiere, wo ich es mache, also sprich in einem Klassenraum, online, da gibt es ganz viele Möglichkeiten. Auch ein Aspekt ist, ob ich die Mitarbeiter informiere. Es gehört alles so in den Bereich Aufbau eines Phishing-Trainings. Wie siehst du den Aufbau eines Trainings, bzw. je nachdem, wie man den gestaltet, siehst du da Risiken oder Chancen, die ich als bestimmten Varianten erhalten kann oder nicht? #00:12:31-4#

Experte 1: Ja, es gibt natürlich Vor- und Nachteile von jeder Art Trainingsmethodik, die man hier anwendet. Ich sage, als Chancen hat man natürlich immer, wenn man diese vielen Variantenmöglichkeiten hat, das zu organisieren, kann man natürlich das Training an die Zielgruppe anpassen. Also wenn man natürlich eine Mitarbeiterschulung macht und sagt, man hat vielleicht nur einen Slot von ein paar Stunden, dann macht das vielleicht auch Sinn, dass man frontal mit den Leuten darüber redet, dass man vielleicht im Raum eines Klassen oder eines Seminars das besprechen kann. Aber es gibt natürlich auch Chancen, wenn man das in einem größeren Rahmen macht, dass man sagt, man stellt den Leuten ein Training zu fügen, die das zum Beispiel machen wollen. Also ich sehe hier, wie die Chancen sind, dass man die Zielgruppe möglichst gut abfangen kann, indem man verschiedene Arten von Trainings anbietet. Bei Risiken ist es natürlich so, wenn man seine Zielgruppe nicht gut kennt oder wenn es eine sehr große Zielgruppe ist, ist es natürlich schwierig zu entscheiden, welche Art von Training wählt man eigentlich. Und das ist das größte Diskurs natürlich, dass die gewählte Art des Trainings überhaupt nicht /. Also keinen Anklang bei der Userschaft findet, dass die Leute, die hier getrainiert werden, das überhaupt nicht mögen oder vielleicht auch nicht damit lernen können, weil das einfach nicht die Art von Methodik ist, die sie gewöhnt sind. #00:13:55-6#

Severin Zimmermann: Sehr gut. Ich habe es vorhin kurz angesprochen, dass Mitarbeiter informieren, das ist auch so ein Aspekt. Besonders aber auch, ob das IT-Personal über eine Phishing, also in bezug auf Phishing Simulation, über eine Phishing-Kampagne informiert werden soll. Wie siehst du das? #00:14:16-9#

Experte 1: Es kommt natürlich darauf an, was man testen will. Ich sage jetzt natürlich, wenn man so eine Studie wie wir uns macht, dann ist es unerlässlich, dann muss man zwingendermaßen die IT informieren. Wenn man jetzt aber natürlich testen will, ob die IT selbst richtig auf solche Phishing-Attacken reagiert, in so einem Fall macht es natürlich, dass man die IT nicht darüber informiert oder dass man dann einfach sagt, man prüft, ob die internen Prozesse korrekt sind oder korrekt funktionieren und die Leute in der IT auch richtig auf eine solche Attacke reagieren können. In so einem Fall macht das eventuell Sinn, aber auch da ist es natürlich immer mit Vorsicht zu genießen, man will ja nicht die Leute vor den Kopf stoßen. Im Endeffekt, um dann eigentlich gemeinsam mit diesen Leuten

einen besseren Sicherheitsstandard oder eine bessere Sicherheitskultur zu pflegen, sage ich mal #00:15:07-1#

Severin Zimmermann: Sehr gut, hast das ist jetzt schon ein bisschen angesprochen und zwar ist es unerlässlich, dass die IT informiert wird, wenn man das in großem Stil durchführt. Siehst den du Risiken, wenn ich das eben dann doch nicht mache? #00:15:25-0#

Experte 1: Der größte Risiko ist natürlich, dass die IT das eskaliert und dass es also echt einen Angriff ansieht und das kann natürlich auch dann außerhalb der Firma oder des Unternehmens kommuniziert werden. Also im Fall eines richtigen Angriffes kann es natürlich dann auch je nach Inhalt dieser Phishing Mails dazu führen, dass diese an nationale Stellen gemeldet werden oder sogar an strafrechtliche Stellen. Es ist meistens bei Phishing weniger der Fall, aber es könnte natürlich im schlimmsten Fall eskalieren, dass es auch rechtliche Folgen hat natürlich. #00:16:01-2#

Severin Zimmermann: Sehr gut, dann zur nächsten Frage und zwar geht es hier um die Cybersicherheitskultur. In der Literatur wird immer wieder beschrieben, dass die Cybersicherheitskultur ein wichtiger Aspekt ist, um Phishing-Angriffe abzuwehren oder auch mit zu pflegen, also die Phishing Awareness mit Cybersicherheitskultur zu pflegen und allenfalls sogar als wichtiger als das Training selbst. Wie siehst du das? Spielt Cybersicherheitskultur eine wichtige Rolle im Zusammenhang mit Phishing-Awareness-Training oder sollte das unabhängig betrachtet werden? #00:16:44-4#

Experte 1: Also meiner Meinung nach ist Phishing-Awareness ein Teil der Cybersicherheitskultur oder der Sicherheitskultur allgemein in den Unternehmen. Es ist natürlich klar /. Es ist natürlich sehr unternehmensspeziphish nicht /. Phishing-Awareness ist nicht für jedes Unternehmen geeignet. Ich meine, in vielen Unternehmen braucht es das vielleicht gar nicht, weil sie nicht in erster Linie über E-Mails kommunizieren oder macht das nicht viel Sinn, weil die Leute vielleicht einen hohen Level bereits an Phishing-Awareness haben. In solchem Rahmen macht es dann nicht Sinn, das als große Rolle zu betrachten. Es ist natürlich ein anderes Thema bei großen Firmen, bei sehr großen Firmen. Bei denen ist es für mich schon ein bisschen ein Muss, dass die Phishing-Awareness oder die allgemeine Schulung gegen Phishing einen festen Bestandteil ihrer Sicherheitskultur ansehen. #00:17:39-9#

Severin Zimmermann: Sehr gut. Siehst du auch Risiken, wenn ich das als festen Bestandteil meiner Sicherheitskultur anschaue? #00:17:49-6#

Experte 1: Das größte Risiko, wie ich schon angesprochen habe, man generiert relativ viel Aufwand mit Phishing-Awareness. Gerade wenn man das in einer großen Firma macht, dann müssen da wirklich viele Personalressourcen eingesetzt werden. Das Risiko ist, wie auch gesagt, wenn man das Phishing Training falsch macht, dann kann das relativ schnell auch Konsequenzen haben, interne wie auch externe Konsequenzen. #00:18:19-1#

Severin Zimmermann: Du sprichst jetzt aber auch wieder die allgemeinen oder generellen Risiken, wenn ich Phishing-Awareness dafür in Bezug auf Cybersicherheitskultur, siehst du hier ein Risiko, wenn ich wirklich den Fokus auf die Cybersicherheitskultur lege und diesen mit Phishing-Awareness trainieren will? Oder ist das für dich dann das gleiche Risiko? #00:18:43-7#

Experte 1: Das ist für mich grundsätzlich das gleiche Risiko, da sehe ich jetzt keinen Unterschied. #00:18:49-2#

Severin Zimmermann: Okay, dann passt das so. Jetzt kommen wir zu den ethischen Aspekten. Hier hast du es vorhin bereits angesprochen mit das /. Wenn man es nicht richtig macht oder je nachdem, was für eine Art von Phishing man macht, dass sich dann die Leute betrogen fühlen oder an den Kopf gestoßen. Sind dir weitere Aspekte bekannt, die im Rahmen der ethischen Durchführung eines Phishing-Awareness-Trainings beachtet werden sollten? #00:19:23-7#

Experte 1: Grundsätzlich kann man sagen, dass Phishing-Awareness klar eine Grauzone im ethischen Bereich ist, weil die meisten Leute, die Phishing-Awareness ausgesetzt werden, haben nicht die Möglichkeit, das zu wählen. Gerade in Firmen oder Unternehmen wird dann einfach von der IT bestimmt, dass so ein Training durchgeführt wird. Man hat oftmals keine Möglichkeit, sich dafür an- oder abzumelden. Das Gleiche haben wir an der Universität auch gemacht. Unsere Studenten hatten grundsätzlich nicht die Möglichkeit, Nein zu sagen zu diesem Training. Man hat es einfach insofern gemacht, dass man gesagt hat, alle, die die IT-Infrastruktur nutzen, müssen auch gestult werden. Da sehe ich schon noch ein bisschen ein ethisches Problem. Gerade im wissenschaftlichen Bereich hat man hier eigentlich nicht die Möglichkeit, vielen anderen Studenten zu sagen, man kann sich für so eine Studie freiwillig melden oder anmelden, sondern meistens ist es wirklich, man ist Teil dieser Studie, ob man will oder nicht. #00:20:25-6#

Severin Zimmermann: Sehr gut, dann die nächste Frage, da hast du auch bereits etwas angesprochen. Und zwar geht es hier um die Klickraten. Das ist vorhin erwähnt mit dem Thema Auswertung und korrekten Daten und so weiter. Wie stehst du denn generell gegenüber Klickraten bei Phishing-Simulationen? #00:20:49-2#

Experte 1: Grundsätzlich, das Erfassen von Klickraten ist eigentlich ein Standard-Use-Case. Das macht man eigentlich, um eine Art Baseline zu haben, wie viele Leute haben diese Phishing-Emails angeklickt. Jetzt ist natürlich immer die Frage, wie man diese Klickraten verwendet. Verwendet man das jetzt so im Stil von, wenn jemand klickt, dann wurde er gephisht oder sagt man einfach, jemand hat geklickt, aber er hat nicht sein Passwort eingeben. Das sind zwei verschiedene Fälle. Und je nachdem, was man für ein Security-Risiko hat, ist das dann ein entscheidender oder. Weil die meisten Leute sagen eigentlich, ein Klick genügt, um gehackt zu werden. Das ist aber eigentlich, wenn man das in der Security-Sicht ansehen sieht, relativ unwahrscheinlich. Es passiert sehr selten, dass ein sogenanntes One-Click-Exploit, also wenn man zum Beispiel einen Browser exploiten kann, stattfinden. Es gibt es. Es ist nicht zu unterschätzen, aber es sind eher wenige Leute, die von solchen Fällen betroffen sind. Das andere ist natürlich, wenn man diese Klickraten als hartes Measurement verwendet für Business-Cases, also für organisatorische Entscheidungen, dann kann es natürlich sein, dass, wie schon angesprochen, diese Klickraten vielleicht nicht so genau /. Oder so genau erfasst wurden /. oder die Daten so genau erhoben werden konnten. Wir haben zum Beispiel während der Studie festgestellt, dass gewisse Anti-Viren oder auch gewisse Funktionalitäten von verschiedenen Email-Client, wie zum Beispiel Microsoft Preview, einen Klick auslösen können. Das heißt zum Beispiel, wenn man jetzt ein Mail im Outlook bekommen hat und Microsoft dann ein Preview dieses Link lädt, meistens so einen kleinen Screenshot der Webseite, dann hat das /. Oder hat unser System das bereits als einen Klick gewertet. Das kann natürlich dann relativ gravierende Folgen haben, wenn man dann solche Fehler nicht entdeckt oder davon ausgeht, dass diese User wirklich geklickt haben, obwohl sie eigentlich gar nicht geklickt haben zuvor oder. Das ist ein bisschen so schwierig einzuschätzen. Es kommt immer darauf an, wie man diese Klickraten verwendet, aber generell würde ich sagen, mit Vorsicht zu genießen. #00:23:03-9#

Severin Zimmermann: Sehr gut. Du hast es aber auch angesprochen, die Rechtfertigung intern für organisatorische Entscheide, sehr wichtiges Thema. Vielleicht noch ergänzend von meiner Seite hier, wird auch sehr oft Schwierigkeitsbasiert angesprochen. Also dass diese Klickraten in Bezug auf die Schwierigkeit des phishings analysiert /. Also analysiert werden sollten, da es ja unterschiedliche Schwierigkeitsgrade geben kann. #00:23:38-0#

Experte 1: Genau. #00:23:40-6#

Severin Zimmermann: Gut, dann kommen wir etwas mehr in den technischen Bereich. Und zwar werden für Phishing-Simulationen sehr oft technische Vorkehrungen getroffen. Beispielsweise SPAM-Filter werden angepasst oder Absender Whitelisting betrieben, damit die Mails auch wirklich beim End-User ankommen. Siehst du bei diesen Maßnahmen Chancen oder Risiken, die im Zusammenhang

mit Phishinge werden es entstehen können? #00:24:09-2#

Experte 1: Diese Chancen sind eigentlich relativ klar. Man will ja eigentlich möglichst die E-Mails an einen End-User bringen. Das heisst, man passt dieses SPAM-Filter an oder macht Whitelisting, damit diese E-Mails wirklich auch gesehen werden. Das ist rein, um eigentlich das Potenzial zu haben, dass die Leute diese E-Mails sehen und sie nicht im Junk-Mail oder im Spam-Folder landen oder. Das macht insofern Sinn. Das Risiko ist natürlich, wenn man dieses Whitelisting oder diese SPAM-Filter falsch anpasst oder so anpasst, dass es eventuell sogar zu einer echten Attacke während der Phishinge kommen könnte, ist das Risiko dann erheblich oder relativ groß, dass die Leute diese E-Mails auch sehen und eventuell auf ein echtes Phishing reinfallen. Das kann man im Normalfall technisch aber relativ einfach minimieren, indem man einfach ein internes Whitelisting macht. Das heisst, man tut eigentlich nicht den Absender Whitelisten, sondern man sagt, ein E-Mail von diesem, speziell dem Server, der dann der meisten intern ist, wird gewhitelistet, was dann das Risiko eigentlich minimiert. Also die Risiken sind hier sehr klein im technischen Bereich, dass das etwas falsch laufen kann. #00:25:24-0#

Severin Zimmermann: Sehr gut. Ich greife jetzt etwas vor, da du es jetzt gerade angesprochen hast, und zwar das Whitelisting auf interne Server. Jetzt gibt es aber in der Praxis auch oft die Variante, dass ich eine SAS-Lösung /. SaaS-Lösung so jetzt hab ichs, verwende und das eigentlich von extern beziehe. Siehst du hier auch Risiken, wenn ich das so mache? #00:25:51-7#

Experte 1: Bei SaaS-Lösungen ist immer das Problem oder die Frage, wie der Datenschutz geregelt wird. Weil die Daten liegen ja dann irgendwo auf einem Server in der Cloud und es ist dann immer die Frage, wer hat Zugriff darauf. Und gerade bei Phishing ist dann die Frage, auf welche Daten haben Sie Zugriff. Meistens kann das dann relativ viele persönliche Informationen sein, gerade wenn man E-Mails schickt, die dann auch relativ persönlichen Inhalt haben. Und darum sage ich immer, bei SaaS-Lösungen ist eines der größten Risiken aus meiner Sicht, dass diese Daten abwandern oder dass diese Daten halt von anderen Leuten eingesehen werden, die man vielleicht nicht will. Das ist natürlich eines der größten Risiken. Und das andere ist natürlich, wie du gesagt hast, wenn dann Whitelistung betrieben wird und dieser Server freigeschaltet wird, kann es sein, dass man das Whitelistung falsch macht und auch andere Dienste freigeschaltet, die man gar nicht freigeschalten will. Da muss man natürlich das Testing eigentlich wieder in den Vordergrund stellen und auch schauen, ob das wirklich so funktioniert, wie man sich das vorgestellt oder wie das konfiguriert wurde oder. #00:26:57-9#

Severin Zimmermann: Sehr gut. Siehst du aber auch Chancen, die ich erhalte, wenn ich das mit einer SaaS-Lösung durchführe? #00:27:08-3#

Experte 1: Ja, meine Chancen sind ganz klar. Man hat meistens dann eine Partnerfirma, die eigentlich für einen dieses Phishing-Training durchführt. Und es ist wie beim meisten Security-Themen, wenn man durch eine Partnerfirma, die darauf spezialisiert ist, noch ein Training durchzuführen, dann ist das Know-How meistens größer, als wenn man das in-house macht. Oftmals haben diese Leute dann mehr Erfahrung, weil sie in verschiedenen Firmen tätig sind und halt auch aus verschiedenen Firmen oder verschiedenen Unternehmen ein bisschen das Know-How entwickeln können, sage ich mal. Natürlich ist es auch die Frage ein Kostpunkt im Endeffekt. SaaS-Lösungen können auch manchmal kostengünstiger sein als eine On-Premise-Lösung, die man selbst hosten, betreiben, updaten, konfigurieren muss. Und das ist vor allem auch gerade in der IT Insofern wichtig, als wenn man eine externe Firma hat, dass das meistens auch eine Zeit ersparniss ist für die internen Mitarbeiter. Weil ja, gerade im Security-Bereich haben wir nun mal einen Fachkräftemangel und da ist man wahrscheinlich dann relativ schnell froh, wenn man sehr viele Arbeitsstunden auslaken kann, gerade für solche Tasks, die eigentlich gut von einem externen Dienstleister durchführbar sind. #00:28:18-2#

Severin Zimmermann: Sehr gut, vielen Dank. Jetzt möchte ich aber nochmals zurückspringen und zwar zu den technischen Vorkehrungen. Du hast vorhin die Chancen und Risiken erläutert. Jetzt gibt es in der Praxis aber oft auch die Tatsache, dass diese technischen Sicherheitsmaßnahmen zu einem falschen Vertrauen bei den Mitarbeitern führen. Und zwar, dass sie denken, unsere Firma hat ja technische Lösungen, alles, was ich bekomme, sind normale Mails, also kann ich auch klicken oder denken, es sollte alles abgefangen werden. Wie siehst du das? Sind das Probleme, die wirklich sein können? Vielleicht gibt es dadurch auch Probleme beim Phishing-Awareness-Training? #00:29:06-3#

Experte 1: Ja, es ist definitiv ein Problem. Man muss realistisch sagen, dass wir heute einen Großteil der Phishing-Mails rausfiltern können. Wenn man das statistikmäßig anschaut, sind das über 99 Prozent. Das Problem ist eben, wie bei den vielen Dingen, es kommen halt immer noch Phishing-Mails durch. Es ist nicht so, als ob Phishing gelöst wäre durch die technischen Maßnahmen. Im Gegenteil, Phishing ist immer noch eines der größten Probleme im Cybersecurity-Bereich. Man wird das wohl nicht so einfach lösen können. Und ich denke schon, dass man hier auch ein bisschen das Problem hat, dass wenn die Leute nicht oder nie damit konfrontiert sind, dass sie dann eher anfällig sind für Phishing-Mails. Und das macht das Phishing-Awareness-Training eigentlich umso effektiver, einfach ab und zu wieder mal die Leute daran zu erinnern, dass es eben doch auch mal sein kann, dass ein Phishing-Mail durchkommt. #00:30:03-4#

Severin Zimmermann: Also verstehe ich das richtig. Du siehst da in diesem Fall das Phishing-Awareness-Training eher sogar als Chance und zwar um genau diesem falschen Vertrauen vorzubeugen. #00:30:17-1#

Experte 1: Genau. #00:30:18-5#

Severin Zimmermann: Sehr gut. Dann Schulung ist das eine. Viele sagen aber, Schulungen reichen nicht aus, sondern es sollten technische zusätzliche Informationen dem End-User angeboten werden. Beispielsweise als Warnhinweis bei einem Mail, wenn sie von extern kommt oder wenn ich auf eine Webseite gehe, die vielleicht nicht ganz konform ist, aber nicht identifiziert oder hundertprozentig identifiziert ist, dass ein Warnhinweis kommt. Wie siehst du das? Sollten solche technischen Maßnahmen hinzugefügt werden, die dem User helfen oder siehst du hier eher Probleme? #00:31:08-7#

Experte 1: Das Problem ist natürlich auch Hinweisen wie implementiert man das technisch und wie oft werden diese Warnhinweise angezeigt. Es gab Studien zu diesem Thema. Man hat sich auch in der Wissenschaft damit und in dieser Thematik befasst und es hat sich eigentlich gezeigt, dass diese Warnhinweise nicht viel Security bringen. Die meisten Leute gewöhnen sich nach einer gewissen Zeit an diese Warnhinweise und ignorieren sie dann. Weil das ist so ein wenig das gleiche Problem, das man heutzutage mit vielen Warnhinweisen, ist immer, wie geht ein Benutzer mit dieser Warnung um? Was kann er überhaupt tun, wenn er so eine Warnung sieht? Und versteht ein User diese Warnung auch? Das sind so zwei Aspekte, die oftmals im Vordergrund gestellt werden von Studien. Es hat sich einfach gesagt, dass es gerade bei technischen Themen eine Warnhinweise nicht viel bringt, weil die meisten User gar nicht wissen, wie sie im Falle einer Warnung reagieren müssen. Und darum sage ich einfach grundsätzlich, meiner Meinung nach bringt eine Warnhinweise, also sicher nicht schlecht, wenn man es macht, aber es bringt nicht viel mehr Security. Es bringt nur den technischen Usern etwas. Zu den generellen Usern ist es dann meistens eher ein Hindernis. Und ich sage immer so, eigentlich, wenn es zu einer Warnung kommt, ist es meistens schon zu spät, weil dann ist die E-Mail bereits in der Mailbox eines Users. Und selbst wenn jetzt noch ein neun oder ein User diesen Warnhinweis liest und dann der zehnte liest, diese Warnhinweise vielleicht nicht und ignoriert ihn und wurde dann trotzdem gephisht oder. Also man sollte eigentlich mehr den Hebel ansetzen, dass man die Leute darauf schult, das zu erkennen oder eben halt technisch das komplett zu verhindern, dass es überhaupt so weit kommt, dass ein Warnhinweis angezeigt werden muss. #00:33:02-5#

Severin Zimmermann: Sehr gut, also wenn ich das richtig verstehe, bringt es deiner Meinung nach bei normalen Usern, sage ich mal, nicht sehr viel, sondern ist eher störend und könnte höchstens die Chance bei technisch versierten Benutzern bieten, um phishings besser zu erkennen, falls mal eins durchkommt. #00:33:23-4#

Experte 1: Genau, aber wie gesagt, es kommt immer auch ein bisschen darauf

an, wie man diese Warnung implementiert. Ich meine, die ZAHW hat mal einen Versuch gestartet, so wie ich weiß, dass sie alle E-Mails von extern mit einem gelben Warnbalken versehen haben. Also dann kam bei jedem E-Mail dieses E-Mails von extern. Und ich denke, gerade solche Warnhinleiten bringen dann genau gar nichts, weil die kommen dann einfach bei jedem zweiten oder dritten E-Mail, also die Häufigkeit ist sehr hoch. Und das führt dann einfach dazu, dass die Leute das ignorieren, ganz klar. Also das bringt eigentlich sehr wenig Security in solchen Fällen. Es ist natürlich klar, wenn man durch einen Warnhinweis hat, so im Stil von, ja, dieses ist jetzt ein Phishing-E-Mail, zum Beispiel Chrom macht das sehr oft bei Webseiten. Wenn man auf eine Phishing-Webseite kommt, wird die ganze Webseite rot angezeigt und eine klare Warnung, dass diese Webseite geblockiert wurde oder eine hohe Wahrscheinlichkeit für phishen bereitstellt. In solchen Fällen bringt natürlich eine Warnung sehr viel. Weil das ist dann schon ein Alarmzeichen auch für die Leute und dann sagen sie vielleicht lieber, ja, ich lasse das Sinn sein. Aber wie gesagt, wenn so eine Warnung angezeigt werden muss, dann muss eigentlich der Fall technisch bereits klar sein, dass das ein Phishing-E-Mail ist. Und nicht der User muss dann überlegen oder eigentlich wissen, was zu tun ist oder. Sondern es ist dann wirklich ein Last Line of Defense im Endeffekt. #00:34:45-6#

Severin Zimmermann: Sehr gut. Dankeschön. Dann die nächste Frage. Und zwar in der heutigen Zeit sind wir sehr mobil unterwegs und nutzen oft auch unsere mobilen Geräte wie Mobile Phones, Smartwatches, Tablets etc. um die eigenen Mails zu prüfen. Nun ist es aber so, dass das Prüfen von Links und Absendern auf end /. Oder mobilen Endgeräten und Umstände anders funktioniert, gar nicht funktioniert oder halt einfach ganz anders aussieht, weil es auf einem viel kleineren Bildschirm geschieht. Denkst du, solche mobilen Plattformen sollten im Schulungsmaterial des Phishing Awareness Trainings inkludiert werden, damit die Benutzer auch wissen, wie damit umzugehen ist auf den mobilen Plattformen?

#00:35:39-4#

Experte 1: Ja, da kann ich auch Zahlen dazu geben. Wir haben ja eine Studie durchgeführt und geschaut, wie viele Leute klicken unsere Phishing-E-Mails auch auf mobilen Geräten an. Und es zeigt sich schon, dass gerade Smartphones sehr häufig verwendet werden. Also es macht in jedem Fall Sinn, dass man auch Phishing Awareness eigentlich auf mobile Geräte abstimmt und auch testet, ob diese mobilen Geräte das anzeigen. Es macht auch insofern Sinn, nicht nur auf Trainingssicht, sondern auch aus Angreifersicht, weil es gab in den letzten Jahren vermehrt Phishing-Attacken, die gezielt auf User, die mobile Devices verwenden, abgezielt wurden. Das heißt, auch hier macht es insofern Sinn, dass man auch up to date bleibt mit dem, was die Angreifer machen und eigentlich schaut, dass die Phishing Awareness auch für mobile geeignet ist. Und für genaue Zahlen kann man auch auf unserer Studie referenzieren. Da steht es einfach genau drin, wie viele Leute bei uns, zumindest an der Universität, ihre Phishing-E-Mails oder Phishing Awareness-E-Mails abgerufen haben auf den Mobile Client. Und das ist schon sehr viel. #00:36:51-9#

Severin Zimmermann: Sehr gut, danke. Ja, ich denke, das kann auch sehr unterschiedlich sein von Unternehmen zu Unternehmen. Gewisse Unternehmen lassen allenfalls auch die Synchronisation auf mobile Geräte gar nicht zu. #00:37:03-6#

Experte 1: Genau. #00:37:04-8#

Severin Zimmermann: Aber zum hier noch etwas weiter drauf einzugehen. Jetzt ist mir gerade die Frage entfallen. #00:37:15-5#

Experte 1: Du warst bei dem Mobile. #00:37:17-8#

Severin Zimmermann: Ja, genau. Vielleicht fällt sie mir nachher wieder ein. Ich würde sonst mit der nächsten Frage weiterfahren und sonst nochmals kurz zurückgehen. Genau. Und zwar siehst du /. Nein, ich muss anders anfangen. Mit Phishing Awareness Trainings werden sehr oft auch Meldeplattformen, interne Meldeplattformen integriert oder zumindest Prozesse für eine interne Meldeplattform geschaffen. Siehst du Chancen und Risiken, wenn ich solche Meldeplattformen implementiere? Vielleicht kurz als Beispiel, wenn wir einen Button im Outlook hinzufügen, wo Phishings gemeldet werden können oder eine Webseite, wo Phishings gemeldet werden können und diese dann an die entsprechende Stelle weitergeleitet werden. #00:38:10-3#

Experte 1: Das ist eine sehr interessante Frage. Es gab dazu letztes oder vorletztes Jahr eine Studie der ETH, die genau das geprüft hat, ob so ein Button im Outlook einen positiven Effekt hat auf das Melden von Phishingemails. Und soviel ich weiß, oder soviel ich das noch im Kopf habe, haben sie wirklich zeigen können, dass das eigentlich positiv ist, um die Reaktionszeit der IT runterzubringen. Also sie reagieren dann schneller, wenn halt mehr Leute das gleiche E-Mail reporten und das intern reporten können. Die können dann natürlich viel schneller reagieren. Und es macht es natürlich auch wahrscheinlich für die User einfacher, solche Dinge zu melden, wenn sie einfach einen Button haben oder wenn sie einfach eine einfache Möglichkeit haben, an das zu melden. Ich kann auch aus privaten noch sagen, ich hatte letztens einen Fall von einer Kollegin, die hatte ein Phishing-E-Mail gekriegt für so eine wie sagt man, für eine Verlosung und hat da mit gemacht und hat dann erst später festgestellt, dass die Verlosung, in der sie teilnimmt, eigentlich ein Phishing ist. Wusste aber nicht, wo man das melden tut. Und viele wissen auch nicht, dass man das, oder dass man eigentlich generell Phishing bei einer Meldestelle, der Melanie, also einer nationalen Meldestelle melden kann und dass diese dann auch blockiert wird auf nationaler Ebene. Und

ich denke, das Melden generell von Phishing-E-Mails oder auch Phishing-Webseiten kann sehr hilfreich sein zur Bekämpfung dieser Webseiten, weil wenn viele Leute das melden, kann man viel schneller reagieren, als wenn eine Person gephisht wird und 100 Personen auch gephisht werden und niemand meldet oder. Das ist das gleiche, wie wenn ein Delikt passiert oder wenn natürlich niemand etwas dagegen sagt oder tut, dann passiert auch nichts oder nicht so schnell zumindest. Ich denke, hier ist wirklich die Chance sehr groß, dass man mit solchen Report-Buttons die Reaktionszahlen unterbringen kann. Das Risiko ist natürlich immer da, wenn man eine User-Base hat, die vielleicht nicht so gut im Reporting ist oder im Erkennen von Phishing-E-Mails. Das kann natürlich auch dazu führen, dass falsche E-Mails reportiert werden oder dass der Aufwand dann groß ist, um zu überprüfen, ob diese E-Mails wirklich legitim sind oder Phishing-E-Mails. Aber für einen Informatiker, der eigentlich darauf geschult sein sollte, sollte das eigentlich ein Minimalabband sein im Normalfall. #00:40:30-7#

Severin Zimmermann: Sehr gut, danke. Dann hast du hier auch bereits das Risiko, also meine ergänzende Frage, beantwortet. Jetzt ist mir das, was ich vorhin sagen wollte, nochmals eingefallen, daher will ich nochmals kurz zu den Plattformen zurückspringen. Und zwar hast du gesagt oder warst der Meinung, dass es Sinn macht, solche unterschiedlichen Plattformen zu integrieren, besonders auch, weil es sehr oft verwendet wird, wie in eurer Studie rausgekommen ist. Jetzt wenn ich das richtig verstanden habe, siehst du dann da vor allem die Chance, dass die User halt besser geschult werden und auch geschult werden im Umgang mit online /. oder mobilem Plattformen und so quasi die Awareness erhöht wird. Ist das richtig? #00:41:20-0#

Experte 1: Genau, also ich finde es einfach wichtig, dass die Leute auf den Programmen geschult werden, die sie auch verwenden oder. Es bringt natürlich nichts, wenn man Leute eine Outlook-Schulung macht und ihnen zeigt, wie man im Outlook mehr oder weniger Phishing-E-Mails erkennt, aber dann niemand Outlook verwendet oder. Weil man kann dann vielleicht gewisse Grundprinzipien beibringen, wie zum Beispiel ein Phishing mal aussieht oder wie Phishing-Absender aussehen, aber oftmals ist das Design dieser Applikationen oder dieser Mail-Client so anders, dass viele Leute Probleme haben, ihr Wissen von einem Mail-Client auf den anderen zu übertragen. Also ich empfehle ganz klar, die Leute auf den Programmen zu schulen, die sie auch tagtäglich verwenden, um diese E-Mails zu öffnen. #00:42:08-5#

Severin Zimmermann: Sehr gut. Und dann haben wir vorhin die Thematik Risiken noch nicht in diesem Bereich angesprochen. Denkst du, es können auch Risiken entstehen, wenn ich unterschiedliche Plattformen /. Oder Probleme, wenn ich unterschiedliche Plattformen in Phishing awareness Training inkludiere? #00:42:27-2#

Experte 1: Ja klar, das Risiko ist natürlich das man /. Oder dass der Aufwand

exponentiell groß ist, weil man hat eine unendliche Anzahl von verschiedenen Geräten und man muss dann halt ein bisschen schon entscheiden, welche Geräte man schulen will oder auf welchem Programm man schulen will. Und das ist natürlich heute sehr schwierig, weil mit dem ganzen Bring Your Own Device kann man natürlich dann nicht sagen, man macht eine Schulung für alle Geräte, die eine große Firma zur Verfügung stellt. Also das Risiko ist hier ganz klar, dass man halt vielleicht einen Großteil der Benutzer schulen kann auf den Geräten, die sie tagtäglich verwenden oder den Programmen, die sie tagtäglich verwenden, aber dass man dann hier auch User hat, die dann eben nicht geschult werden können auf den Geräten, die sie haben oder. Das ist eigentlich der Nachteil, wenn man möglichst viele Geräte versucht da reinzubringen oder die Phishing-Kampagne darauf anzupassen. #00:43:21-3#

Severin Zimmermann: Sehr gut, vielen Dank für die Ergänzungen. Jetzt kommen wir zum Umfeld. Vielleicht nochmals als Einstieg, sind hier externe Einflüsse bekannt, die du bis jetzt noch nicht erwähnt hast, welche bei der Durchführung eines Phishing-Evernis-Trainings beachtet werden sollten? #00:43:42-5#

Experte 1: Ja, das ist natürlich jetzt eine schwierige Frage immer, weil man es extern anschaut oder. Ich meine, für uns als wissenschaftliche Mitarbeiter war natürlich auch extern unser IT, sozusagen das externe Dienstleister. Die muss man natürlich sicher mit ins Boot holen bei einer grösseren Phishing Awareness. Wenn man jetzt sagt extern, so ausserhalb des Unternehmens, dann ist es klar, dann kommt es ein bisschen darauf an, in welchem Land man tätig ist. In der Schweiz würde ich jetzt empfehlen, man sollte das National Cyber Security Center, also NCSC, informieren, wenn es eine grössere Phishing-Kampagne ist. Man sollte den eigenen Domain-Registrar mit ins Boot holen, weil diese Domains können natürlich auch gesperrt werden, was dann ein Phishing-Training natürlich unmöglich macht. Und eventuell, je nach Größe, sollte man die Switch also den für den Schweizer Markt tätigen, wie sagt man, Domain-Registrar, auch mit ins Boot holen oder darüber informieren, dass solche Domains registriert werden und für Trainingszwecke verwendet werden. Ansonsten kann es natürlich sein, wenn man gerade von externen E-Mails versendet, dass diese dann auch von externen geblockiert werden, dass der Domain-Registrar diese Phishing Emails oder diese Domains erkennt und auch blockiert und die E-Mails gar nicht bei den Absendern /. Also bei den Usern ankommen oder dass die Website-Links, auf die dann verwiesen werden, bereits gesperrt sind. #00:45:19-4#

Severin Zimmermann: Sehr gut, vielen Dank. Dann die nächste Frage, die haben wir bereits angesprochen, und zwar geht es da um die externen Partner zum Implementieren im Phishing-Awareness-Training. Du hast hier bereits deine Sicht oder Chancen und Risiken erläutert, die aus deiner Sicht entstehen können. Eine Frage, die ich hier noch nicht ergänzend gestellt habe, siehst du Risiken oder Chancen, wenn ich mit ausländischen Partnern zusammenarbeite? #00:45:54-2#

Experte 1: Ja das ist natürlich /. Der Punkt ist, jedes Land hat seine eigenen Regulierungen, wenn es um Phishing-Awareness geht. Wenn man mit ausländischen Firmen zusammenarbeitet, muss nab sich natürlich /. Oder muss die ausländische Firma sich bewusst sein, wie die Regulierungen im eigentlichen Land sind oder. Das ist schon noch wichtig, dass man da auch ein bisschen Konsens hat. Das ist vor allem dann sehr wichtig, wenn man auch internationale Partner hat, die übersehen sind, zum Beispiel aus den USA. Weil das US-Recht ist schon sehr unterschiedlich zum europäischen Recht. Gerade auf rechtlicher Ebene muss man hier sehr viel beachten. Man sollte schon immer sehr aufpassen, wenn man an so einem Phishing-Training durchführt, dass das auch den länderspeziphishen Regulationen angepasst ist. #00:46:48-2#

Severin Zimmermann: Sehr gut, danke. Dann vielleicht allgemeiner hast du Ergänzungen zu der Zusammenarbeit mit externen Partnern oder hast du hier bereits alles gesagt? #00:47:00-5#

Experte 1: Generell sage ich mal noch, was wichtig ist, dass man sich auch bewusst ist, dass wenn man Branding von externen Partnern verwendet, dass man auch dementsprechend, wie sagt man, dementsprechend die Einwilligung dieser Partner einholen muss. Das heißt, wenn ich zum Beispiel ein Phishing-Email mit Google Branding versende, müsste ich grundsätzlich auch die Einwilligung von Google haben. Das ist oft mal etwas, das viele Leute nicht wissen, was ich einen sehr wichtigen Aspekt finde. Und das andere ist natürlich, wenn man mit den externen Partnern zusammenarbeitet, dass die sich auch bewusst sind, wer die Verantwortung übernimmt, dass die Verantwortung klar geregelt ist. Dass wenn jetzt zum Beispiel eine Firma für uns Phishinge Awareness durchführt, dass sie sich bewusst sind, dass sie auch einen Teil der Verantwortung tragen oder und dass sie auch diese Verantwortung dann rechlich, falls das jetzt rechtere Folgen hätte, auch tragen oder die Verantwortung dafür übernehmen. #00:48:06-7#

Severin Zimmermann: Sehr gut. Du hast es jetzt gerade angesprochen. Meine nächste Frage wären rechtliche Aspekte. Du hast es jetzt erwähnt mit Markenrecht und Branding. Auch zuvor hatten wir bereits das Thema Recht mit Regulatoren in unterschiedlichen Ländern etc. Mir auf die Schnelle fällt kein weiterer rechtlicher Aspekt ein, aber vielleicht dir? #00:48:35-2#

Experte 1: Ja das ist noch interesant. In der Schweiz, also einfach so als Info, wird Phishing Awareness grundsätzlich als Phishing anerkannt, also auf rechtlicher Basis, wenn dies nicht offiziell gemeldet wird. Das heißt, rein theoretisch könnte man als phisher verklagt werden, wenn man Phishing Awareness in der Schweiz macht, wenn man die in dementsprechenden Fälle also (unv., #00:49:02-1#) Stellen nicht informiert, sowie auch eben wie gesagt das Branding einhaltet. Es kann sehr hohe rechtliche Konsequenzen haben, wenn man das

falsch macht. Nicht zu unterschätzen. #00:49:18-7#

Severin Zimmermann: Okay, sehr gut. Wusste ich so auch noch nicht. Die nächste Frage hast du auch bereits angesprochen und zwar das Informieren von externen Parteien wie eben Regierungsinstitutionen, Hosteregistrar. Jetzt meine Frage hat hier mehr auf zwingend abgezielt. Das ging vorher aus deiner Antwort nicht hervor. Also darum, sind dir /. Oder sind dir bekannt, dass externe Parteien zwingend informiert werden müssen? #00:49:52-7#

Experte 1: Aus meiner Sicht ist es kein Zwang, es ist eine Empfehlung grundsätzlich. Wenn wir zumindest von der Schweiz reden, gibt es kein keine /. Also keine Pflicht, dass man diese Leute informiert also "zwingendermassen". Man will aber natürlich nicht unbedingt auf Konfrontationskurs mit diesen Institutionen geben. Und wie gesagt, es kann natürlich sein, wenn man diese Nicht-Vorgänge informiert, dass diese einen sozusagen blokieren das die domains (unv., #00:50:22-2#) blockiert werden. Aber meines Wissens nach ist es keine Zwingendermaßen, dass man die informieren muss. Es ist mehr eine Empfehlung. #00:50:32-0#

Severin Zimmermann: Sehr gut, danke. Dann nochmals bezüglich melden hier jetzt aber wenn ich Opfer eines phishings wurde, also eines echten phishings, sind dir da Meldepflichten bekannt? #00:50:45-5#

Experte 1: Soviel ich weiß, gibt es keine Meldepflicht für Opfer werden. Es ist klar, wenn natürlich eine Firma gehackt wurde und Daten abfließen, sieht das ein bisschen anders aus. Da gibt es eine Meldepflicht grundsätzlich. Vor allem dann, wenn persönliche Daten, also Kundendaten gestohlen wurden. Hingegen, wenn jetzt eine Privatperson gephisht wurde, gibt es keine Meldepflicht. Es gibt natürlich eine Empfehlung, dass man das meldet bei den staatlichen Stellen, zum Beispiel bei der Polizei, die dan den /. Oder bei denen man dann Anzeige erheben kann gegen Unbekannt im Normalfall. Und die sind natürlich froh, wenn sie auch solche Fälle erhalten, weil dann kann man auch rechtlich dagegen vorgehen oder. Wenn das nicht gemeldet wird, dann ist das immer das Problem da, dass es niemand weiß und dass dann auch nichts dagegen unternimmt oder oftmals nichts dagegen unternommen wird. Aber soviel ich weiß, gibt es keine Meldepflicht für Phishing Attacken. #00:51:49-9#

Severin Zimmermann: Sehr gut. Jetzt fällt mir gerade aufgrund deiner Antwort noch eine weitere Frage ein, die ich noch interessant fände. Und zwar siehst du Risiken mit solchen externen Meldungen, also wenn jetzt beispielsweise ich als Person eine Meldung extern aufgebe, aber es war nur ein Phishing Awareness Training von der Institution. Könnte zum Beispiel im Zusammenhang auftreten, dass sich die Mitarbeiter nicht informiert haben über eine Phishing Simulation

und diese sich dann an die externen Stellen melden. Siehst du das als Risiko oder eher nicht? #00:52:29-5#

Experte 1: Das ist ein sehr großes Risiko, das ist uns während der Studie auch passiert. Es ist sehr wahrscheinlich, gerade wenn man einen größeren Rasen Phishing Awareness macht, ist die Wahrscheinlichkeit fast 100%, dass Leute das an ausserhalb der /. Also zumindest im technischen Bereich außerhalb der Universität bei uns melden. Und das kann natürlich dann Prozesse bei anderen Firmen auslösen, dass zum Beispiel wenn man jetzt davon ausgeht, dass ein Unternehmer eine Phishing Awareness Kampagne macht und jemand meldet das an das NCSC, kann das natürlich dann sein, dass das NCSC ihre internen Prozesse startet und natürlich die Firma informiert, dass so ein solches Phishing E-Mail gemeldet wurde. Und dann überprüft, ob die Firma eventuell gehackt wurde oder sich mit der Firma in Verbindung setzt. Und das kann natürlich dann je nachdem, was für E-Mails gesendet werden, durch auch weitreichende Folgen haben. Also es kann zum Beispiel auch sein, dass man die Firma informiert, wenn es jetzt zum Beispiel eine Branded E-Mail ist und dass dann die Firma anfängt, ihre internen Prozesse laufen zu lassen, zum Beispiel eine Warm-E-Mail herauszuhenden an ihre Kunden. Solche Dinge können möglicherweise passieren. Das ist wahrscheinlich ein sehr großes Risiko, wenn man natürlich diese Meldepflicht gegen extern macht oder wenn man sagt, okay, man muss jedes Phishing E-Mail melden. #00:53:49-9#

Severin Zimmermann: Sehr gut, danke. Dann wären das eigentlich auch alle meine Fragen gewesen. Hast du vielleicht noch Punkte, die wir noch nicht angesprochen haben oder Punkte, die ich vergessen habe, die deiner Meinung nach noch wichtig sind? #00:54:04-3#

Experte 1: Nein, ich denke, wir haben alles angesprochen. #00:54:08-8#

Severin Zimmermann: Sehr gut. Dann meine letzte Frage. Ich werde noch weitere Interviews durchführen. Dürfte ich dich, falls da neue Aspekte auftreten, die ich /. Oder von denen ich auch gerne deine Meinung hätte, dich nochmals kontaktieren? #00:54:24-5#

Experte 1: Ja klar. #00:54:25-6#

Severin Zimmermann: Sehr gut. Dann würde ich jetzt die Aufzeichnung beenden.

E Transkript Experten-Interview Experte 2

Administrational	
Interview date	12.04.2023
Interview partner	Experte 2
Employer	ThriveDX Enterprise
Recording OK?	Ja
Anonymization data?	Nein

Severin Zimmermann: And will start with my first question. May I ask you to briefly introduce yourself and maybe your position and function in your company? #00:00:13-9#

Experte 2: Yes, so my name is Experte 2. I was born in Israel. I did my Bachelor and Master's in Computer Science in Tel Aviv University. It's one of the top universities in Israel. My research in my Master's was about security. It was technical, computer science, DDoS attacks, and so on. I submitted a research proposal. The SNF gave me money to continue it and I came to (unv., #00:00:52-2#) to do my PhD. Then I was in various positions after that in Switzerland, in the Zurich area. Security architect of a big managed security provider.I was a senior data scientist in Swisscom with really cool business applications. Then I was an enterprise security architect at Sixgroup, which is ifrastructure /. Financial infrastructure of Switzerland practical. Also not so many people know, but Sixgroup also owns the Spanish stock exchange. One company owns both the Swiss and the Spanish stock exchange. Then later I decided to move to the company called /. To join the management of a company called Lucid Security, which is a Swiss startup which is selling actually security awareness platforms. I was there working as a co-CEO, replacing the CEO. Right at the stage where I was supposed to replace the CEO, we already (unv., #00:02:02-4#) a company called ThriveDX, which is specialized in cyber security education. We are selling also other products related to cyber education like application security, education, and so on. My role in the company right now is managing all the business in Europe. It's more like a senior position and more like focusing on what the company needs at the moment. We don't have a very specific position rather than really manage the whole business and know an authority like what the product, about cyber security, how to do education, and so on. When it comes to experience and knowledge in cyber security then (unv., #00:02:52-6#). #00:02:55-6#

Severin Zimmermann: Okay, thank you. You already answered my next two questions about your experience with phishing and phishing awareness. I will just

skip that as I see you have experience with phishing awareness training. You worked in a company who sells products for phishing or sold products for phishing awareness. I will skip them and go on with my main questions. Do you see positive aspects that can result with, or by doing phishing awareness training? #00:03:32-8#

Experte 2: Positive aspects? #00:03:35-2#

Severin Zimmermann: Yes. #00:03:36-6#

Experte 2: Okay, so it's always a trade-off like you mentioned. It could be /.So there are several problems when people are building security awareness programs. Many /. OK so One thing that's important to understand is that there are different maturity levels for security awareness program. Many companies are really focused on just to be compliant because many security framework or even just compliance framework require you to teach all your employees about phishing and about I don't know what and about not letting the outsider into the building and all kinds of basic stuff hide away or destroy secret documents and so on. So this has to be for the sake of compliance. We have policy, we have directive in the company, you must educate everybody about it. Here you at and you need to tick this box. In many companies what they're doing is that they're buying this kind of solution, sending it to all their employees, making sure they did it, they passed the test, it means they know the knowledge and that's it. This is where it ends. Many of the platforms today what they're doing they're also allowing you to do a phishing attack simulation. Then the employees are getting some kind of phishing email or some different attack, not even to an email, it can be through an SMS, it can be through even a different way or even like a QR code somebody is printing or even USB stick somebody forgets in the kitchen and see how many employees fall in that. This also can have limited effect in the way that it's done. The secret is how you tailor this kind of attack to make it also interesting and also make it effective. About your specific question, maybe I don't know if I'm jumping to the end, what are /. so this specific question is about what are the benefits, right? #00:05:36-9#

Severin Zimmermann: Right, what are the benefits when you're doing phishing awareness training? Of course the employees get educated and aware of this specific type of attack but maybe you know some other positive or benefits which results in phishing awareness? #00:06:00-7#

Experte 2: Okay so I mean /. Okey i don't know if you're using the term phishing awareness because this is what you know or this is what you mean but I want to talk about security awareness program so yeah. Security awareness program is a program that is directed to teach the employees about the regular employee

about what he needs to know and do when it comes to security. There are many things you should teach the employee. Phishing is just a small subject but it gets all the spotlight because this is everything we think of and because of the phishing attack simulation they're very specific about phishing. But what other topics do you have that the employee needs to know? He needs to know physical security, how to behave in the office, where to hide what, not to stick his password on the screen, whatever password security we just mentioned that, mobile security, when he's in the train, how can you use his phone, his laptop and I don't know what, can he have phone calls with clients or with colleagues, what can he say or not saying these phone calls and so on. Bring your own device security, well you can now install your office 365 on your laptop or on your tablet at home, what should you do to secure it and so on. There are many different topics, cloud security, IOT, internet of things, you know a lot there are many different topics, biggest one privacy. So in privacy education we teach the employee about all the different aspects and regulations coming to privacy, GDPR or the Swiss Data Privacy Act for example, what do you do with it, what are your obligations as an employee, most importantly. What we in our company, what is the different classification that we define in our company to different documents and how do you know which document is classified and in what way. So in the past and this is a very complex topic because in the past it was very simple, the documents that are public, documents that are internal, some secret maybe some top secret, you know so there was like a secrecy spectrum. But now there is another dimension and it's privacy spectrum. So it would be a let's say very general information that I can find on the web, for example a picture of you in bikini on a beach, this is really not classified for the company, this can be public, it was actually posted on your Instagram, great, but we cannot store it in our computers because this is the private information that belongs to you, right. So from privacy it has a very high value but from secrecy it has a very low value and it becomes very complex and every company depends on their business, financial, insurance, retail, they have different even definitions of different names, different stages of privacy and secrecy. This is another big topic and all these topics that I just mentioned they are huge and all the employees need to learn how to work with them. And I can continue but you understand phishing is one topic of them and the security awareness is a program that is teaching the employee about them so the employee can get a force about fishing, they can also get the force that is teaching the employee about each of these things separately, you understand? #00:09:35-1#

Severin Zimmermann: Yes, so if I get it right and summarize it, so phishing awareness is one aspect of security awareness, just a small part, but you have /. As a company you have to look at all these kinds of different security #00:09:56-5#

Experte 2: we call it topics or domains #00:09:58-6#

Severin Zimmermann: Topics yes #00:09:59-1#

Experte 2: That very regular employee needs to know about. #00:10:04-0#

Severin Zimmermann: Okay, but may I ask, so specific on just phishing awareness, do you know benefits, so if a company besides the other topics is doing phishing awareness do you think there are some other benefits that just the awareness itself the company can gain out of it? #00:10:29-6#

Experte 2: Okay, so what is the awareness, what is the business value of the awareness is your question? #00:10:35-9#

Severin Zimmermann: For example, so maybe another example #00:10:40-1#

Experte 2: or maybe something else beyond the awareness, no let me let me answer that, okay? #00:10:43-5#

Severin Zimmermann: Okey #00:10:44-5#

Experte 2: So the business value of the awareness is it's following first reduced risk of breach, so people know how to identify a phishing emails, they know how to identify not only fishing emails also fishing SMS or fishing phone calls, right, this is the first thing, first benefit, right. Sometimes the employees already know that, but the awareness course or the awareness the whole process reminds them of that, you know, sometimes you know how to do that, so like if I give you a test you will know how to answer it completely perfectly, you'll get 100 out of 100 percent in the score, but you when you're doing your everyday job you completely forgot about this topic, so sometimes this this course is active reminder and by the way for that sake it's important to also understand and good security awareness tools to that they know to tell between let's say the slow employees still need to learn and let's say the smat employees that they already know everything they just need to be reminded, now so. And this brings me also to the let's say the your next question if I'm jumping too fast, what are the let's say then the the disadvantages, so the disadvantages of course wasting the employee's time and annoying them, that's the main disadvantage of that, and also yeah when if you thought if it's done especially too much then the employees can just assume everything is just phishing training and don't really understand when something really is coming their ways. Now another benefit that a security program has besides specifically, I mean the entire security program is used not only to teach phishing but not only to teach other topics of security, it can also explain and validate first that the users read and know the policies of the company, this is business value one in terms of compliance that you're compliant but you also reduce risk of people at risk not doing not following your directive and policies.

And another indirect let's say byproduct of that is that the security team has an opportunity to present themselves and their services saying hey guys we are here if you need this you come to us we are going to help you understand you we care about you and so on. And one last thing another indirect one again not in all companies you benefit from that when the CISO when the security group actually say okay we need to take all our policies and push it in the face of each and every one in the company including my manager including the CEO i'm going to tidy up a little bit and make sure it makes sense and it's not annoying and it's easy to read and that it fits the business. Now because sometimes when you just give a bunch of lawyers some documents to write and then they just put it in some folder and everybody just need to read and click then sometimes you forget about it but when you really do such a program you spend so much time writing and education writing the course we have a password policy you have to follow it and you start making videos about it and writing text about it then it makes you rethink your your entire policy and you also get feedback from people feedback you wouldn't get. So a big part of a good security awareness program is that you also collect the feedback from people what do they think about this aspect of security you taught them about privacy for the most physical security what phishing also what do they think about. So this is /. Starts maybe another point you can write it starts it initiates a conversation with employees about security about the policies and if it makes sense and if you feel safe anyway this is what matters. #00:14:57-5#

Severin Zimmermann:Okay perfect thank you so yes you already the next question questions the negative aspects so disadvantages so i will go on you mentioned a lot of /. Or now a lot of organizational aspects so advantage on organizational factors and disadvantages #00:15:21-9#

Experte 2: But wait wait wait wait wait don't jump over questions because maybe i said something but i didn't cover everything so i want to give you good material so the next question that was about the negatives more negative stuff is that the security team is always every security thing there are endless things to do and nobody has the time to have the people to run this program this looks always like the least important thing but also it's important but it's another thing the team has to do. And it usually also uses products that cost money so there are serious costly. And can also generate a lot of noise in the sense of you're running it and then a lot of employees are annoyed and sending you emails and questions and why is it like this why is it like that what what do you want from me and so on (unv., #00:16:13-2#) . Another thing it can also a security program done wrong can create like any kind of security measure that is done wrong can give a false sense of security that's why. #00:16:30-0#

Severin Zimmermann: Okay thank you. Do you also know /. Sorry do you also know some technical advantage and disadvantage so by that i mean usually if i'm doing phishing awareness training within my company and for example sending phishing simulations i have to adjust my rule set and other things so do you

know some advantages or disadvantages from the technical point of view? #00:17:09-1#

Experte 2: Okay so most products also most people they are using the SAS service which means there is some server on the internet but it's doing all this stuff sending all the education sending all the phishing emails so it means that you need to open some ports white list this server maybe and so on. Some companies like ours because our company was actually built by pen tester for the Swiss financial sector allow you to install it onprem in the company's data center so you still have everything inside the data center and sort of secure. But again still you can create a lot of mess right so it's still /.You're opening yourself to some yeah we need to do some integrations and the most substantial integration is the integration with active directory so active directory is like the phone book of your company and you synchronize everybody either not only like what kind of fields you want to synchronize but it's enough that you have the name the full name usually the language at least the email and everything you know goes into this program they're also collecting all kinds of information. Let's say if i'm setting up a fake website where you're supposed to log in so radically my tool can also record the credentials you're putting in so this would it be. You can also disable it but this is also something that theoretically can happen um and if some malicious actor is taking over this server that is doing this fishing training theoretically can launch real attacks on your employees because it is completely whitelisted. Technical disadvantages um yeah i mean like all the potential on our (unv., #00:19:06-7#) you have when you're buying software advantage main advantage is that many solutions okay not many but a lot let's say you have many (unv., #00:19:22-5#) many solutions they also give you the option to install a phishing reporting button so if you /. So if the employee sees an email that he suspects is a phishing email he can press it and then it's reported to the security team and as part of the training they you teach the employee to use it and you can use it with the security operation center to build the playbook to handle this kind alerts thats the advantage. #00:19:55-3#

Severin Zimmermann: Okay nice that was something i actually did't know that that comes with most of the tools or with some of the tools. The next question would be. Do you know from environmental factors aspects that affect phishing awareness so maybe how can i say that if you work with an external partner for example or some regulations do you know there are some aspects #00:20:36-1#

Experte 2: Environmental aspects? I mean the solution itself is very thin i mean it's a software that you install and send email (unv., #00:20:47-9#) do any computational overload so that's not a problem really. But the way that you use it can be completely digital in many ways it replaces physical training so we don't have like a trainer that has to travel to some place and stay in the hotel take a airplane and so on so it's very efficient. no nothing nothing special with it not an environmental i think the footprint is very very low i mean you can think about something there are physical aspects of it so like when security imprint posters or even using

real usb sticks that they're putting around but that's really the maximum they can do #00:21:46-8#

Severin Zimmermann: okay We will come later on with some detailed questions about that, that was just to get the the default point of view and so i will start /. I will ask you the next questions do you know any other aspect that remains open from your point of view while doing phishing awareness training #00:22:15-8#

Experte 2: what do you mean aspect that is still open? #00:22:19-6#

Severin Zimmermann: Tthat's my question to you do you think about a aspect that's still open or advantage or disadvantage that you that we haven't talked about yet that you think it's important to phishing awareness #00:22:38-0#

Experte 2: Advantage and disadvantage always um relative to something so maybe you're saying about. Something that is good about it for the company something that is bad about it for the company is that what you mean? #00:22:57-7#

Severin Zimmermann: Yeah #00:23:01-3#

Experte 2: Advantage over what over not doing it this is what you mean? #00:23:05-0#

Severin Zimmermann: So it's more meant what you can get out oh what why you should do Phishing awareness training #00:23:15-2#

Experte 2: Okay #00:23:15-6#

Severin Zimmermann: But we already have talked about it i it's just the question if you have any other points that maybe i've forgotten or i didn't mention or something like that? Otherwise it doesn't matter we can go on with the detail questions and if #00:23:37-4#

Experte 2: i mean listen listen i mean there are some there are some research that is saying ah doing a lot of fishing training can actually reduce in the way that i like um i'll call it thomas um but i think this this kind of results are quite biased so i think if you're doing it wrong you're over teaching people that already know and you're under teaching people that don't understand you're just even annoying it's scary even more that can be even worse so yeah you need to. And if people are not going to be effective /. It's like a surgery in a way right. It's like a medicine you're taking a medicine doesn't fit the body doesn't feel patient it can also do even a bit harm than fixing stuff. #00:24:36-7#

Severin Zimmermann: Yes so that was a good other aspect um i will ask you the next question so now i asking more detailed questions specific questions so the first will be. A lot of /. Or it's often mentioned that you that you should personalize phishing awareness training to your specific employees and train them differently about different people work from maybe HR department or financial department what do you think about that is that important or is /. #00:25:31-1#

Experte 2: Yeah very important very important #00:25:35-0#

Severin Zimmermann: Okay good. #00:25:36-5#

Experte 2: should i elaborate okay maybe i just tell you the aspect so it's important first of all that the content is relatable okay for example we had a client in saudi arabia he looked at all the /. You know in saudi arabia most of the employees of course and they're arabs but actually most of them are indians or people um or black people from africa sometimes even and they wanted the avatars the people that are that appear in the courses to be to look like them to dress like them they didn't really relate to this uh tall blonde guy in a suit or this suit or this blonde girl in mini skirts and high heels this is not how people dress in a corporate environment in saudi arabia so this is first thing relate to the culture relate to the language also translate it to the language. The second even more important thing is to adjust the content to the country to their laws in the country and also specifically to the policies of the company itself i've seen many companies just buying some let's say password course and just like playing it okay so i bought a video teaching you about password security but then the instruction how to set a secure password doesn't fit the company policy tell you in the video they tell you you have to have like different characters different this and in the company you can just set up six numbers and that's fine. And also there should be an adjustment to the industry if you're a person working in retail you like to read stories about security related to people working in a big store not people working in procurement department somewhere or some sales people that took us on airplanes the whole time related to me. So these are the most important thing but of course also to tailor the entire programs to the real challenges and the risks of the company so yeah but this doesn't really relate to the localization um yes and also gender is also important for being able to speak to women and men. And also uh when you

talk about two languages like the german language um if you're speaking /. Some companies want to speak in the do language someone to speak in the c language so it really it sounds it really needs to fit what the company is doing and for many companies they actually insist it's very important to them that the colors and the fonts is according to the company style guidelines i don't know if you're aware of that but like every company has their own fonts and colors and then and icons that are using for all the presentations and ads and they want also the security awareness to fit. So then the employee feels it's like any other training but without that he receives from the company but it's like something from us you know not some random something that we bought. Yeah that's it. Oh and of course also if you put some anytime you can put some intranet links specifically intranet links and name of real people or a personal message from the CISO or from the CEO or even a video from them (unv., #00:28:55-6#). #00:28:59-8#

Severin Zimmermann: Okay very nice thank you. And the next question is about the course material. There is many different ways to deliver the course material you can do like you said early embedded training where you send phishing emails and teach the people who clicked on the link there is also different kind of content such as gamification video fact sheets and also the delivery method in a class-room or online and another aspect is do you inform your employees that you're doing phishing awareness especially in phishing simulations or just center phish-ing simulations what do you #00:29:55-9#

Experte 2: Yes you do i mean i don't think it's a legal requirement but for many companies their internal policy does not allow them to do something like that like to do phishing simulation attack without alerting the employees first but it's not like it's more like some article you have in the intranet like the next month or quater will have some phishing attack simulations so nobody (unv., #00:30:22-5#) #00:30:22-5#

Severin Zimmermann: So do you think to it's important to think about how you do the phishing simulations or phishing training or do you think it's just important that you do it doesn't matter in which way #00:30:45-7#

Experte 2: Okay you're mixing here several things. Let me separate it okay there is the education there is the one thing the education is a course they need to sit 20 minutes do it learn it. And then and then there is testing there are two types of testing whenever testing in the end of the course questions about what you learn another type of test is the phishing attack simulation isn't like a real-world test but both of them are in the test you do and there is the learning now there is another type of education because some companies like to call teachable moment is after the user clicked the link but he shouldn't click then there is like this website and "oopsie" you clicked on the phishing link why don't you see this really cute five minutes video that or two minutes video that explains a bit about the basics of

phishing or playing this game whatever but these are these are called micro learning and they are more like for reinforcement this are not this is not really the place to teach the the user about phishing because you assume /. You must assume that the user will not do any of that if he's doing it's nice but because when the user click your link it was while he was in the middle of the meeting middle of four this is not the time that we wanted to do this training. What you need to /. And when it comes to the training you need to ask yourself is this user educated in phishing or not it has nothing to do really if you click the link or not you know. The people that click the phishing link it doesn't mean oh he didn't he just doesn't know how to analyze the domain this is not really the reason in real world why people click the links could be /. So if you're using a good software that can understand what is the level of every user you can also adjust sending harder or easier phishing attack simulation. And also let's say more basic education or more like fun and short education that is just reminding you the things that you already know. So i don't know if i answered your question but i tried to go over what is the education and how it should be done #00:32:59-3#

Severin Zimmermann: So i get out of it. You have to different. differentate if you're doing phishing awareness teachable moment for example and so it's important you think about that and also think about how you deliver that so is it just to remind someone so you're doing a fun a funny video or something like that just to remind him or if you do a course which really should educate and not just remind the employer so that /. Is that right? #00:33:39-0#

Experte 2: Yes. #00:33:40-6#

Severin Zimmermann: Okay then another question it's often discussed if you should inform so let's say especially for phishing testing if you should inform your IT personal about the phishing testing or not what do you think about should the it be informed or not? #00:34:06-3#

Experte 2: um yes of course not on the specific details but telling them look this is the server uh it is has been practically in most cases they need to be in the know because they need to whitelist a lot of the phishing attack simulation coming in. And also there might be a lot of reports from employees you know some employees are smart they're saying okay this is a phishing email and many of the many times the phishing emails look very tailored you know it's like it's not just some random email from fedex it's like somebody that is trying to pretend to be our very specific CEO like there is maybe campaigning and stuff. So they are panicking and calling the IT support and everybody and they this is why it's important to notify an entire company there is a campaign going on if you find something he'll relax but also specifically to the IT people or the people managing the security incidents telling them there is this server there are these emails there are these links from these domains they are okay it's all fine it's all part of the simulation don't worry about it it's definitely that you know about it #00:35:15-5#

Severin Zimmermann: Okay #00:35:16-6#

Experte 2: I mean what do you again by not telling them about it? #00:35:19-9#

Severin Zimmermann: It's often mentioned so IT personal is uh um how i call that i really #00:35:33-8#

Experte 2: wait i'm not saying you should not test them you should test them. #00:35:38-2#

Severin Zimmermann: Right but often it's mentioned. If they know about that they are more aware about phishing and they won't react like they usually react that's often discussed so that's why it's discussed. #00:35:52-4#

Experte 2: Okay listen what is aware i mean the entire company should know there is a campaign running should tell them it doesn't help them really that much. Look the only reason why run a campaign without telling anybody in the company is because when you run /. Won't run you want to have baseline results because you cannot /. Nobody can learn anything if you just start phishing campaign by doing the test nobody learns anything you want to do some education first and then doing a test it's like when the when you drive your car and you see sometimes signs saying oh be careful there are speed cameras ahead so people are more aware and they are in general driving more securely let's say. So it's the same with phishing texting just letting know people know that oh. there is a phishing attack the next quarter there is another fish every quarter you tell them there is a phishing simulation in the next one two months so people are always alert you know they don't want to /. Tthey don't mind if they click something and then somebody in russia i don't know get something from it but if you know my colleagues are going to know about it maybe they tell my boss or i don't want to click it again it's much more important to them #00:37:12-1#

Severin Zimmermann: Okay nice yes i agree with you so if you inform them so they will be aware which gains the same effect you want to get out of the phishing awareness they are more aware. So the next question is about uh cyber security culture do you think the cyber security culture of a company plays a role in phishing awareness or do you think it doesn't matter which cyber security culture a company has #00:37:56-2#

Experte 2: Define /. I will let you first define what is the cyber security culture in your eyes? #00:38:02-2#

Severin Zimmermann: So in my eyes it's how the employees sense about security is so in this case i may /. I mean not just phishing awareness or how they are aware of phishing awareness or also the other topics you mentioned in the beginning. So and how the people talk about security things inside the company so they do they talk about if they get a email that they are not sure if it's real or not or is the culture like it's my own problem and i don't ask anybody else #00:38:51-2#

Experte 2: Okay so the security culture is what the security team is making of it okay. So if the /. Like i said the security awareness is exactly this thing that you mentioned is the security awareness is the security culture the security awareness program is meant to design the security is meant to design the security culture and the security awareness is based on what is the current state of your security culture and what /. How do you want to change. For example let's say a company that now moved from using outlook on prem they want to go to the cloud and use outlook in the cloud you need completely different way of thinking you need to to classify documents that you send as an attachment. You need to for example stop sending you know when you're using microsoft 365 you don't want to send attach, attach files to emails you share the link you know so you need to teach the employee so. So the security is also by the way that you're behaving in what your company is doing what are the risk and what is important. For example if you're working in the stock exchange your security is completely different and if you're working /. Not completely different but it's different there the stock exchange it's more important the secrecy yeah in the secrecy but more um yeah the availability of the servers then in other department where it's not that important if you just lose some information just lose some money but you don't reach any personal customer information and so on. But again i think i think relatively but the most important thing for the culture is what the security team is making okay what does it mean. It means if they are a bunch bunch of arrogant guys that think oh my god we are the superheroes all the other people in the company just "dummies" don't know all the risk we're saving them from every day and they're just writing these horrible policies don't listen to people everybody hates the security team nobody listens to them they're striking annoying policies. Then nobody /. Everybody is getting first of all bad sense a false sense of security that people think dude i cannot do anything on my computer i cannot even save a file i cannot even connect it to a network so obviously it's super secure but they don't realize so they get this false sense of security. Second they don't care about security they're saying okay well i i'm not part of the security the security team treats me like an idiot and they are just protecting and putting me in a tin box anyway so no matter what i do i'm secure just treating me like a baby that they're strapped into the key to the children's side (unv., #00:41:44-0#). And also when i have a problem these guys will come and destroy me i don't want to tell them if i suspect something or if i'm project manager and i feel like i have a problem and i would need their advice i would afraid to ask them because they will come and trash my project they will stop everything you tell me you cannot do this you cannot do that.

So part of the goal of a good security team is to make themselves in security awareness program make themselves approachable and change that culture if they have like toxic culture the problematic culture and security teams especially in the company that the security is more like a risk slash legal entity and it's quite separated from the IT then what happens is that they come up with a lot of policies that really annoy IT so they cannot do their work or cannot implement stuff. For example now you cannot ping from this firewalls (unv., #00:42:45-4#) firewalled and why because i read some article that says it makes everything vulnerable and allow attackers (unv., #00:42:51-1#). In the cloud and we do not allow that in the cloud. So if you get /. If the security culture is that you're helping your employees you care about their business and you're really trying to be creative about it. And you (unv., #00:43:22-2#) to help you (unv., #00:43:23-5#) your your friend then yeah it means a lot. And also it could be that in some company /. I'm just blaming the security guys all the time. Not in every company all the corporate people they are just super highly educated people earning 150'000 a year many of them are just you know teenagers on their summer vacation working in co-op or in 7-eleven or i don't know they're they're quite stupid and you just need to teach the very basic stuff just don't touch this don't press that don't talk about this it really is. It depends on the culture so yes so to summarize it it's very much depending on the culture because this security awareness program is the program to catch the culture upgrade the culture so it's very much depends on where the culture is right now and where do you do you think it should be. #00:44:21-2#

Severin Zimmermann: Oke thank you very much. Now i looking at the times do you have to leave at four o'clock or do you have some #00:44:31-1#

Experte 2: No no i i have more time i have more time. #00:44:33-4#

Severin Zimmermann: okay because #00:44:34-6#

Experte 2: I'll try to make it shorter don't worry. #00:44:36-6#

Severin Zimmermann: So just let me know a little bit earlier before you have to go so i can #00:44:42-9#

Experte 2: no no I'am Fine we have Timer. #00:44:45-0#

Severin Zimmermann: Okay perfect. Then i will just go on. Do you /. Or in your point of view, do you think there are ethical aspects you have to consider when

you're doing fishing awareness training? #00:45:06-6#

Experte 2: Ethical #00:45:15-8#

Severin Zimmermann: Yes #00:45:16-4#

Experte 2: Yes several um. Okay first one don't make your goings feel stupid more than than you have to okay. Sometimes it's very fun especially for security people that they like to hack things to make like attacks that are almost insulting you know. Sometimes also the messages you get they're quite insulting in also in the security in security courses /. Let's say and not only insulting but also let's say disappointing for no reason. For example there was a very big company in south in mexico i think it was and that CISO there did like a very mean trik to the employees so he did a fishing attack where the the email was all the employees of the companies are getting a free disney plus there was like a huge campaign in the country for disney plus that is coming to the country and they were promoting themselves everywhere and then this season made a fishing attack simulation where all the employees getting a free disney plus account actually everybody clicks it you it you just get automatically and they not only clicked it they also talked to their friends and made sure they click it so they get their disney plus account and some people even send it to their friends and family outside of the company to get that gone. So we can imagine that you know like every employee like we're happy or sad about this company but i was thinking okay well this company is not so bad it's giving me this disney plus and they're like oh man i hate this company it's like finally that i thought they did something good they did something bad. And like another thing in this category also pulls all these kind of attacks so you've got a bonus from HR click here to log in with your appropriate account or you've been promoted or i don't know what this is also like very mean. This is all in the category of promising you like a false gift other thing that are i'm not sure if it's yeah it is ethical slash legal already um when many of the Phishing attack emails are pretending to be other companies for example we are using /. if you're using the swiss government logo or they are available or a (unv., #00:47:56-8#) logo or fedex or i don't know or post it's not fun for post right so people thinking that /. For example if i'm sending an email to post hey dude we were at your office you missed your box click here to register it at the post website and you're just creating negativity towards their logo right. I mean it's not so many companies this is actually a gray area in in the business of security awareness and many companies do not allow that to fall. This is for the fishing attack simulation and yeah there are many there are many different attacks that really rely on your kindness. For example yeah i'm stuck without money can you help me and then they're just turning turning you to be more paranoid but maybe this is this is part of uh you know do you know the term tailgating? For example there was a company where the security team what they did is they just you know /. Everybody leaves the tram and then everybody just like goes into the building so they just ask the guy in front of me hey can you hold the door for a second i just want to go in don't want to pass my card because like five people came out of the

tram all of them and this person just hold the door for you it's just police nice nice human being and then they're just like uh-huh got you, you should have closed the door in the face of this person and not let him pass in. Well for that there are other physical solutions to solve that right only one person to pass at a time. But i mean all these kind of things now when it comes to the education itself some Phishing stories they are a little bit /. Not so politically correct right i mean like they're using race they're using sexuality they're using sexism a lot of let's say fun stuff like that. So because some of them are based on real stories that happen like that but it doesn't fit in the corporate setting yeah so for the ethical point of view there is also how ethical it is from the /. There is the old data collection aspect of the fishing training simulation there is data collection things that you write in tests also your grades and also /. Yeah it's all this kind of stuff some companies can use them not in a nice way hopefully they don't but i mean this is also theoretically can be one aspect of it. I don't know if you know that but security teams especially the ones that sit in the security operations center they have access whether they like it or not to all the raw information going in the conf. So theoretically they could read an email they could they /. They're used to have access to all this stuff and sometimes they can see all kind of stupid things people are writing and if you collect somebody's password i don't know if you know that but that's where it is considered pii personal information it's not a random sequence it can has the name of the person you love or whatever other important private stuff in you life. So yeah i think that is also how you use it. And especially because big parts these tools they're also rating giving a rating for every person let's say how security smart or stupid is he or she. #00:51:48-8#

Severin Zimmermann: Okay thank you the there were some very interesting aspects i definitely can use them. To answer your question yes i know this because i working in a smaller company but i'm working in a company in the IT as a engineer so i doing security but also infrastructure and client so i worked there since probably about 10 years so. I know some it and security things that are important. #00:52:33-6#

Experte 2: yeah no good it's important for this technical understanding. #00:52:37-5#

Severin Zimmermann: Just to answer your question and you know that. okay the next question is also about phishing testing so often it's used the click rate to argue about higher instances to do phishing simulations and do phishing education or to go on with phishing education. What do you think about using click rate as a argue again /. To higher positions to argue for phishing simulation or phishing training #00:53:19-5#

Experte 2: I mean as long as they know what they mean click rate means the first it should be done individually it's not like you can say ah the click rate in the company is lower than i stopped. First of all click rate has no meaning when you

don't know how difficult the attack is if the click rate of a person is very low it doesn't mean that he's protected against phishing it just means that now it's the time to sending harder attacks that's the only thing it says. If the click rates are too high for a very specific person it means maybe you're giving him too hard attacks maybe it's giving something simple and if he fails in that teach him how to learn it how to avoid it like for example after it clicks it then there is a screen explaining that. And then slowly increase the difficulty but the click rates by itself of the entire company or department simply nothing about the security of the company or no conclusion should be drawn from it not even a vague one. #00:54:30-8#

Severin Zimmermann: Okay thank you that's also my opinion and the opinions i got from other ones. #00:54:39-7#

Experte 2: It is important but you need to know it means it has meaning only in the possible context of one person and it it speaks more on the difficulty of the of the treating attacks instead rather than the person attacked. #00:54:54-5#

Severin Zimmermann: Yes thank you. Just take a look at the next question. #00:55:06-5#

Experte 2: You know i can also read them i have the the document in front of me if you want and read them and just answer them if it's easier for you? #00:55:14-3#

Severin Zimmermann: How you like. So the next question would be about technical precautions you do in companies you already mentioned it in the beginning do you want to add something else? #00:55:32-7#

Experte 2: Okay so there are no precautions actually so when you do simulation simulated Phishing there are no precautions they're just like stuff technical stuff that you do in order to to do that like you mentioned like uh whitelisting in a SPAM filter or a sender whitelisting and so on. Let's not forget it's usually not /. Yeah okay it's not usually classified as /. Do you see risks or opportunities in this, no i don't see any risks yeah i mean i think i told you in the beginning like you're just opening an attack vector theoretically you're /. What you're doing you're taking a server that is usually outside and you're trusting by whitelisting access to it. So you need to be, to make sure that it's as secure as any other server you keep this kind of access. On the other end you're also sending information there from your active directory you need to understand if this is something that is allowed in your country many companies in in europe will never allow their information to go to

the united states about all their employees and so on so that's that's what you need aboit it. #00:56:41-6#

Severin Zimmermann: Okay thank you the next question is tech technical security measures or technically security stuff you do to protect your company can create a false sense of trust on the employees because he thinks every email i get should be fine because we have security that /. such as spam filter and else that /. #00:57:19-7#

Experte 2: I mean there are many things like that for example. Let's say i cannot save any document from my from i don't know my email account into my computer so i'm thinking okay so even if somebody hacks my my email he will not be able to download any file which is not really about true. Another thing is the classic is all this antivirus all these scanners and so on and so every everything that you're open you're saving you have like some something in the email saying this file has been scanned blah blah blah and this can make people think sometimes it means it's safe and so on. For another typical let's say a classic classic case of false sense of security is that many companies they block the usage of usb drives in their computers right so you connect it and it doesn't talk but what we do at least our company we are selling um we're selling special usbs that actually when you connect them to the computer they pretend to be a mouse okay, or a keyboard and then the computer accept them and run the script that they're asking the computer to run. So companies where you think well my usb is protected i'll just try anyway you know so nobody educated that it shouldn't do that so and it's funny how many people fall for that also they know or maybe they should know that their computers don't work elsewhere um yeah i mean yeah security measure create full sense of security. And in general it's not only that sometimes you think okay there is a security measure on my email attachment so i'm sure they're secure. Please also the sense of like everything is overly secure i don't need to care about anything it's like i'm wearing a life jacket a life-saving jacket i don't care if i fall from the boat you know because it's so annoying but this thing gets into something else. So if you teach if you teach people exactly where they are secure and where they are not and this is also very very important. I mean for example if you're really let's say some companies they they're blocking any kind of macros in word files and so on sellsheets. But if you're doing that why send the employee to read 15 minutes about it just don't teach them that teach them some other stuff other important things for the employee that can be really bit dangerous #00:59:57-6#

Severin Zimmermann: Okay thank you. Then the next question is about platform so it's normal or today it's normal that users open their ob /. Check their emails on their mobile phone and maybe smartwatch or whatever tablet. So do you think it's important to integrate or consider this platform within /. #01:00:26-0#

Experte 2: I think you you skipped question 14 was it intentional or not? #01:00:34-1#

Severin Zimmermann: I did actually yes. Right sorry thank you for that so yeah do you think training is sufficient enough for users or should you implement additional security features like technical warnings #01:00:57-4#

Experte 2: Yes that that makes sense of course if you can give the person warnings in the place where then let's say in the place of the crime it's always very important especially in very /. For example you have emails that when you some companies add a notification hey be careful this email is from external sender or before you upload the file hey be careful don't upload sensitive files make sure you're just uploading. So this is not a bad thing to do i think as long as it's in a good place and not harming business it makes makes sense. #01:01:37-1#

Severin Zimmermann: Okay do you see maybe any risk to add some technical #01:01:45-7#

Experte 2: Yes so if you add them. It really needs to be in a good place like maybe you need to see this maybe once twice a day if you see that all the time you just become blind and don't care anymore. #01:01:57-9#

Severin Zimmermann: Okay thank you. So now the next question with the different platforms so do you think different platforms such as mobilephones tablets should be considered in the course material because it's often used to check the email or do you think you should focus on the desktop version of email client because it's the most used one #01:02:29-4#

Experte 2: you're asking two things actually the question here is about the training and the phishing attack simulation for phishing so for both of them both the phishing attack simulation and the training should be where the user is okay that's the idea. So if he's using tablets all the time or mobile defined why not use phishing attack simulations that which is mobile maybe not even just by email maybe by SMS or other means or if he's walking around scanning your codes all the time why don't you put a malicious code in the cafeteria for example it's another way to do it. In general training sound training let's say let's say the extensive training it's okay if it's a big course that it's better to do it with a mouse and drag and drop you play all the game properly this course is an extensive course you need to find 20 minutes sit with yourself and do it this in front of the computer but most of this especially small bite education should be mobile friendly because this is where people are and especially we want them to consume education in a way that is

comfortable for them so they can just /. They can see it as a let's say a break from work they can take their phone just sit on the sofa and just click through it um learn another one rather than the torture that every sit in front of them of the desktop and click around. #01:04:00-8#

Severin Zimmermann: Perfect thank you. The next question is about in internal reporting platform so you already mentioned that with some tools it already come a button in the outlook.Do you think that's important and it gains some chances or opportunities for the company or does it also gain some disadvantages. #01:04:40-9#

Experte 2: Okay so disadvantage it's like everything related to security for security of what is a security operation center. It's a place where a lot of noise signals from different machines different places all over the company is arriving different forms even from external sources like threat intelligence so the question is what do you do with it okay? It's very easy to collect all this information but if you're not doing anything with it you're just doing damage to yourself so you don't want to collect information you don't benefit from and once you do that you put this button and let the people click on it um it can create a lot of noise in big companies you will be bombarded with emails all the time. And what's the problem there are too many problems with it. Many many times people are using it as a not as a phishing button so that oh i think this is an attack i have to tell everybody about this attack no usually the case is that i don't know this is spam i don't know if it's a spam or phishing i don't care i use this people using it as a spam button okay so most of the time the stuff that they are proposing (unv., #01:05:53-3#) . You know for the benefits of course security operations center if they are building good playbooks good automation to filter out most of the cases then of course you can benefit from the benefits is that for example to like at least the one that we sell can use it and also others using a little better rating of the employee so for example an employee reported the phishing email part of our simulation then it gets positive points for that and is risk factor decreased um. Another important aspect of it first of all i mean it can help you to detect fishing attack right if you handle all the alerts correctly. The company third important aspect is that this button is always there so it reminds the user when he opens his mailbox there might be some phishing some email so like like an ad for that and yeah that's it i think. #01:07:04-9#

Severin Zimmermann: Perfect thank you i never thought about as a button just as a reminder but of course if you open the mail client and see this button you maybe got reminded of phishing that's a really good benefit you told me here thank you. The next question based on the questions we had in the beginning about external factors that influence phishing awareness training do you have anything else to to add or /. #01:07:47-6#

Experte 2: Yes i mean i don't know what you mean by external influences but /. I

mean you should see what are the the current trends in the industry right not in industry in the what are the risks to your company. For example after the war in ukraine there are a lot of phishing email shoot specific attacks that are asking you to donate for the ukraine and stuff like that so i know that poland was flooded with it and people they were like really in favor of the ukraine and it's funny because both Ukrainian and Russian hackers used it for their benefit. Another thing all these kind of crazy stressful sms is uh oh we have the vaccination for corona just click here on this sms send me all your private details put your credit card to save your your place in line and stuff like that so there are always things and you also need to learn about new attack vectors all the time there are always new stories. Right now there are /. It's nothing new right when everybody started working from home they got the phone call hi this is your IT this is /. All these kind of things that are just new that people are not used to so you need to understand what is the landscape what kind of attacks (unv., #01:09:16-7#). There are many things you cannot /. Yeah you just need to be keep your education up to date with everything and also when you talk about external you know it's not it's not necessarily that external so external to what? Like i said if you do any kind of transformation in the company whatever it is you need to have like a human education part of it when usually there is like a security aspect in almost everything you do almost everything you do. Okay another external influence is a big important topic these days is the supply chain security you're working with external people external companies delivering stuff this did not happen in the past and it's really important how you work with them and what they're doing. Maybe let's say we started to work with a big company that is building some big data center for us in the cloud and we need to teach our employees how to let them access or not give them access so now right now we have like these external developers that are experts in ais but i need to teach my development team not to give them access not to give them code you have to give them access to i don't know integration areas they should develop on the development areas. Yeah another external influences is actually changing regulations right. Changing regulation uh new privacy act or for example right now suddenly i don't know the american government decided not working with the russians anymore so now we need to update our education your russian team cannot talk to them or i don't know what or you cannot hire freelancers from russia through upwork or i don't know what all this kind of stuff needs to be considered.

Yeah more or less it's very broad i can speak to you tomorrow. #01:11:31-1#

Severin Zimmermann: Okay so thank you um the next question would be about external partners i think i already mentioned it also in the beginning. So do we want to add something maybe? #01:11:49-8#

Experte 2: Okay so i mean they need to /. Again when you work with external partners they need to deliver what you want to /. You need like the company i mean we do it as then we are many many times i am the external partners (unv., #01:12:06-8#). They don't know what your company needs you need to tell them what are your needs what are your priorities what is your culture now where do you want it to be and how do you. And what is their part in doing that i forget

they're just providing technical aspect of you're supposed to be leading the whole orchestra of all other measures that link art in the security awareness program so. But you need to make sure they don't have access to they don't have access, they don't collect and don't have access to more than what they have to of course that you get the service you want with all the dashboards all the reports whatever. I think it's a very good idea because there was a research recently just showing how much effort it takes to run and manage your own security awareness program within the company and there is a trend already in the recent years more and more companies they like to outsource it to other companies to do that for them, because usually they want to use their security officers let's say for real security work you know this is always sounds like oh this is like that, something that the HR department should do this is not why i became it's even sent courses and other stuff like that. Because it's also something very generic that can be done quite externally because of course so much internal knowledge to do it don't need to know any knowledge about our zone concept about you know about our platform you don't need to know anything we have people they're opening emails that's more or less what you need to do in order to train. I think it's if it makes sense financially and it makes sense for most things #01:13:58-2#

Severin Zimmermann: Perfect thank you so you told me you are working for the whole europe so that question is interesting for you especially do you think it makes a difference if i have a foreign partner to do phishing awareness training? #01:14:21-2#

Experte 2: Yeah i mean you want to have /. First i mean the main advantage of having let's say a partner to do your training is that this partner has a lot of experience doing other trainings for other companies like you so if he has /. If you are i don't know if you're a bank in switzerland and this person or i don't know just training the police in thailand so it's not really going to help him. If he was training i don't know other let's say um aldi in germany well that's actually cool. Well he's was training Migros in switzerland actually more relevant for you already local but oh it was like doing ZKB okay even better it's exactly like me just tell me what they did just do whatever they did for them most for me like so you won't do is also this aspect one also not understanding of only that but like not to not freak out your employees because your employees they are going to be exposed to the content and they many times they will say what the hell is this thing. Why are they writing this kind of text what you know so you want to have like company or content that has been running the country for quite some time like swiss people are used to do these courses and nobody's complaining it means it's a good thing but if you have a lot of content that maybe people were running it i don't know in the united states and there are people thought it's cool or funny uh then in switzerland then well /. Or for example or if you do something in switzerland which is considered here cool it might what you don't have experience in the united states and there they would consider you sexist very easily you could considerably consider sexist in the united states so it could be a problem so yeah that that answers your question? #01:16:17-0#

Severin Zimmermann: Yes #01:16:19-2#

Experte 2: And also another thing it's also the sense of the business culture every time you do business from people from another country like they don't delivering time in your swiss company you're curious to get your stuff on time and in some quality and there are some ethics. And let's say for example and i'm telling you as an israeli and swiss representive. When you're telling when a swiss person tells another swiss person i think you may want to consider that, it means you want that right? #01:16:52-9#

Severin Zimmermann: Yes #01:16:53-6#

Experte 2: In israel just people think you're just giving them advice and that you really don't care what they decide. So you you if you have like this cultural differences in business then this is (unv., #01:17:03-0#). And one thing you know it's one thing when you're having business with somebody and you have miscommunication it's another thing when you as a CICSO this is the only part /. So CISO's they are doing spend shit load of money on security stuff they buy firewalls web application firewall they build networks say these whatever they do spend a lot of money nobody the regular employee never exposed to any of that the regular employee never logging into the firewall the regular employee don't you know check the cables in the server room how they are connected and other (unv., #01:17:40-5#). The only part of the work that people see "the tip of the Iceberg" of the CISO that is up outside of the water that all the employees see is including the CEO is the security awareness program this is the only thing the CISO is doing that all the employees can come and feel and see and touch and lick okay it's the only thing that it's the only thing that he cooks that they eat. Okay and if this is crap if you're getting them lunch from vietnam they might not like it this is what they think about your entire work and this is what they think about your entire security this is how much they care also about the security itself. So this is super important this is why you want it to be like super on point this is why there are so many even CISO's that are completely obsessed with the aesthetics of the programs beyond the content itself and it's very hard to do it for instance. #01:18:39-6#

Severin Zimmermann: Yes okay that makes definitely sense. The next question do you know /.Or from your point of view do you know any legal aspects that should be considered in phishing awareness training? #01:18:56-8#

Experte 2: Yes i mentioned them here and there. So again the first again the first one is that in some places you have to notify the employees before you do a phishing awareness training and in some cases after the phishing like immediately after they click or not click the email you may have to tell them that this was

a phishing email. If you're using external logo you must in some cases some some companies really a must but it is a legal issue we need to consider that's what you said by what do you need to consider should they use external logos or not. Any kind of promises that you're telling an employer any kinds of things that can be /. As it as a corporate you don't have then the privilege of a dick talker saying no this was just a prank no no no you cannot slap somebody in the face and then say it's just a prank so you need to understand like what you're doing when it comes to everything also the information you collect. So i mean there are several aspects right so let's say over the phishing attacks don't mess up don't insult don't be sexist don't do don't use um don't hurt other companies or other businesses. Another aspect of course also with your clients right if you're using some names of your clients you can get your employees to do that. Another legal aspect yeah /. Okay so this is when it starts to the phishing attack to the education we told you it's it can be problematic if you have like all kinds of funny content that shouldn't be there also by the way uh also content that was copied from other places so you need to make sure that the company that is using it also the pictures and so on that we have the ability to use the content. What else? Yeah i think that's it mostly that's it mostly. And one thing you know sometimes employees /. Another let's say family of legal aspect is the actions that your employees might do you know for example if you if you're saying one of your big clients has been i don't some of your attack stories about something that happened to one of your big clients and then it makes your employee completely freak out and call your clients and tell you stuff that he shouldn't maybe it's not even illegal for him to tell him that then you'd also be aware of that like not trick your employees to move or push them to the illegal stuff. I Think that's it (unv., #01:22:16-1#). And also about around their data privacy and grade privacy and so on. #01:22:22-2#

Severin Zimmermann: Rright you already mentioned that earlier. No i think that's very good like that so i would ask you the next question do you know any parties that have to be informed mandatory be informed while using phishing tests or simulated phishing attacks such as government other institutions hosert or registrar #01:22:55-1#

Experte 2: Not really. So i mean they when you're using /. Okay it depends right and i don't know anybody that has to be in informed legally but i mean we are using some cloud provider to run our phishing platform and they very often they receive complaints or reports oh they say that we see a lot of phishing activities all their the machines that are like reporting all the time there are some phishing activities that our servers are performing phishing but our behavior looks like phishing um so obviously we tell them. Many times let's say smart employees they report our website let's say our fake website because they don't know it's a phishing they report it to google so sometimes we have to tell google this is not a this is not a phishing domain but this this can be solved very easily because for almost every attack you just register new domains (unv., #01:24:05-8#). Also by the way when you're doing the phishing attack simulation you don't we don't make it over weeks because usually after three days several people already reported the website and that's it it blacklisted and then the other other employees when they get it they already get like a warning from the chrome browser. Let's say you

know Melanie? #01:24:34-6#

Severin Zimmermann: Yes. #01:24:36-2#

Experte 2: So one of our phishing attack templates had Melanie in it and one of the one of the employees that received the phishing attack simulation reported to melanie that we are using their logo they got really pissed. So we removed this attack anyway but i think in general if you're using any logo of any organization you should tell them. But yeah no other parties that i know of maybe internal right. #01:25:05-7#

Severin Zimmermann: So you say it makes sense to inform certain parties or certain institutions because they block you or they get requests from from your employees #01:25:24-4#

Experte 2: (unv., #01:25:24-8#) To be honest us we only report to the cloud provider where we /. But we do not know telling about every campaign we just tell them this is a phishing attack server don't pay attention if you see some warnings or regards from other people in the company performing it and practically besides this and the company itself that receives it nobody needs to know about. #01:25:52-1#

Severin Zimmermann: Okay #01:25:53-3#

Experte 2: It's none of their business. #01:25:55-1#

Severin Zimmermann: Okay thank you so. The last question is do you know any reporting requirements if you got a victim of a phishing attack so of a real phishing attack not a test? #01:26:10-1#

Experte 2: I don't think any company is required to do that by law no i don't think there are any. #01:26:19-0#

Severin Zimmermann: Okay so now just my last two administrative questions do you think there are still points open or remain open that we haven't covered or do

we want to say anything else about phishing awareness training that i didn't mention? #01:26:44-2#

Experte 2: Like i said in the end it's you call it phishing awareness but we're talking about security awareness program the tests are about phishing but the education is about a wide range of topics and also this program is education program supposed to be part of an awareness program that could sell the entire security changing the security culture and i discussed with you about many let's say advanced things tailoring education and tests for specific employees and so on it's very important for companies like to understand where they stand now in the maturity level and decide where they want to do what i said is very very advanced it's the top but maybe it's okay to understand okay right now we're just taking the compliance box this year we want to get one step forward that maybe in two years we go and do all this fun stuff that woody is talking about that also maybe cost a bit too much and then takes too much of our time that we don't have now. So this is my take here it's not about any phishing program but call it security always because it is what it is and one last thing in many companies this it really looks like oh this is just a task everybody can do well that's not some stupid generic education we do for the employees and they don't waste the time let's say smart people just put somebody that has no education what so ever to do that. Because they want to have like that the smart people to manage that but not only that it's not like that you need like a really crazy good pentester to run this it's a human thing so you need also a person that understands people that has knowledge and education to do that and this is an aspect that many people are missing. Yeah that's maybe one of those additional points there #01:29:08-1#

Severin Zimmermann: Okay thank you very much i totally agree with you so it's not just about phishing awareness so it's way more with the other topics in security awareness i can't cover all that stuff in my bachelor thesis because it's just too much but thank you for this input um my last question is i will do some further interviews maybe i will get some new aspects of things i didn't mention /. Or i will figure out some other things aspects that i haven't covered yet can i contact you if i get some other aspects i want to know your opinion in it? #01:29:56-8#

Experte 2: Yes you can #01:29:58-8#

Severin Zimmermann: Perfect thank you so i will stop the recording now #01:30:03-4#

F Transkript Experten-Interview Experte 3

Administratives	
Interview Datum	13.04.2023
Interview-Partner	Experte 3
Arbeitgeber	ZHAW
Aufnahme OK?	JA
Anonymisierung Daten?	Nein

Severin Zimmermann: Sehr gut, das müsste jetzt soweit auch laufen. Darf ich dich als erstes bitte, dich kurz vorzustellen und deine Position und Funktion zu nennen? #00:00:17-9#

Experte 3: Ja, mein Name ist Experte 3. Ich bin als ICT Security Engineer unterwegs. An der ZHAW bin ich seit zwölf Jahren. Habe gestartet Business Applications and Project Management, Technische Projektleitung, Applikationsbetreuung bis Richtung Netzwerk und bin jetzt seit fast vier Jahren eben in der Rolle als ICT Security Engineer an der ZHAW unterwegs. Versuche mich einzubringen in diversen Architekturthemen, also nicht nur was Security angeht, sondern allgemein auch ein bisschen die Strategie mit einzuwirken. Ja, das ist so meine Rolle. #00:01:08-2#

Severin Zimmermann: Sehr schön. Dann die nächste Frage. Hattest du bereits Erfahrungen mit Phishing Angriffen? Wurdest vielleicht selber einmal Opfer oder einer deiner Kollegen? #00:01:18-0#

Experte 3: Um Opfer zu werden, hat es zum Glück für die Angreifer noch nicht gereicht. Aber trotz technischem Fachwissen und immer in einem wachsamen Auge ist jeder der Gefahr ausgesetzt. Das muss man sich einfach bewusst sein. Wenn gewisse Konstellationen zusammenkommen, ist jeder gefährdet. Da darf man sich nicht von frei machen. Das wird der größte Fehler, den man tun kann. So Phishing geht mich nichts an nach dem Motto. Und ja, ich kam stark damit in Kontakt eben auch über ein Forschungsprojekt an der ZHAW. Das OptiPhish Projekt. Ich weiß nicht, ob dir das so weit "geläufig" ist. Ich denke schon, oder? #00:01:58-5#

Severin Zimmermann: Ja, also ich hatte /. Oder das dient als Grundlage auch.

Also da wurde ja noch ein Datensatz daraus generiert. #00:02:08-0#

Experte 3: Ja #00:02:08-5#

Severin Zimmermann: Diesen werde ich auch in meiner Bachelorarbeit auswerten. Und von daher stammen /. Oder habe ich auch deine Kontaktdaten erhalten in diesem Zusammenhang. #00:02:18-7#

Experte 3: Ja, tipptopp. Ja, da war ich halt stark involviert und man merkt halt dort verschiedene Faktoren, die einfach mitspielen. Aber ich denke, da geben wir in den Fragen nachher gezielter drauf einem. #00:02:32-5#

Severin Zimmermann: Sehr gut. In dem Fall, du hast es jetzt schon erwähnt, OptiPhish Projekt, das Phishing Awareness Training Projekt, sag ich jetzt mal. Also hast du auch bereits Erfahrungen mit Phishing Awareness Training? #00:02:43-6#

Experte 3: Jawohl. #00:02:44-3#

Severin Zimmermann: Sehr gut. Dann würden wir zu den Hauptfragen überkommen. Die erste wäre hier: Sind dir positive Aspekte bekannt, die im Rahmen eines Phishing Awareness Trainings resultieren können? #00:02:58-8#

Experte 3: Ja, am Schluss geht es ja immer um Risikominderung, oder? Und das ist die Frage, wie viel Geld nimmt man in die Hand, um wie viel Risiko zu mindern? Im Sicherheitsbereich allgemein, aber beim Fishing im Speziellen. Es ist natürlich alles mit Kosten verbunden. Also positive Aspekte sind wirklich gegeben. Wir haben sehr gute Rückmeldungen bekommen. Dankbare Endanwender, die gesagt haben, ja danke, dass ihr uns das mal zeigt, dass ihr uns darauf hinweist. Ja, das ist es eigentlich schon. Die Negativseite ist deine nächste Frage, oder? Magst du dich stellen? #00:03:40-2#

Severin Zimmermann: Du darfst auch direkt drauf eingehen. #00:03:42-8#

Experte 3: Okay, die negative Seite ist halt eben, es bedeutet Aufwand. Es be-

deutet organisatorisch Aufwand. Es bedeutet Aufwand auf der technischen Implementationsseite, in der Betriebsseite. Inzidenz, die auftauchen. Also Inzidenzvolumen war sehr hoch bei uns. Wir haben wirklich uns von unserer Anstellung müssen Ressourcen freischaufeln vorher, vorgängig. Dann läuft man in Thematiken rein. Wie informiere ich den Service-Desk, dass wir das machen? Informieren wir nicht. Es sind viele solche Prozesse, die man vorher sich gut überlegen muss, wie man das abbildet. Und dann ein wesentlicher Faktor ist einfach die Masse. Im OptiPhish Projekt haben wir natürlich, dabei eine gewisse Datenbasis gebraucht haben gerade was so Machine Learning angeht. Mit Aussagekraft geht nur über Datenbasis, über eine Menge. Haben wir recht viele Kampagnen gefahren und die Leute waren, drücken wir es aus, dezent angenervt irgendwann. #00:04:42-9#

Severin Zimmermann: Ja, das habe ich auch schon gehört. Das kann ich auch durchaus verstehen. Du hast jetzt organisatorische, aber auch technische Aspekte bereits genannt. Vielleicht hier kurz die Frage, möchtest du zu diesen zwei Punkten noch etwas ergänzen? Also wir kommen später sowieso nochmals mit Detail Fragen darauf zu, aber jetzt im ersten Teil habe ich etwas vergessen. #00:05:09-0#

Experte 3: Nein, ich glaube dann reicht das auf der "Flughöhe" jetzt erst einmal und du kannst nachher noch mal gezielt darauf eingehen. #00:05:15-3#

Severin Zimmermann: Sehr gut. Dann, was du bis jetzt weniger genannt hast, sind Umfeldfaktoren. Also seien das mit externen Partnern, seien das mit der Regierung etc., sind dir hier Aspekte bekannt, die beachtet werden sollten? #00:05:30-6#

Experte 3: Ja, auf jeden Fall. Es gibt einmal den Faktor, man versucht ja gerne, um Phishing Awareness zu betreiben, erstmal in Anführungszeichen die Mail so auszurollen, dass jemand drauf reinfällt. Dann ist man natürlich sehr geneigt dazu, Logos zu verwenden, die Hersteller draußen haben und dann begibt man sich sofort in eine rechtliche Grauzone. Da muss man also wirklich aufpassen, was man dort darf und nicht darf. Diese Abklärungen sind wichtig, Einwilligung von eventuell Einholen draußen. Das zweite ist, Phishing Kampagnen, die durchzuführen, denkt man so im eigenen Unternehmen, ja, kann ich tun, kein Problem, ist ja das eigene Unternehmen, es ist abgesegnet bis oben hin. Auch hier ein klares Jein, man sollte diese Phishing Kampagnen ganz klar anmelden. Wir haben hier offizielle Instanzen dazu, Melanie hieß es früher und jetzt ist mir das Kurzzeichen wieder ein Fall. #00:06:35-8#

Severin Zimmermann: NCSC heißt das. #00:06:38-2#

Experte 3: Ja, NCSC genau, National Security Center Swiss, oder Switzerland. Genau, dort sollte man die Kampagnen ganz klar anmelden. Es ist auch verständlich, denn viele, die irgendwo in einem Unternehmen nur temporär angestellt sind oder eben nur zu einem gewissen Beschäftigungsgrad, die leiten ihre Mails weiter, die kommen also irgendwo an, die denken, was ist das hier und melden das einfach an der offiziellen Stelle und die offizielle Stelle bewertet das und sagt, ja, ist das jetzt SPAM, das sieht ja wirklich ganz verrückt aus, was da ankommt und deshalb ist es wichtig, die Themen einfach vorher anzumelden. Ja, das sind so die zwei Dinge, die mir jetzt da in den Sinn kommen, die wesentlich sind. #00:07:26-4#

Severin Zimmermann: Sehr gut, vielen Dank für den ersten Überblick. Jetzt habe ich das Frage, wobei wir haben jetzt schon alles angesprochen, ob dir noch andere jetzt in diesen Bereichen Aspekten bekannt sind, möchtest du noch etwas ausführen? Ansonsten würden wir einfach zu den Detailfragen übergehen. #00:07:41-4#

Experte 3: Ja, ich denke, wir gehen zu den Detailfragen und falls mir nachher noch was einfällt kann ich schon noch mal zurückspringen. #00:07:48-7#

Severin Zimmermann: Selbstverständlich. Gut, die Detailfragen, also jetzt werden zuerst /. Oder ich werde zuerst auf organisatorische Punkte eingehen, danach etwas auf technische und dann nochmals Umfeld. Zum Schluss fallen dann noch administrative Fragen, aber ich würde sagen, wir legen los mit den organisatorischen und zwar wird bei Phishing Awareness Trainings oft gesagt, dass man sie auf User abstimmen soll, also auf bestimmte User Gruppen, auf ihr Verhalten, ihre emotionale Lage. Da gibt es unterschiedliche Personen mit ihrer Risikobereitschaft? Bist du der Meinung, Phishing Awareness Training sollten so personalisiert werden? #00:08:38-3#

Experte 3: Ja, gute Frage. Ich denke, man sollte erstmal generisch ausrollen und generische Kampagnen gegenüber jedem, also jeder Zielgruppe. Einen Rückschlussziehen auf einen Endanwender kann zum Teil auch kritisch werden. Nehmen wir als Beispiel, wir haben eine Authentisierungsmaske, der gibt seine echten Credentials ein. Also hier ist auch, Klammer auf, wichtig, was man loggen darf und ob man gewisse Dinge opfusszieren sollte. Das ist auch ein wichtiges Thema. Aber ja, Ich bin auch der Meinung, dass man es gezielt machen sollte. Im Sinne von einfache Kampagnen, mittelschwere Kampagnen, schwere Kampagnen, um es mal irgendwo zu klassifizieren und zu schauen, okay, der Benutzer hat jetzt siebenmal die einfachen Kampagnen kapiert, dann bringt es kaum mehr was, ihm häufig einfache Kampagnen zukommen zu lassen. Dann sollte man wirklich auf den nächsten Level gehen. Und das ist eine Geschichte, die Schwierigkeit oder wie gut das Phishing gemacht ist, das kann man dann eben

nochmal steuern, um auch den Endanwender am Ende nicht zu nerven. Das ist ein Faktor und der will ja auch eventuell noch was Neues lernen und nicht immer nur dasselbe. Sagt, hey, das habe ich jetzt schon so oft gesehen, das brauche ich nicht mehr. Das ist das eine. Und die soziale Komponente, das ist das, was ich gerade in der Einleitung schon angesprochen habe, die ist immens. Wenn du gestern irgendein Geschäft getätigt hast, irgendwas bestellt hast im Internet oder auch außerhalb und heute kommt eine E-Mail dazu, die einfach im Kopf den Link herstellt, dann ist die Gefahr hoch. Ah ja, das ist ja trustworthy, ich klick's einfach an. Also die Wachsamkeit und Achtsamkeit, die ist dann einfach per se mal unten und das sind so Faktoren, die sollte man schon beachten und auch spezifisch austesten. Ebenso, ich sage jetzt mal, Finanzabteilung, die bekommen andere Mails am Tag als jemand in der IT, als Techniker. Auch das ist so ein Thema, wo man wirklich individuell drauf eingehen kann. Und die dritte Sache ist einfach Anstehendeereignisse, Weihnachtsferien stehen an, alles sind unter Druck, Jahresabschlüsse, solche typischen Termine. Und dann kommt doch schnell eine Mail vom Chef, du, ich brauche ganz dringend diese Unterlagen, ich finde sie aber nicht, kannst du mal hier auf den Link klicken und schauen. Ja, oder dann nimm doch schnell am Meeting teil, ganz kritisch, bevor du in Ferien gehst. Das sind so Faktoren, die man da nicht unterschätzen darf. Also ich bin, ja, zwiegespalten. Man sollte es generisch behalten, immer wieder, aber auch auf Zielgruppen eingehen. #00:11:37-7#

Severin Zimmermann: Sehr gut, vielen Dank. Dann vielleicht ergänzend, Entschuldigung, siehst du Chancen und Risiken, die sich ergeben können, wenn ich jetzt eben ein

User Awareness Training personalisiere und auf Zielgruppen abstimme und nicht einfach nur generisch? #00:11:57-3#

Experte 3: Ja, also Risiko ist natürlich in dem Sinne Datenschutztechnik, dass man diese Seiten betrachten muss und man darf einem Mitarbeiter, also den Mitarbeitern nicht das Gefühl geben, man will sie hinter das Licht führen oder sie bloß stellen. Das darf nie der Fall sein. Das muss man ganz klar vermitteln. Ansonsten, wie gesagt, spreche ich mich für die Mischform aus. #00:12:24-4#

Severin Zimmermann: Ja gut, vielen Dank. Dann die nächste Frage betrifft das Material oder die Durchführung selber von der Schulung. Also es gibt ja unzählige Möglichkeiten, um ein Phishing Awareness Training durchzuführen. Sei das embedded mit ich versende Phishing Mails und wenn jemand klickt, bekommt er das Schulungsmaterial oder wird zur Schulung aufgeboten oder präventiv. Das Ganze kann wiederum in unterschiedliche Formen vermittelt werden, Gamification, Video, Fact Sheets, um ein paar Beispiele zu nennen. Auch die Zustellung selber mache ich es online, führe ich Schulungen in Klassenräumen durch etc. Und der letzte Punkt auch, also es sind sehr viele Punkte, ich weiß informiere ich meine Mitarbeiter, dass ich eine eben bei embedded Training ein Fishing Simu-

lation durchführe oder nicht. Wie stehst du dem gegenüber? Sollten solche Trainings /. Oder wie sollten solche Trainings aufgebaut sein beziehungsweise siehst du hier Vorteile und Chancen von gewissen Trainings? #00:13:35-4#

Experte 3: Alle Varianten durchführen. Das ist ganz klar meine Meinung. Es muss Abwechslung rein, es darf nicht stupide werden. Also auch in der Front oder halt jetzt online mal das ganze demonstrieren, gewisse Fälle aufzeigen, was kann denn passieren, was passiert im Hintergrund vielleicht für auch die vielleicht etwas technisch versierteren Benutzer. Es darf nicht zu tief reingehen, dass es alle andere abhängt, aber das macht auf jeden Fall Sinn. Aber wichtig ist, dass die Endbenutzer Erfahrung einfach ist. Es muss wirklich aus meiner Sicht ein Portal sein, wo alles zusammenläuft. Es darf keine Hürden haben, sich dort kompliziert anzumelden. Ja, dann kommt einfach der Faktor, ja jetzt habe ich keine Zeit dazu, ich habe andere Aufgaben zu erledigen. Muss also erinnert werden, bitte macht doch noch so ein Training. Und wichtig ist einfach, dass man auch Rückmeldungen für die Druchführenden gibt. Also so eine Portalseite ist eigentlich was Ideales, dass man auch sieht, hey der hat jetzt ein Training durchgeführt oder hat es begonnen. Diese Art von Training in Video anschauen im Spiel im Sinne von Game oder einem Quiz ist auch schön. Muss man halt sehen, warum brechen die Hälfte jetzt einfach ab "mittendrin". Muss man sich dahinter fragen, was war der Grund. Und das funktioniert eben nur, wenn die Durchführenden auch eine Rückmeldung bekommen. Das geht eigentlich nur über ein Portal. Risiken sehe ich eigentlich dort wenig. Verlieren kann man nicht. Das einzige Risiko ist halt immer wieder, dass die Leute genervt werden, dass sie sagen, oh nein, das ist mir jetzt wirklich to much. Hört doch bitte mal auf damit. Ich habe es kapiert. Die Erfahrungszeit, sie haben es im Kopf kopiert und stumpfen ab und klicken dann beim nächsten Mal doch drauf. Das ist einfach das Thema, diese wiederkehrende Durchführung von solchen Kampagnen und auch von den Trainings ist einfach wichtig, um einfach in den Köpfen wieder bewusst zu machen, oh ja, das kann uns böse treffen. Vielleicht sollte man auch die Auswirkungen zeigen, was passieren kann, wenn man so etwas tut, was für Impact das hat, haben kann auf ein Unternehmen. Das ist nicht ganz zu unterschätzen. Ja, Chancen, die Chancen sind einfach, wie gesagt, es geht immer um Risikominimierung. #00:16:12-9#

Severin Zimmermann: Aber so, wie ich das jetzt verstanden habe, haben auch eigentlich unterschiedliche Varianten, dass der Benutzer oder der Einbenutzer nicht gelangweilt wird und so auch wirklich das Training durchführt und nicht einfach auch nicht schon wieder das uns beiseitelegt. #00:16:27-7#

Experte 3: Genau, auch die Frequenz ist so ein bisschen Thema, wenn man nur, ich sag jetz mal dreimal im Quartal, vielleicht ist es spannend, nicht nur einmal im Monat zu machen und der Endanwender weiß dann, oh ja, ich war jetzt einmal im Monat dran, jetzt bekomme ich keine Mail mehr, dass es auch wirklich variiert, dass es dreimal in einem Monat sein kann und dann in den nächsten beiden nicht zum Beispiel. Also auch da muss man ein bisschen Flexibilität zeigen und einfach auf das Real-World-Szenario eingehen. #00:17:02-0#

Severin Zimmermann: Sehr gut, vielen Dank. Dann Hier habe ich noch eine ergänzende Frage und zwar ist es sehr oft umstritten, ob das IT-Personal informiert werden soll und zwar Grund ist hier, dass IT-Personal oft auch als genauso anfällig gilt wie jeder andere auch und halt der Schulungseffekt minimiert wird, wenn man diese vorgängig informiert weil /. Also besonders bei Embedded Training, weil sie wissen und sind unter Umständen übervorsichtig und darum nicht klicken und so gar nicht zur Schulung aufgeboten werden. Was denkst du darüber? Sollte das IT-Personal informiert werden oder sollte man diese "im dunkel stehen lassen"? #00:17:40-4#

Experte 3: Informiert werden über die Schulungen oder informiert werden über die Durchführung von Kampagnen? #00:17:47-9#

Severin Zimmermann: Die Durchführung von Kampagnen, jetzt spezifisch. #00:17:50-7#

Experte 3: Okay, wir hatten das Thema bei uns. Ich sage jetzt mal, IT sollte ein gewisses Level haben. Klar, sollte auf einfache Dinge nicht mehr reinfallen. Aber wie schon erwähnt, wenn die Konstellation da ist, dann versagt das Gehirn bzw. die Hemmschwelle, was einfach anzuklicken, die sinkt. Das muss man sich wirklich zu zwingen. Also ich würde das IT-Personal per se nicht ausschließen. Die Frage ist allerdings, muss ich vielleicht doch eine Hand voll involvieren? Weil eben Incidentaufkommen, was passieren kann und so weiter. Das sind so Themen. Für uns war der Hauptfaktor mehr fernab von der ICT, der Service Desk. Weil einer der größten Einfallskanäle, was Fishing angeht, ist eben der Service Desk. Da kommen ja die "mannigfaltigsten" Anfragen an. Von die Toilette ist verstopft bis zu keine Ahnung und das bis zum konkreten IT-Problem. Und die müssen wirklich eigentlich jede Mail hinterfragen, was steckt denn da dahinter. Und deshalb Service Desk schließen wir auch ungern aus, haben aber in der Vergangenheit es so gehandhabt, dass wir zumindest den Vorgesetzten informiert haben, dass da was läuft. Also falls dann irgendwie Unmut, ob der Menge oder komischen Anfragen entsteht in seinem Team, dass er dann eingreifen kann. #00:19:21-1#

Severin Zimmermann: Okay, sehr gut, vielen Dank. Dann die nächste Frage, die betrifft die Cybersicherheitskultur. Etwas schwierig auszulegen, aber grundsätzlich gilt die Cybersicherheitskultur als relativ wichtig, also sprich wie Personen auf Sicherheitsvorfälle reagieren. Reden sie miteinander, wenn sie ein komisches Mail erhalten. Bevor sie jetzt etwas anklicken, reden sie mit ihrem Kollegen oder klicken sie es einfach an, um zu schauen. Spielt deiner Meinung nach die Cybersicherheitskultur beim Phishing Awareness eine Rolle und sollte das im auf /. oder sollte das mit dem Phishing Awareness auch unter Umständen aufgebaut werden oder inkludiert werden? #00:20:10-9#

Experte 3: Ja, ich sag mal so, Phishing Awareness Training kann natürlich zum Aufbau einer solchen Kultur beitragen. Ein wichtiger Punkt ist, wie eben angesprochen, dass man hier keinen an den Pranger stellt, nur weil er geklickt hat. Oder ein sehr technisch basierter Benutzer, der kann ja auch hingehen, erkennt das als Phishing Awareness Kampagne und schaut sich trotzdem mal an. Also auch bei den Rückschlüssen muss man aufpassen, was ist denn ein false positive. Man darf nicht alles für "bare Münzen nehmen", was dort die Datenbasis dann hergibt. Und ja, für mich ist die Cybersicherheitskultur höher anzusiedeln, weil das ist eine Grundaltung, die man entwickelt überhaupt zur Sicherheit. Wie gehe ich mit Dingen um und Phishing Awareness ist ein Unterbereich von was spezielles, was dazu beitragen kann. Aber mir wäre jetzt die allgemeine Cybersicherheitskultur, hey, da hat einer sein Passwort irgendwo hingeklebt, jetzt als blödes Beispiel, oder der sperrt das Büro nie ab und da liegen doch kritische Unterlagen rum und so was. Dass man auf so was ein Auge hat, finde ich einfach wichtiger als das punktuelle Thema Phishing Awareness. #00:21:27-9#

Severin Zimmermann: Okay, vielen Dank. Dann ethische Aspekte, sind dir ethische Aspekte bekannte im Rahmen einer Phishing Awareness /. Oder bei einer Durchführung von Phishing Awareness Trainings beachtet werden sollten? #00:21:42-8#

Experte 3: Ja. Aber auch das ist eigentlich ein generisches Thema, was man sonst auch immer hat. Was ist meine Adressatengruppe? Wie kommuniziere ich mit der? Man muss sich hier vorstellen, wir haben ja vom Studierenden bis zum Mitarbeiter, bis zum Dozenten, Einzelentschädiger, Weiterbildner es wird ja letztendlich sehr unterschiedliche Personenkreiser werden angeschrieben, die da noch aus ganz anderen Fakultäten kommen. Ich meine, Department Gesundheit, Beispiel Hebamme, die sind vielleicht, das kann man "auf den Schlips treten", aber die sind vielleicht nicht ganz so IT-affin wie die Informatikstudierenden. Das ist einfach so. Man muss sich bewusst machen, wie kommuniziere ich dort, dass man wirklich eine Sprache findet, die von jedem verstanden wird, aber für keinen despektierlich ist. Das ist das eine. Und ja was noch zu beachten ist, dass man echt wirklich überlegt bei jeder Kampagne, die man macht, komme ich da mit diesem Thema einem nicht zu nah. Ich meine, das Thema schwarzer Humor, der eine der nimts, ja der lacht drüber oder kann drüber lachen, obwohl er die Ernsthaftigkeit versteht und der andere, der fühlt sich wirklich angegriffen. Und so ist es in dem Fall auch. Man muss wirklich überdenken, wie weit kann ich gehen? #00:23:15-1#

Severin Zimmermann: Okay, also wirklich bei den Phishing Simulationen, die Mail die man rauslässt, aber auch beim Schulungsmaterial, wen spreche ich an und wie könnte es vom Gegenüber empfunden werden, sich sicher das /. Oder sich sicher darüber Gedanken machen und entsprechend darauf eingehen. #00:23:32-7#

Experte 3: Genau, das ist jetzt bei den, du sprichst jetzt die Awareness Kampagnen an, aber noch wichtiger, wenn du die Phishing Mail rauslässt, dass du da keine Grenze übertrittst. #00:23:43-9#

Severin Zimmermann: Okay, sehr gut, vielen Dank. Dann das nächste Thema, du hast es vorhin kurz angesprochen mit dem Fals Positives und zwar Klickraten. Wie stehst du generell gegenüber Klickraten? #00:23:58-3#

Experte 3: Die "Eierlegendevollmilchsau" als Tool fehlt mir einfach da noch und man hat auch technische Limitierungen einfach, die es nicht ermöglichen, das Ganze auf die Datenbasis wirklich voll und ganz vertraulich zu machen. Man muss also wirklich die Daten, die man nachher rauszieht, hinterfragen. Kann das sein? Passt das? Ja, deshalb eine gewisse Datenmenge für eine Analyse ist schon mal ein Punkt. Ich mache ein Beispiel, die hatten beim OptiPhish Projekt Leute, die haben 5-6 mal auf den Link geklickt. Jetzt kann sich, ne man kann nicht man muss sich fragen, warum. Jemand hat auf den Phishing Link geklickt und ist darauf reingefallen und denkt nachher, irgendwas war doch da komisch. Komm, ich ruf's noch mal auf und guck's mir noch mal an. Das ist so eine Möglichkeit. Die andere Möglichkeit ist eben der technisch versierte, der sagt, du, ich habe das angeklickt, mir ist das bewusst, jetzt wollte ich mir noch ein bisschen Analyse machen, mach mir noch einen Spaß, schau mir noch ein bisschen rum und ruf das halt mehrfach auf. Oder jemand, der sagt, er zeigt zum Arbeitskollegen, guck mal hier, das da habe ich angeklickt, was hältst du davon? Er will es halt noch mal zeigen. Und ja, das ist jetzt ein konkreter Fall oder ein konkreter Bereich, wo man halt mehrfach auf solche Links klickt. Das ist die Frage. Auch bei der Eingabe von Credentials. Ich meine, man hat gewisse Passwortrichtlinien, man könnte ja an dem Passwort sehen, hat da jetzt einfach jemand aus Spaß mal probiert, was passiert denn da oder hat wirklich jemand möglicherweise ein Passwort eingegeben. Und Opfusszierung von dem Passwort hat man eben schon angesprochen, finde ich ganz wichtig, dass niemand an das vollständige Passwort zumindest gelangt. Idealerweise schaut man sich diese Themen gar nicht an. #00:25:52-6#

Severin Zimmermann: Sehr gut, dann vielleicht hier auch noch ergänzend, oft werden jetzt Klickraten als Rechtfertigung gegenüber höheren Instanzen verwendet, um ein Phishing Awareness durchzuführen, oder vorzuführen. Wie stehst du dem gegenüber? #00:26:10-0#

Experte 3: Das Problem ist die Vergleichbarkeit. Wenn wir jetzt eine Phishing Awareness Kampagne durchführen und dann, sagen wir mal, über ein paar Monate und wir messen die Klickrate jetzt userspezifisch, oder auch Benutzergruppen spezifisch, Monat für Monat und vergleichen die. Dann werden wir vermutlich sehen, die Raten sinken. Aber wie eben gesagt, haben wir vorher fünf einfache

Kampagnen gefahren und jetzt waren wir fünf schwere. Das heißt, die Vergleichbarkeit, die müsste eigentlich immer gegeben sein. Das ist schwierig. Ich denke, was man einfach machen muss, ist die Wiederholung. Also mal aussetzende Zeit lang und es dann wieder machen, um wieder das Bewusstsein zu schaffen, oh ja, da ist hier noch irgendwas. Oder wenn es neue Angriffsvektoren gibt, die vermehrt auf dem Markt sind, dass man die immer noch mal versucht zu trainieren. Also eine effektive Methode, um den Return of Investment zu gerechtfertigen, ist für mich die Klickrate nicht. #00:27:15-7#

Severin Zimmermann: Okay, also spricht, es muss im Kontext angeschaut werden. Wie war die Schwierigkeit? #00:27:22-9#

Experte 3: Ja #00:27:24-5#

Severin Zimmermann: War vielleicht das Thema auch einfach gerade aktuell und deshalb schwieriger oder solche Dinge? #00:27:34-0#

Experte 3: Genau, es ist einfach, wie ich sage mal, bewusst und auch unbewusst manipulierbar. Die Vergleichbarkeit hierherzustellen ist extrem schwer. #00:27:42-9#

Severin Zimmermann: Okay, sehr gut, danke. Dann kommen wir bereits zu den technischen Aspekten. Und zwar wir beim Phishing Awareness Training, besonders bei Simulation, öftermals Freischaltungen gemacht auf der Firewall oder auf anderen Systemen, Whitelisting, SPAM Filter etc. Denkst du, hier bestehen Chancen und Risiken, wenn das durchgeführt wird? #00:28:07-4#

Experte 3: Ja. Es bestehen Chancen. Die Hoffnung, dass es mal ein Tool gibt, was da alle Aspekte, die man braucht, abdeckt. Aus meiner Sicht ist da noch nichts auf dem Markt, was das wirklich gut kann. Die Integration in die Infrastruktur stellt sich sehr häufig als schwierig dar. Man denkt so, das ist ein einfaches Thema, man deployt da irgendwo eine VM oder einen Container hin. Aber das Ganze funktioniert in der Infrastruktur, gerade wenn man in der Mixed Clouds Szenario unterwegs ist, also teilweise onprem, also Hybride-Geschichten, teilweise dann in der Cloud oder in mehreren Clouds, wird das schon ganz schön "tricky". Whitelisting und dann auch aufpassen, baue ich mir nicht irgendwo noch eine Hintertür jetzt da ein, das ist nicht so ganz ohne. Und das wichtigste, was ich da mitgeben kann, ist einfach, die Nachvollziehbarkeit muss gegeben sein. Also nicht, dass man dann jetzt irgendwas tut und sagt, ja alles, was über den Kanal geht, interessiert uns nicht. Das ist jetzt Phishing, wenn man da einen

Transport Mail oder so eingerichtet hat. Nein, auch das sollte man bitte monitorieren, weil Fehlkonfiguration ist nun mal einer der häufigsten Faktoren für einen Angreifer. #00:29:27-7#

Severin Zimmermann: Sehr gut, danke. Dann bleiben wir bei technischen Sicherheitsvorkehrungen, nur das mal im positiven Sinne. Also sprich, um echte Phishing Angriffe abzuwehren, werden ja genau solche technische Vorkehrungen durchgeführt, sei die Spamfilter oder eben auch KI-benutzte Systeme, die Links bereits prüfen und in Quarantäne setzen etc. Das führt aber auch teilweise zum Problem, dass die Mitarbeiter diesen Techniken zu viel vertrauen und der Meinung sind, alles, was ich bekomme, müsste ja legitim sein, da ist ja schon herausgefiltert wurde, was bösartig ist. Wie siehst du das? Ist das ein Problem oder stellt das kein Problem? #00:30:20-1#

Experte 3: Das ist ein Problem und die Aussagen haben wir auch gehabt. Normalerweise wäre diese Mail doch im Spamfilter gelandet. Ja, normalerweise. Spamfilter könnte auch mal versagen, schlecht konfiguriert sein. Man verlässt sich vielleicht sogar auf einen Trittpartner, der das Ganze für einen übernimmt und auf dessen Intelligenz, die dahinter steckt. Irgendwo ist es Blackbox auch oft, was denn dort passiert. Und ja, wenn ich nur in meine Mailbooks schaue, in den letzten zwei Wochen sind zwei Mails dort gegangen, wo ich mir sage, wie konnten die jemals in meinem Postfach landen, da schreit alles nach Phishing, aber es ist passiert. Und deshalb die letzte Instanz ist immer der vor Monitor. Und nein, die technischen Maßnahmen, klar, die versucht man so weit wie möglich nach vorne zu treiben, ohne massiv False positives zu erzeugen, aber das ist keine abschließende Sicherheit. #00:31:26-4#

Severin Zimmermann: Sehr gut. Also technische Maßnahmen helfen, können aber nicht alles abwehren. Wie sehen /. Oder wie siehst du das, wenn jetzt zusätzlich zu den Schulungen noch Warnhinweise beispielsweise als technische Hinweise den Usern mitgegeben werden oder bist du der Meinung, die Sensibilisierung reicht aus? #00:31:52-3#

Experte 3: Das kommt drauf an, welches Risiko, wo man mitigieren will. Also sinnhaftig könnte es sein, so eine Geschichte wie, ich haue irgendwo einen Banner rein oder einen taggenden E-Mail mit, die kam von extern. Die wurde nicht von intern versendet. Das ist immer hilfreich und ein Indikator für, hier bitte erhöhte Sensibilität, genauer hinschauen. Solche Hilfsmittel, für die spreche ich mich stark aus. Ansonsten bleibt /. Bleibe ich dabei, der, der vor dem Monitor sitzt und an der Tastatur, der muss immer sensibel sein. #00:32:28-9#

Severin Zimmermann: Sehr gut siehst du auch Risiken mit solchen technischen Hilfsmitteln? #00:32:34-3#

Experte 3: Ja, auch die kann man natürlich als Angreifer versuchen zu faken oder dazu umgehen. Es suggeriert natürlich über die Dauer, dass das funktioniert, aber auch das kann mal aussetzen oder nicht funktionieren. Und wenn man sich immer darauf verlassen hat, dann passieren die Unfälle. #00:32:54-5#

Severin Zimmermann: Okay, sehr gut, vielen Dank. Dann auch in der heutigen Zeit sind wir oft sehr mobil unterwegs. Also wir prüfen unsermäß nicht nur noch klassisch auf dem Mail-Client am Desktop, sondern auch auf den Mobile Phones, Smartwatches, Tablets, was auch immer. Technisch funktioniert aber zum Beispiel das Prüfen von Links auf dem Mobile Phone ganz anders als auf einem E-Mail-Client am Rechner. Denkst du, dass diese Punkte im Schulungsmaterial integriert werden sollen, also diese unterschiedlichen Plattformen, dass die uns auch lernen, wie man mit Links auf Mobile Phones umgeht beispielsweise? #00:33:38-6#

Experte 3: Unbedingt. Das ist ganz, ganz wichtig, dem Endanwender mitzugeben, welche Möglichkeiten hat er denn zu prüfen. Und den technisch weniger versierten muss man halt eben die verschiedenen Varianten aufzeigen. Und das am besten auf jeder Plattform. Der eine /. Nimm mal nur der Unterschied von iOS zu Android, das ist schon immens. A In der Darstellung von Links hängt jetzt vom Browser ab, der hinten dran läuft oder und auch vom Handling von diesen Links oder Rechtsklick, mal den Link kopieren, irgendwo einführen, fügen oder eben du musst lange mit dem Daumen draufhalten, bis du dann mal ins Kontextmenü kommst und solche Dinge. Wo sind hier die Risiken auch bei dem Vorgehen? Ein Mobile-Endgerät ist häufig auch sehr klein. Da hat man sich auch mal /. Oder man rückt nicht richtig drauf und schon hat man den Link angeklickt. Also hier verschiedene Vorgehensweisen zu differenzieren macht auf jeden Fall Sinn. #00:34:40-7#

Severin Zimmermann: Sehr gut. Siehst du auch Risiken, wenn ich das in meiner Schulung integriere? #00:34:47-0#

Experte 3: Nein, eigentlich nicht, weil jeder zieht aus dieser Schulung das raus, was für ihn zutrifft. Wenn er kein iOS-Endgerät hat, dann kann er dann sein Gehirn für die zwei Minuten auf Durchzug stellen und ist halt wieder bei Android dabei oder whatever. #00:35:02-1#

Severin Zimmermann: Okey, gut, danke. Dann zur Frage von Meldepflattformen. Und zwar werden mit Phishing Awareness Trainings oft auch Meldepflattformen integriert, sei das eine Webseite, wo Phishings gemeldet werden können oder

ein Button im Outlook. Wie siehst du das? Oder siehst du hier Chancen, die generiert werden können, wenn ich so eine Meldepflattform integriere oder auch Risiken, die dadurch entstehen können? #00:35:32-2#

Experte 3: Jetzt verlässt du den Bereich Awareness und gehst auf echte Phishing Angriffe. Ist das richtig? #00:35:42-5#

Severin Zimmermann: Ja, auch. Also es ist auch im Zusammenhang mit Awareness. Also als Beispiel, was ich bereits als Risiko identifiziert habe, wenn ich natürlich eine Phishing-Kampagne habe und so eine Meldepflattform und das im großen Stil dann durchführe, können natürlich dann, wenn ich die Kampagne fahre, sehr viele Mails gemeldet werden und dann natürlich auch entsprechend Aufwand generiert werden. #00:36:09-4#

Experte 3: Gut, das ist die Thematik, die wir am Anfang hatten mit NCSC, dass man eben die Kampagnen anmelden soll und deren Handling über die Masse, das ist für die okay, das funktioniert. Wichtig ist einfach, dass man nicht auf Sperrlisten kommt, dass zum Beispiel auch große Provider wie dann die Switch sich auf eine DNS-Sperrliste nehmen. Da sollte man halt wirklich aufpassen. Ja, das ist eigentlich das Einzige, was dort wichtig ist und deshalb eben der, der es durchführt, sollte es auf jeden Fall anmelden. Ja, ansonsten sollte man den Endanwendern klar kommunizieren, wie sie denn beim Verdacht auf Phishing, Schlagklammer jetzt mal Spam aus, als nicht der effektive Schadensverursacher, sondern Phishing, wie sie reagieren sollen und wie sie reagieren sollen, wenn sie die Mail wirklich eindeutig als Phishing identifiziert haben. Ich glaube, dort muss man kurz und knackig den Endanwendern mitteilen und auch Möglichkeiten geben über einen Button, über ein Kontextmenü, ihnen sagen, wie machst du das in deinen, in den häufig genutzten Mail-Clients, auf den häufig genutzten Endgeräten, wie hast du da vorzugehen. Also die User schauen, dass die da vereinheitlich ist und einfach. #00:37:31-9#

Severin Zimmermann: Also vielleicht zum das zusammenfassen, also du siehst es als Chance und solche Buttons oder Meldeplatformen zu integrieren, dass auch echte Phishings gemeldet werden können. Es sollte aber, was ein Risiko darstellen könnte, die User genau informiert werden, wann sie solche Meldungen machen, damit nicht über häufig Meldungen oder auch Spam, die kein Risiko sind, gemeldet werden. #00:37:59-0#

Experte 3: Nein, sie sollen, wenn sie es eindeutig identifiziert haben oder glauben, es eindeutig identifiziert zu haben, sollen sie es als Phishing melden über diesen Weg. Wenn sie sich unsicher sind, haben wir das bei uns, läuft so, wir machen ein Incident auf und unser Security Operations Center nimmt sich dem an und beurteilt das Ganze, gibt dem Kunden dann Rückmeldung, hey, das war

kein Phishing, sieht für uns legitim aus oder nimmt halt die Maßnahmen vor, DNS Sperre melden bei den entsprechenden Stellen, bei Switch und Co. und sagt, hey, das war wirklich echtes Phishing, danke. Also bei Unsicherheit, nicht lieber nichts tun, sondern ruhig melden, aber halt auf dem Weg, Fragezeichen, ist das eins oder ist das keins. #00:38:45-3#

Severin Zimmermann: Okay, sehr gut, vielen Dank. Dann sind wir beim Umfeldfaktor und zwar, so viel ich weiß, habt ihr bei der Durchführung vom OptiPhish Projekt mit externen Partnern zusammengearbeitet. Sind dir hier Aspekte bekannt oder auch Chancen und Risiken, die mit externen Partnern bei der Durchführung eines Phishing Awareness Training auftauchen können? #00:39:14-3#

Experte 3: Jetzt muss ich aufpassen, was du jetzt als externer Partner verstehst. Externer Partner, wir haben eine Software eines externen Partners eingesetzt, die häufig Templates aktualisiert hat, neue Templates reingebracht hat, auch neue Trainings, neue Quizzes und sowas auf der Ecke, also das kam mit. Bei der Implementierung selbst haben wir, sagen wir mal, eine Grundschulung bekommen und die Implementierung wurde dann selbst durchgeführt. Also da haben wir jetzt keine große Hilfe vom externen Partnern noch bezogen. Haben also quasi mit den vorgefertigten Templates, die kopiert, auf uns adaptiert und dann die Awareness Trainings durchgeführt. Aus meiner Sicht, wir wollen ja auch Awareness Training weiterführen auf einer anderen Plattform und dort werden wir wirklich Unterstützung brauchen auch beim Aufsetzen dieser Kampagne. Also es ist für Anbieter, glaube ich, wichtig zu wissen, dass es nicht reicht, die Software hinzustellen, die technisch funktioniert. Die Templates hatten ein paar oder auch sehr viele, sondern dass man wirklich die Anwender dann auch so weit bringt, dass sie verstehen, was haben wir für Möglichkeiten, auf was es zu achten. #00:40:38-0#

Severin Zimmermann: Okay, und jetzt ihr habt eben eine Software eingekauft, denkst du, es gibt Chancen und Risiken, wenn ich das als SaaS mache und wirklich eng mit dem Anbieter arbeite, wo dann nicht nur die Templates zur Verfügung stellt, sondern auch Unterstützung bei den Kampagnen und die Durchführung der Kampagnen. #00:41:05-2#

Experte 3: Das Ganze als SaaS zu beziehen, ist vielleicht nicht falsch, aber man darf nicht den Fehlglauben dann annehmen. Im Unternehmen hat man keine Arbeit mehr, weil du hast ja in den Fragen vorher es auch rausgekitzelt ist. Es bleibt immer ein sensibles Thema und ein externer Partner kann das gar nicht abschätzen. Wie sind deine Zielgruppen? Wie ticken die Leute? Wann ist es zu viel? Wann ist es zu wenig? Wann wird was überschritten? Wann ist die Schmerzgrenze erreicht? Das ist alles etwas schwierig und von daher SaaS das Ganze zu beziehen, wenn man es technisch integriert bekommt. Da sind ein paar Hürden, die man nicht vergessen darf, technischer Natur, vor allen Dingen auch, wenn man dann Qustom Domains verwenden will, Bezug von SSL-Zertifikaten,

ohne dann zu zeigen, ja okay, hinter dem SSL-Zertifikat stecken wir, verraten uns quasi damit. Das sind so spezielle Themen. Ich sag mal, für einfache und mittelschwere Trainings ist das vielleicht obsolet, aber wenn du dann natürlich mal einen IT-Lehrer, der denkt, er hat es im Griff, phishen willst, dann muss das passen, sonst findet er es raus. #00:42:20-3#

Severin Zimmermann: Sehr gut, dann vielleicht nochmals ergänzend, wenn ich das mit externen Partnern mache, die nicht in der Schweiz ansässig sind, sondern im Ausland, siehst du hier nochmals andere Risiken oder Chancen? #00:42:35-2#

Experte 3: Das Risiko ist nach wie vor das Thema mit Brandings, eben rechtliche Seite, wo es der Gericht stand. Ich glaube, das wäre dann so ein Thema, falls sich jemand draußen eschoffiert fühlt, hey, das spielt doch stark auf unser Branding ab und man hat /. Man geht Richtung Rechtsstreit, dann sollte man wirklich aufpassen, dass es auch vom Gerichtsstandort dann halt rechtlich dunktioniert. Die rechtlichen Abklärungen im Vorfeld, die sollte man auch nicht unterschätzen, sollte man machen. #00:43:08-6#

Severin Zimmermann: Sehr gut, denkst du denn auch, dass es vielleicht zu einem erhöhten Risiko kommen kann, da man doch sehr viel Information mit dem Anbieter austauschen muss, sei das eben E-Mail-Adressen, Namen der Anwender, wenn man es personalisieren will, noch mehr Information, dass es da zu einem Risiko kommen kann, wenn es jetzt beispielsweise ein Data-Leak gibt beim externen Anbieter, wo man halt selber keine Hand darüber hat und dann quasi Opfer /. Oder vielleicht echte Phisher an diese Daten gelangen. #00:43:44-4#

Experte 3: Ja, aber die Thematik ist eine generische Thematik, die haben wir bei jeder Software, die wir irgendwo aus der Cloud beziehen oder die von einem Drittanbieter kommt, dort müssen wir einfach ganz klar die Verträge aushandeln und auch richtig darauf hinweisen, gerade wenn es schützenswerte Daten sind, personenbezogene Daten, müssen wir halt auch die Auflagen entsprechend hochlegen und auch auditieren, erfüllt der Anbieter das Ganze. Mein Data-Leaks komplett verhindern, das wird wohl nie möglich sein, aber die Hürden einfach und wieder das Thema Risikominimierung, das muss man natürlich ganz klar angehen. Aber das ist ein generisches Thema, bei jeder Software, die irgendwo Daten bezieht. #00:44:26-3#

Severin Zimmermann: Sehr gut, vielen Dank. Du hast es bereits angesprochen, rechtliche Aspekte. Möchtest du hier noch etwas ergänzen, ob es rechtliche Aspekte zu beachten gilt? Du hast es ja bereits erwähnt, mit Logo, Datenschutz, wenn ich das richtig im Kopf habe, etwas ist deiner Meinung nach, noch mehr rechtliche Aspekte zu beachten? #00:44:52-9#

Experte 3: "Jaein", für mich ist es Transparenz wichtig. Man sollte dem Endanwender klarmachen, wir haben dein Passwort jetzt nicht geloggt, wir haben nur gesehen, du hast was eingegeben, oder ja, wir haben es mitgelockt, aber es ist obfosziert. Wichtig ist bei diesen ganzen Dingen, dass man einfach Transparenz schafft und Vertrauen. Wenn man das alles im Dunkeln lässt und die Benutzer denken sich, was machen die jetzt mit meinen Daten und "salopp" formuliert ist das jetzt für die nächste Lohnrunde relevant, ob ich jetzt geklickt habe oder nicht, das darf einfach nicht passieren. #00:45:32-0#

Severin Zimmermann: Okey sehr gut, danke. Dann sind /. Oder wir haben das auch bereits ein wenig besprochen, ob die externe Partner bekannt sind, Regierungsinstitutionen, Melanie oder NCSC, das wir bereits angesprochen haben, Hostel, Registrar etc., die zwingen über das Phishing Awareness Trainings informiert werden sollten, so wenn man eins durchführt. #00:45:57-0#

Experte 3: Ja, das hängt eher damit zusammen, wo beziehe ich denn meine Domains. Irgendwo muss ich ja meine Domain registrieren, wenn ich eine Phishing, Fremddomain oder Drittdomain durchführen will, dann macht es natürlich auch Sinn, den Hostel zu informieren. Wir verwenden diese Domains zur Durchführung von internen Phishing Kampagnen. Das ist unser Vorgehen, das sind die Zeiträume, wo das abläuft. Also wenn dort Meldungen kommen, müsst ihr nicht zwingend direkt sperren, sondern kommt auf uns zu. Wir stehen Rede und Antwort. Eine Ansprechpartner bekannt geben ist dort ganz wichtig beim Domain Registrar. Sonst ist man nämlich ruckzuck auch auf irgendwelchen Blacklisten. Und wenn das vermehrt aus dem IP Bereich kommt, IP Block kommt, kann es dann auch der IP Block drauf kommen und das wollen wir natürlich nicht. #00:46:49-9#

Severin Zimmermann: Sehr gut. Ja, du hast es bereits gesagt, weshalb das diese Parteien informiert werden sollen, eben dass man nicht plötzlich irgendwo geblockt wird. Deshalb die nächste Frage. Sind dir Meldepflichten bekannt, die /. Oder ja Meldepflichten bekannt die man angeben muss, wenn ich jetzt Opfer eines Phishings wurde, also eines echten Phishings und nicht einer Simulation? #00:47:17-7#

Experte 3: Ja, das sind dieselben Vorgaben von NCSC. Dort kann man danach suchen und es ist ganz klar dort kommuniziert, was du zu tun hast, wenn du Opfer eines Phishings wurdest. Also das ist das einzige mir Bekannte, jetzt von offizieller Seite her. Eine gute Frage ist eigentlich, ob wir unsere Anwender davor dazu verpflichten an der ZHAW, wir das zu melden. Ja, das ist mal spannend, würde ich mal in die Runde werfen, ob wir da eine Weisung haben. #00:47:59-7#

Severin Zimmermann: Das ist eine gute Frage ja, das wüsste ich auch nicht, hätte ich vielleicht im Interview mit eurem CISO ansprechen können. #00:48:10-7#

Experte 3: Weil das ist ja noch spannend, letztendlich hast du ja Anstellungsbedingungen, da könnte sowas natürlich irgendwo auch generischer verpackt sein, dass du das musst. Ich glaube, wir haben sowas, aber wie gesagt, ich bin jetzt die letzten Monate nicht eingedreht, ich kann nicht sagen, wie das da aussieht. Ja, das ist auf jeden Fall nicht zu unterschätzen, die Thematik. Aber letztendlich Weisungen und so ist es eine, Papier ist geduldig, wirklich vermitteln, hey, ihr braucht keine Angst zu haben, es verurteilt euch niemand, meldet es, kommt auf uns zu und wir schauen, wie wir es bestmöglich draus machen. Niemanden an den Pranger stellen. #00:48:55-1#

Severin Zimmermann: Sehr gut, danke, das war auch noch ein sehr interessanter Punkt, den ich so noch nicht gehört habe, eigentlich interne Meldepflichten. Ja, definitiv auch ein Punkt. Dann wäre ich eigentlich schon mehr oder weniger durch mit meinen Fragen, vielleicht zum Schluss, sind aus deiner Sicht noch Punkte offen Aspekte, die wir noch nicht behandelt haben, die du hier noch sicher diesem Rahmen sagen möchtest. #00:49:21-2#

Experte 3: Eine Sache ist, denke ich, wichtig für Unternehmen, man kann so eine Phishing Awareness Kampagne mal punktuell machen, aber beiläufig ist das nicht möglich, das ist wirklich ein Job, der einen fordert, wenn man die Kampagnen durchführen möchte, das Ganze technisch aufbaut, technisch begleitet, organisatorisch begleitet, man kommt in viel Diskussion mit unterschiedlichsten Stakeholder in Unternehmen, wie gesagt, der eine fühlt sich schon beübt nach der dritten Mail, der andere legt die Zehnte einfach weg oder löst sie. Wir sind Menschen, wir sind unterschiedlich, das ist wirklich schon ein Job für eine Person, auch das Durchführen von den Awareness Trainings jetzt nicht nur online, sondern also digital, jetzt über Portal, über Quizzes, sondern wie eben schon gesagt, über wirklich Awareness Trainings auch vor Ort oder per Cam. Wir haben das erkannt und haben da auch eine Person bei uns, die als einen Teil seiner Anstellung das in Zukunft abdecken wird. #00:50:39-5#

Severin Zimmermann: Okay, sehr gut, dann danke für die Ergänzungen, meine letzte Frage wäre dann nur noch, ich führe noch weitere Interviews durch, falls ich da zu neuen Aspekten komme, die ich jetzt noch nicht behandelt habe, aber trotzdem gerne deine Meinung dazu hätte, dürfte ich dich nochmals kontaktieren? #00:51:02-8#

Experte 3: Ja, absolut kannst du machen, am besten natürlich per Mail, dann die konkreten Fragen auftreiben, so wie jetzt hier im Leitfaden und dann kann ich die, wenn es nicht so viele sind, schriftlich beantworten oder wir telefonieren noch

mal. #00:51:18-1#

Severin Zimmermann: Sehr gut, vielen Dank, dann werde ich die Aufnahme jetzt beenden.

G Transkript Experten-Interview Experte 4

Administratives	
Interview Datum	11.04.2023
Interview-Partner	Experte 4
Arbeitgeber	ZHAW
Aufnahme OK?	Ja
Anonymisierung Daten?	Nein

Severin Zimmermann: Sehr Gut. Das Transkript hat auch gestartet. Dann zur ersten Frage. Dürfte ich Sie kurz bitten Ihre Position und Funktion zu nennen? #00:00:20-6#

Experte 4: Ja ich bin. Also Experte 4 oder ich bin ICT Sicherheitsbeauftragter an der ZAHW seit etwas über 8 Jahren. Ja zu meinen Aufgaben gehört alles was rund um Cybersicherheit an der ZHAW passiert. #00:00:39-9#

Severin Zimmermann: Sehr gut. In dem fall auch den Bereich Phishing. Hatten den bereits Erfahrungen mit Phishing, wurden Sie villiecht selbst einmal Opfer oder einer Ihrer Kollegen? #00:00:52-9#

Experte 4: Also wir haben ander ZHAW immer wieder Phishing Vorfälle. AlsoTäglich wäre zu wenig wir haben das alle paar Stunden irgendwo an der ZHAW wir /. Wir sind zuständig für etwa 50'000 Benutzerkonten und Phishing ist da einfach omnipräsent. #00:01:18-8#

Severin Zimmermann: Sehr gut. Kann ich mir gut vorstellen, hatten sie den auch bereits Erfahrungen mit Phishing Awareness Training? #00:01:30-0#

Experte 4: Ja genau. Wir haben da grad im vorletzten Jahr gabs an der ZHAW ein grosses Forschungsprojekt zu Phishing Awareness Training und auch Trainings. Es war vom Institut für Informationstechnologie. Wir haben über den verlauf von etwa 12 Monaten 288'000 Mails versendet an unsere Hochschulangehörigen. Und hatten dann eben auch da Training mit gekoppelt, das heisst wenn

jemand darauf geklickt hat auf einen von diesen Phishing Links, dann wurde entsprechen ein Training angeboten. #00:02:10-2#

Severin Zimmermann: Ok. Das nehmi ich an war die OptiPhish Kampagne. #00:02:18-5#

Experte 4: Ja das ist so richtig genau. #00:02:20-6#

Severin Zimmermann: Gut. Dann würden wir zu den Huptfragen rüberkommen. Sind das Ihre Sicht positive Aspekte bekannt, die im Rahmen eines Phishing Awareness Trainings resultieren können? #00:02:34-4#

Experte 4: Ja, also aus meiner Sicht. Ich glaube, wir kommen dann später noch dazu oder also grundsätzlich ja. Positive Aspekte sind sicherlich vorhanden, man muss aber mit Fingerspitzengefühl vorgehen. Ja. Und natürlich geht es darum, dass das Risiko letztlich auch für die Organisation für die Hochschule jetzt in unserem Fall zu minimieren. Und die Person zu sensibilisieren, auf das auf das Thema Phishing die damit verbundenen Risiken und vielleicht auch auf neue Trends, also die Phisher gehen ja auch immer mit der Zeit passen ihre Kampagnen an. Was war das zu Corona Zeiten haben die Phisher dann versucht, mit günstigen Schutzmasken und günstigen Desinfektionsmitteln die Leute zu /. Anzuziehen und dann als Ukraine Krieg startete haben, sie haben sie da auch Ängste geschürt und so versucht zu Phishen. Also wir müssen, wir müssen unsere Mitarbeiterinnen und hochschulangehörigen eigentlich konnte ich auch informieren über das Phishing Awareness Training Was sind eigentlich die aktuellen Bedrohungen. Die aktuellen Phishing Risiken. #00:03:58-0#

Severin Zimmermann: Genau, das ist mir so auch bis jetzt aufgefallen. Vor allem auch die Aktualität des Phishing , das Sie genannt haben. Kennen Sie denn auch ne gative Aspekte, welche bei der Durchführung eines Phishing Awareness Trainings auftauchen können? #00:04:18-9#

Experte 4: Ja, also allen voran ist das jetzt auch nach der OptiPhish Kampagne oder 288000 Mails über ein Jahr an die Hochschulangehörigen zuzusenden. Es war zuviel, das hat auch für Aggressionen geseogt bei manchen Personen und genau. Also das ist dann kontraproduktiv, oder wenn man wirklich /. Wenn plötzlich die. Die Adressaten vom Phishing Awareness Training einfach nur noch sauer sind auf Security und nichts mehr wissen wollen von Security, dann haben wir dann plötzlich ein Problem. Ansonsten ja negative Aspekt /. Also vom Phishing Awareness Training per se darüber hinaus sind eigentlich nicht. Es gibt so ein paar Side Effekts, wenn man eben nicht mit Fingerspitzengefühl vorgeht.

Aber ich glaube, da reden wir dann auch gleich noch drüber, was dann passieren kann, oder? #00:05:24-4#

Severin Zimmermann: Ja gut, danke für den ersten Überblick. Sie haben jetzt viel organisatorische Aspekte genannt im Mitarbeiter werden sauer, weil es zu viele Mails sind etc. Sie kommen auch mehr aus der organisatorischen Perspektive sind ihnen vielleicht dennoch technische Aspekte bekannt, welche im Rahmen eines Phishing Awareness auftauchen können oder beachtet werden sollten. #00:05:56-1#

Experte 4: Ich würde gerne noch bei den organisatorischen Aspekten noch kurz ergänzen. Aus meiner Sicht muss so ein Phishing Awareness Training muss an die Organisation und die Organisationskultur auch angelehnt sein. Das heißt für uns an der an der Hochschule damit das von der Hochschulleitung auch getragen mitgetragen wird, muss es ich sag jetzt mal vorsichtig, eher akademisch angehaucht sein, oder. Das heißt so wir hatten mal über Gamification im Awareness Training gesprochen und so weiter, aber das kommt grundsätzlich eher nicht so gut an in unserem Umfeld, sondern da wird /. Und deswegen das muss einfach an die Organisationskultur angepasst sein oder. Jetzt bei den technischen Aspekten. Jein ist vielleicht ich weiß nicht, ob das jetzt also wo das Thema genau rein gehört, aber bei so einem Awareness Training /. Wenn Sie jetzt sagen Awareness Training meint Sie dann nur den Teil, den Schulungsteil oder meinen Sie auch den Teil, wo Testmails vielleicht verschickt werden? #00:07:13-4#

Severin Zimmermann: In meiner Arbeit inkludieren ich das versenden von Phishing Simulation, also von testmails mit als Training #00:07:22-9#

Experte 4: OK #00:07:23-6#

Severin Zimmermann: Was ich nicht beachtete, ist Effektivität von gewissen Methoden, oder solche Sachen also wie effektiv sind gewisse Schule oder welche Schulungsmaßnahmen ist jetzt die Beste? Das ist nicht im Rahmen meiner Arbeit. Aber klar, Phishing Testmails beziehungsweise Simulation gehören mit zu einem Training und werden dementsprechend auch mit einbezogen. #00:07:52-0#

Experte 4: Okay dann also, da gibt es verschiedene Punkte zu beachten. Einer einmal ist es sicherlich, dass die angeschriebenen Adressaten, dass die vielleicht auch randomisiert sind, also einerseits /. Also die Person reden miteinander, wenn sie in einem Büro sitzen, dann reden die miteinander. Ich hab jetzt grad

blöde Phishing Mail bekommen schau mal hier, das war von der Post Paketzustellung, dann weiß das der Kollege, dann bekommt der Kollege (unv., #00:08:25-4#) Kollege in sein Postfach hat es auch drin, klicke nicht mehr drauf. Das verfälscht dann letztendlich das Ergebnis und den Sinn und Zweck, sondern /. Ich finde es wichtig, dass das randomisiert wird idealerweise, wenn man das, wenn die Systeme das hergeben, dass nicht all /. Nicht mehrere Personen in einem gemeinsamen Büro zu einem dieselbe Phishing Mail bekommen, sondern dass man vielleicht mehrere Kampagnen fährt und die dann entsprechend verteilt geschickt verteilt, dass die, dass, wenn einer /. Wenn sie untereinander darüber reden dass, dass sie da das Ergebnis nicht verfälschen oder. Das finde ich noch einen wichtigen Aspekt muss dann auch technisch gelöst werden, oder. Dann aus dem Umfeld ich komme schon zum nächsten Punkt. #00:09:16-5#

Severin Zimmermann: Kein Problem nur zu. #00:09:18-4#

Experte 4: Aus dem Umfeld ist noch wichtig wir hatten tatsächlich im Rahmen der OptiPhish Kampagne Schwierigkeiten Marken wiederzuverwenden. Also nehmen wir an, wir verschicken intern ist jetzt rein fiktiv oder! Internen im Namen der Post, die solche Paketzustellung Phishing Simulationen, dann müssen wir damit rechnen, dass die Post von unseren Mitarbeitern in einem 50'000 Personen oder, dass die Post kontaktiert wird und dass sich einzelne bei der Post beschweren werden. Die finden das überhaupt nicht "lässig", wenn ihr Support ihre Supporthotline plötzlich geflutet wird mit ZAHW Angehörigen, die sich über über das Phishing beschweren. Und /. Also es gibt Unternehmen, die unterstützen das. Ich weiß zum Beispiel nicht, wie die Banken dazu stehen. Aber grundsätzlich muss auch da mit Fingerspitzengefühl vorgegangen werden und wenn man eine bekannte Marke wieder verwenden möchte in seiner Phishing Simulation, dann muss da die Einverständnis von den Markeninhabern eingeholt werden, na. #00:10:31-9#

Severin Zimmermann: Sehr gut vielen Dank für die bereits sehr umfangreichen Aspekte. Ich werde jetzt hier auch nicht weiter drauf eingehen, für das haben wir jetzt nachher noch die Detailfragen. Möchten Sie zu diesen Aspekten aber dennoch etwas ergänzen oder ist noch ein Aspekt, dass ihre Sicht offen? #00:10:52-0#

Experte 4: Also vielleicht einfach ergänzend. Der Aufwand, um die Simulation durchzuführen, ist nicht nur die Inbetriebnahme, die Entwicklung von den Kampagnen, sondern das ist dann auch im Nachgang die Beantwortung von Anfragen dazu. Wir hatten das (unv., #00:11:17-9#). Gut, wir sind jetzt relativ große Organisation, aber wir hatten nach der ersten Durchführung, da waren bei uns eigentlich 4-5 Personen 2 Wochen lang beschäftigt, nur mit den Anfragen zu diesem Phishing Mails, da die zu bearbeiten und zu beantworten, das ist nicht zu unterschätzen, oder. Und Ja, ich hatte noch was anderes, aber das fällt mir nachher vielleicht noch mal wieder ein. #00:11:45-1#

Severin Zimmermann: Gut, ja bei Detail Fragen kommen wir sicher da nochmal zurück und fällt ihnen die Frage vielleicht wieder ein? #00:11:53-3#

Experte 4: Genau. #00:11:54-2#

Severin Zimmermann: Dann würden wir zuerst organisatorische betrachtung ansehen hier die Frage. Sin Ihrer Meinung nach /. Oder soll Ihrer Meinung nach ein Phishing Awareness Training auf spezielle Usergruppen abgestummen werden? Also in der Literartur wird oft beschrieben demographische Eigenschaften oder Verhalten der User beeinflussen ihre Anfälligkeit auf Phishing und deshalb ist auch die Personalisierung des Phishing recht diskutiert. Wie stehen Sie demgegenüber? #00:12:30-0#

Experte 4: Ich also die Kriterien, die ich hier genannt sind, da bin ich mir nicht sicher. Ich hab da eher aus der Praxis dann jetzt Beispiele, wo man sagen muss ja, das muss abgestimmt sein. Zum Beispiel die Human Resources Leute, Unsere Personalabteilung, muss anders adressiert werden wie Dozierende oder Studierende oder. Wir haben gezielte Angriffe, Phishing Angriffe auf Personal unsere Personalabteilung, wo Bezug genommen wird auf echte Ausschreibungen, die im Internet sind, wo sich jemand mit einer Mail bewirbt, sagt Bewerbung auf die Positionen Professur. Und dann wirklich Anschreiben auch formuliert das wirklich maßgeschneidert und dann mit einem Link versehen. Meine Bewerbungsunterlagen finden Sie auf Dropbox und dann oder Google Drive, wenn man da drauf klickt, dann legt man sich dann Schadsoftware runter, oder. Das heißt, die müssen ganz anders auf solche Cases dann vorbereitet werden. Jetzt in dem Fall Personalabteilung. Ich kann mir auch vorstellen Finanzabteilung muss /. Halt auch wieder andere Cases oder die ICT Abteilung wenn hat auch andere Case, also wenn bei der ICT Abteilung jemand sich als Servicedesk oder ICT Helpdesk ausgibt, dann sind wir ja weniger anfällig dafür, als wenn jetzt ein Studiengangssekretariat darüber adressiert wird. Das heißt Ja Trainings müssen abgestimmt sein. Ich geh, ich hab das eigentlich immer eher an der Funktion im Unternehmen festgemacht. Es wird relativ komplex, schnell also das relativ schnell komplex, wenn man wirklich auf alle diese Kriterien und zusätzlich noch auf die Funktion eingehen will und das berücksichtigen will und das hat auch eine technische Herausforderung, weil demographischen Background da ist normalerweise in keinem ICT System, das ich kenne hinterlegt. Also wenn wir jetzt, sagen ok, da kommt jemand ist gebürtiger Nigerianer oder so hat vielleicht einen anderen Bezug zu zu Phishing als jemand aus Norwegen, oder. Die Informationen liegen uns gar nicht vor, das heißt, wir können das praktisch gar nicht umsetzen. Und dann muss das Tool, das die das Phishing Awareness Training realisiert muss dann natürlich diese Informationen auch irgendwie verarbeiten können. Also ich finde, dass ich finde es interessant, aber in der Praxis hat das für mich bisher keine Relevanz gehabt. #00:15:10-2#

Severin Zimmermann: Okay, aber Sie haben dennoch jetzt auch in ihrem Projekt auf zumindest auf Funktionsbasis Phishings oder simulierte Phishings personalisiert, sag ich jetzt mal. Haben Sie da Chancen beziehungsweise, welche Chancen haben Sie sich dabei erhofft? oder auch Risiken festgestellt, die entstehen können, wenn Sie das so durchführen? #00:15:37-7#

Experte 4: Risiken hab ich jetzt nicht. Sind wir jetzt nicht irgendwie präsent, aber erhofft haben wir uns natürlich, dass das unsere Mitarbeitenden, wenn ein echtes Fishing reinkommt, dass sie da vorsichtiger agieren und vielleicht und wirklich zweimal schauen ist ist der Link wirklich echt ist der Absender echt und macht macht der Text der Mail überhaupt Sinn oder ruf ich lieber den Absender an und frag ihn, Ob die Mai legitim ist? #00:16:15-0#

Severin Zimmermann: Okay also so wirklich eine erhöhte Sensibilisierung, auch wenn Spear Phishing, also personalisiertes echtes Phishing reinkommt? #00:16:25-9#

Experte 4: Genau. #00:16:27-3#

Severin Zimmermann: Sehr gut. Dann zum Training selbst es gibt bekanntlich ja sehr viele unterschiedliche Möglichkeiten, ein Phishing Training zu gestalten. Sie selbst haben hier Embedded Trainings verwendet. Es gibt auch die Möglichkeit, präventive Schulungsmaßnahmen zu ergreifen. #00:16:48-0#

Experte 4: Ja. #00:16:48-8#

Severin Zimmermann: Ebenfalls auch unterschiedliche Formen der Wissensvermittlung eben Gamification, wie Sie das am Anfang bereits erwähnt haben oder Video oder per Factsheet. Dann die Zustellung selbst, kann auf unterschiedliche Weise erfolgen, sei das online in Klassenräumen. Und auch ein Aspekt ist werden die Mitarbeiter über Phishing Simulationen informiert oder nicht? Mir ist es nicht bekannt, wie Sie das bei ihrem Projekt gemacht haben, aber hab /. Oder sehen Sie aus dieser Sicht Chancen und Risiken beim Aufbau eines Phishing Trainings. #00:17:30-0#

Experte 4: Also grundsätzlich, wenn ich jetzt ein bißchen "rauszoome" aus den ganzen Phishing Thema, weil ich mache ja auch Security Awareness nicht nur Phishing Awareness, oder. Grundsätzlich versuchen wir über viele unterschiedliche Kommunikationskanäle die Informationen zu verbreiten, weil wir haben es

auch mit ganz unterschiedlichen Persönlichkeiten zu tun. Der eine lernt eherr visuell, der andere eher über das was, ihm gesagt wird und /. Die Menschen haben auch ganz unterschiedliche Wahrnehmung. Das heißt, wir versuchen schon auch Informationen, nicht nur über einen Kanal zu verbreiten. Auch wenn man jetzt technikaffinität damit mit einfließen lässt. Und Ich finde es eher gut, wenn das eben über unterschiedliche Kanäle in unterschiedlicher Gestaltung zu unterschiedlichen Zeitpunkten kommt wichtig ist und das war der Punkt, den ich vorhin noch sagen wollte. Wichtig ist, dass es kontinuierlich passiert. Das ist nicht nur eine einmalige Aktivität ist. Also jetzt machen wir mal eine Woche lang Phishing Awareness, sondern es muss kontinuierlich passieren, dass ist etwas, was wir deutlich feststellen. Die Leute die vergessen das wieder und zwar schneller als man denkt, oder. Innerhalb nach ein paar Wochen ist das, hat das Training keine keine Wirkung mehr, wirklich kontinuierlich bespielen wir haben das auch in der Vergangenheit schon gemacht, ist ja schon ein paar Jahre her mit Plakaten in den Departementen mit Aufstellern in den Eingangsbereichen. Wir haben Veranstaltungen Cybersecurity Breakfast angeboten, dort auch informiert ZHAW. Weil wir haben so eine Tour gemacht durch alle Departemente bei den Mitarbeiterversammlungen, gerade in der Vorweihnachtszeit waren wir mehrere Jahre unterwegs, haben auch immer immer immer wieder auf Phishing Thema hingewiesen und das war eigentlich immer noch zu wenig, dass ist wirklich in den Köpfen bleibt weil. Es muss wirklich noch mehr passieren, dass die Leute das wirklich checken. Und dann noch ein ganz anderer interessanter Aspekt ist. Hat man nämlich selbst, wenn man noch so viele sensibilisierte Personen hat, hat man trotzdem immer noch Personen, die einfach darauf klicken, weil sie neugierig sind, die wissen was ist Phishing. Also hat mir ein Kollege hat mir das damals gesagt hatten wir dann an Vorfall oder. Hat mir dann gesagt, ja zu Hause auf meinem privaten hätte ich nicht darauf geklickt, aber hier bei der ZAHW hab ich gedacht ich schau mal was passiert oder. Und da kann man noch soviel sensibilisieren noch soviel sensibilisieren. #00:20:19-1#

Severin Zimmermann: Ja, sehr interessant hab ich jetzt so auch noch selten gehört, aber ich sehe das stellt definitiv ein Problem darf. #00:20:31-0#

Experte 4: Ja, (unv., #00:20:32-4#) sind natürlich nur wenige, wo das dann das so ankommt dann? #00:20:36-3#

Severin Zimmermann: Gut, wenn ich hier noch ergänzend darf. Das IT-Personal steht oft auch in Diskussion in der Literatur, ob dieses informiert werden soll oder nicht. Viele Literaturen sagen aus, dass das IT /. Und das die IT genauso anfällig ist und entsprechend geschult werden soll, was bei einer Information der Effekt einfach verringert wird. Wie sehen Sie das? Sollte das IT-Personal informiert werden oder eher nicht? #00:21:06-7#

Experte 4: Also es müssen /. Wir machen das an der ZHAW so, dass wir Schlüsselpersonen informieren, also mindestens den Servicedesk, oder weil bei denen

werden dann die Tickets auflaufen. Die müssen vor informiert sein auch stellen wir uns vor, es ist irgendwie Juli, die Hälfte vom Servicedesk ist in den Ferien und wir machen so eine Kampagne, dass muss in Absprache passieren, die werden sonst geflutet und können nicht mehr die wichtigen Themen bearbeiten. Wer auch vor informiert wird, es sind die Verantwortlichen Personen für die E-Mail Infrastruktur. Weil bei den Laufenden sonst auch Fragen auf die Stellen vielleicht Anomalien fest und die natürlich unsere Leute aus dem Security Monitoring, weil bei denen läuft es auch auf. Und das sind dann /. Hat man haben wir vielleicht so /. Wir haben etwa 110 Personen in der IT und 10 von denen sind Vorinformiert, aber auch mit dem Hinweis bitte das für euch behalten. #00:22:10-6#

Severin Zimmermann: Ok, vielen Dank. Also teilweise die IT informieren. Kommen wir zur nächsten Frage die Cybersicherheitskultur, Sie haben diese bereits kurz angesprochen, dass diese im Rahmen des Phishing Awareness Trainings aus ihrer Sicht eine Rolle spielt. Hier noch die Frage durch Cybersicherheitskultur kann ja auch eine gewisse Grund Awareness geschaffen werden. Wie man sich gegenüber Sicherheitsvorfällen oder im Gefahren verhält. Spielt Ihrer Meinung nach das eine wichtige Rolle und sollte in einem Phishing Awareness Training auch entsprechend geschaffen werden /. Eine entsprechende Cybersicherheitskultur oder sehen Sie das als komplett eigenständiges Thema? #00:23:00-9#

Experte 4: Ne ich glaub für mich gehört das zusammen oder das ist es "geht Hand in Hand". Ich finde wenn man eine Cyber sicherheitskultur entwickelt aufbauen möchte in einem Unternehmen dann ja, dann ist Phishing Awareness Training, kann man dann auch als /. Also das kann man als Tool mit verwenden dafür oder. Ich was ich an Phishing Awareness Training da noch sehr gut finde, ist es ist ein greifbares Thema, also bis zu einem gewissen Grad. Aber die Leute können sich was drunter vorstellen, jeder hatte mal irgendwie eine Phishing Mail und das kann wieder helfen als Beispiele, so eine Cybersicherheitskultur dann auch zu schaffen. Und weil man natürlich eine Cybersicherheitskultur auch schon etabliert hat, hilft das wiederum auch bei einem Phishing Awareness Training. Die Leute gehen dann viel offener /. Also wenn die Cybersicherheitskultur gut entwickelt ist, gehen die Leute viel offener mit solchen Phishing Awareness Trainings um. Nämlich ein Risiko was auch besteht, ist je nachdem, wie die Kultur auch ausgeprägt ist, ist das Person sich überwacht fühlen oder reingelegt fühlen von denjenigen, die dieses Awareness Training machen. Also das sozusagen hey jetzt kommt da die ICT und legt uns rein mit /. Und ja, was wir auch immer versucht haben, fällt mir jetzt grad noch in einem Kontext ein. Wir haben immer gesagt, die Ergebnisse werden anonymisiert, es erfolgt kein Monitoring, keine Auswertung auf Ebene der Einzelperson, sondern es wird anonymisiert. Wir haben dann auf Departementsebene, zum Beispiel ne Auswertung. Aber Genau. Aber für mich gehört das zusammen, das "geht Hand in Hand" #00:24:53-9#

Severin Zimmermann: Ok vielen Dank. Ich weiß gar nicht, ob die Anonymisierung noch Thema ist, speziell ist aber sicher auch in meiner Arbeit bereits aufgetaucht, von daher vielen Dank. Kommen wir zu ethischen Aspekten. Ich weiß, Sie haben

in ihrem Projekt sicher ethische Aspekte berücksichtigt. Können Sie vielleicht erläutern, welche aus Ihrer Sicht ethischen Aspekte bei der Durchführung eines Phishing Awareness Trainings berücksichtigt werden sollten? #00:25:33-1#

Experte 4: Ja also. Für mich ist das wirklich wieder das Thema Fingerspitzengefühl, oder. Organisationskultur berücksichtigen aber auch natürlich generell, wo bewegen wir uns? Welche kulturellen Themen gilt es zu berücksichtigen? Und dann natürlich ja das das Übliche /. Ich mein müssen Minderheiten respektieren und ja, auch Andersdenkende respektieren und /. Aber es ist jetzt nicht wir haben jetzt keinen Leitfaden ethischen Leitfaden für Phishing Awareness oder so erstellt, sondern das ist eigentlich "common sense" und wir kennen unser kulturelles Umfeld, oder. Und das müssen wir entsprechend auch leben. #00:26:31-5#

Severin Zimmermann: Ok, vielen Dank. Dann zu Klickraten und zwar oft werden im Rahmen vom Phishing Awareness Training insbesondere bei Phishing Simulation. Mit Klickraten argumentiert wie stehen Sie generell gegenüber Klickraten? #00:26:53-7#

Experte 4: Ich find, Klickraten überhaupt nicht aussagekräftig. Also nein ich muss viel vorsichtiger formulieren. Ich find Klickraten problematisch, weil ein Phishing Dienstleister, also eine Security Firma, war bei uns und hat gesagt: Problemlos, Sie können Phishing Simulationen fahren bei uns, wo 50% der der Adressaten darauf klicken werden. Jetzt kommt das aber. Es ist massiv abhängig davon, wie anspruchsvoll man da die Phishing Simulation auch macht. Also ich kann die sehr low Level machen, wo praktisch niemand hereinfällt, weil das so offensichtlich ist und ich kann die extrem anspruchsvoll machen, wo dann fast jeder drauf hereinfällt oder. Und dann /. Deswegen ist es eigentlich schon noch gut gewesen, im Rahmen der OptiPish Kampagne haben wir über 100 verschiedene Simulationen gefahren das man mit /. Das man wirklich unterschiedliche Schwierigkeitsgrade bei den Simulationen auch verwendet und darüber dann und das wirklich kontinuierlich macht und darüber dann eigentlich so mit den Mittelwerten arbeiten und dann die Klickraten auswertet. Ist aber in der Praxis extrem schwer und wie gesagt, mann läuft dann das Risiko und dass, die Leute einfach nur aggressiv werden, weil man sie so viel bespielt mit Phishing Simulation. Klickraten alleine sind mit Vorsicht zu geniessen würde ich sagen. Außer man verwendet vielleicht auch identische /. (unv., #00:28:43-5#) aber das geht auch wahrscheinlich nicht. Identische Simulationen über mehrere Jahre verteilt das Problem, dass man dann hat, ist das die Themen, das Thema an sich vielleicht nicht mehr aktuell ist. Ja. #00:28:57-9#

Severin Zimmermann: Ok vielen Dank, also in dem Fall wirklich Klickraten im Bezug auf Kontext und Schwierigkeitsgrad zu beurteilen. Dennoch gelten Klickraten sehr oft als Rechtfertigung gegenüber höheren Instanzen um einen Phishing Awareness Training fortzuführen oder durchzuführen. Sehen Sie hier Problematiken oder auch Chancen? #00:29:26-7#

Experte 4: Ja, also. Wir haben das natürlich auch gemacht und das ist tatsächlich, dass worauf die, worauf das Management schaut, oder. Aber wir müssen das immer mit eine "Sidenote" verknüpfen und immer darauf hinweisen: Hey die Zahlen sind mit Vorsicht zu genießen und die Zahlen alleine sagen nichts darüber aus wie dringlich oder nicht dringlich jetzt tatsächlich eine Phishing Awareness Kampagne sein wird? #00:29:55-4#

Severin Zimmermann: Ok, vielen Dank. Dann kommen wir ein /. Zu den technischen Fragen, und zwar bei Phishing Simulation, hatten Sie wahrscheinlich auch werden auch technische Vorkehrungen getroffen SPAM-Filter Anpassungen, Absender Whitelisting etc, damit die Mails auch wirklich ankommen, sehen Sie da Chancen oder Risiken im Zusammenhang mit diesen technischen Vorkehrungen? #00:30:26-3#

Experte 4: Ja also. Das Risiko ist natürlich, dass man kein echtes Szenario mehr hat, wenn man explizit für ein Phishing Simulation die Konfiguration anpasst, teilweise vielleicht auch noch sichtbar für die Benutzenden, dann hat man kein echtes Szenario mehr und beeinflusst dann auch wieder Klickraten. Wir haben aber die Probleme, wir haben die Probleme auch an verschiedenen Stellen und mussten eben für unsere Simulation Konfiguration anpassen. Also ich finde das problematisch. Chancen /. Chancen hab ich jetzt /. Chancen sehe ich jetzt irgendwie nicht ich sehe mehr Risiken. #00:31:18-3#

Severin Zimmermann: OK. Dann ist Phishing oft auch / . Oder nein, ich muss das anders angehen. Technische Sicherheitsmaßnahmen sorgen für oft ein falsches Vertrauen bei den Mitarbeitern. Sie haben es vielleicht vorhin angesprochen mit dem Mitarbeiter, der im Unternehmen dennoch klickt, obwohl er wusste das ist ein Phishing ist, weil ich weiß den Hintergrund nicht, aber vielleicht, weil er ein Vertrauen in die Technik hatte und dachte. Die Schutzmaßnahmen der ZHAW reichen aus und das abzuwerten ich teste das jetzt mal. War /. Wo sehen Sie da /. Also sehen Sie das als Problem? Oder wie stehen Sie demgegenüber? #00:32:07-8#

Experte 4: Ja, also das wird uns schon /. Also uns wird häufiger vorgeworfen, wenn einzelne Mitarbeitende Mails bekommen, Phishing Mails bekommen, wird uns vorgeworfen, dass unsere technischen Sicherheitsmaßnahmen nicht ausreichend wären, oder. Was die Mitarbeiter natürlich dahinter nicht sehen sind, ist die ganze Komplexität aber vieleicht ganz kurz um die Frage zu beantworten fällt nämlich auch Grad noch noch ein anderer Punkt ein. Ja, ich ich glaube wirklich, dass das technische Sicherheitsmaßnahmen für falsches Vertrauen sorgen. Ich hör das auch regelmäßig, oder das. Ich, weise aber trotzdem auch immer wieder darauf hin, dass die, also wenn ich Vorträge halte, auch zu dem Thema das technische Sicherheitsmaßnahmen alleine eben nicht ausreichend sind. Aber das

kommt nicht nicht bei allen Mitarbeitenden an. Ich muss jetzt ich gebe Ihnen jetzt hier auch für die Bachelorarbeit vielleicht nochmal kurz eine Zahl mit. Wir hatten in der Vergangenheit eine Auswertung gemacht und zwar bekommen wir in der ZAHW pro Monat etwa 4'000'000 Emails aus dem Internet zugestellt. Von den 4'000'000 werden mehr als 3'000'000 automatisch herausgefiltert. Also das sind Mails, die sind ganz offensichtlich als Phishing erkannt. Die haben irgendwie verseuchten Email Anhang oder sind irgendwie anders als schadhaft eingestuft, die werden wir werden grundsätzlich schon herausgefiltert und dann bei denen bei der Millionen oder knappen Millionen, die wir zu stellen in die Postfächer da ist natürlich immer mal wieder auch gut gemachtes Fishing dabei oder das kann durchrutschen ja. #00:33:59-4#

Severin Zimmermann: Das sieht sehr interessante Zahlen. Also eben ich komm selber auch aus der Praxis und kenne das Problem. Ich würde sonst einfach zur nächsten Frage übergehen, und zwar reichen ihrer Meinung nach technisch /. Schulungsmaßnahmen aus, oder sollten technische Ergänzungen mit einfließen und ich meine jetzt aber hier nicht eben, wie Sie es angesprochen haben, dass Blocking von Mails vorher, sondern für den User ersichtliche technische Warnhinweise beispielsweise, die dem User helfen, ein Phishing zu identifizieren auch wenn er eigentlich geschult ist? #00:34:43-4#

Experte 4: Das haben wir auch umgesetzt an der ZHAW aber nur für die, ne für den Bereich Finanzen und Services. Wir haben tatsächlich einen Banner entwickelt, der warnt, wenn eine E-Mail von außerhalb der ZAHW eingeht. Da steht dann in oranger Schrift steht dann Vorsicht diese Mail kommt von außerhalb. Das Problem damit ist das bringt gar nichts. Nach einer Woche nehmen die nehmen, die mitarbeitenden das nicht mehr war diesen Banner. Die sehen das einfach nicht mehr, man wird blind dafür. Also Ich /. Die technischen Warnhinweise halte ich nicht für nachhaltig, oder. Deswegen, man muss mehr machen als so etwas auf jeden Fall #00:35:37-4#

Severin Zimmermann: Bestens. Sie haben jetzt auch gleich meine ergänzende Frage damit beantwortet. D aher würde ich auch schon wieder zur nächsten Frage übergehen. Und zwar ist in der heutigen Zeit das Nutzen vom Mobiltelefon oder auch Tablets, Smart Watches etc. üblich und es werden auch auch immer häufigerMails darauf geprüft. Technisch funktionieren diese aber etwas anderes, also zum Beispiel das Hovern über einen Link zum diesen zu prüfen, ist auf dem Smartphone etwas ganz anderes als auf dem Desktop Rechner. Sollten also Ihrer Meinung nach die unterschiedlichen Plattformen im Schulungsmaterial inkludiert werden oder sehen Sie das eher als zeitraubend, diese Schulungsmaterialien anzupassen? #00:36:32-0#

Experte 4: Nein das finde sehr wichtig. Also man muss /. Was wir machen können ist, wir können auswerten welche Plattformen werden bei uns zu welchem Grad

genutzt oder? Und dann können wir die Schulung Schulungsunterlagen entsprechend auf die am häufigsten genutzten Plattformen Email Clients etc. auch ausrichten. Ich finde das wichtig, dass die Leute sich dann auch dort wiederfinden oder mit sich damit identifizieren können. #00:37:07-6#

Severin Zimmermann: Okay. Aber ich sehe, Sie würden das wirklich auswerten, wer nutzt welche Plattform und entsprechend auf den User die vom meisten genutzten Plattformen das entsprechende Schulungsmaterial zur Verfügung stellen. #00:37:22-4#

Experte 4: Ich glaub, das ist schwierig, Das ist aufwendig. Aber ich würde allen die Informationen für die am häufigsten genutzten Plattformen zur Verfügung stellen. #00:37:33-4#

Severin Zimmermann: Okay, sehr gut. Dann. #00:37:38-5#

Experte 4: Ich mein, was man machen kann, ist zum Beispiel an unserem Department A bei den Architekten da wird fast ausschließlich werden da Mac Geräte benutzt oder und dann kann man sagen Ok, das Schulungsmaterial für Sie für das Departmental A, das beschränkt man auf Mac Geräte müssen wir mit Windows gar nicht erst anfangen. Aber dann kann man dann einfach das Deck, was man zur Verfügung hat das Schulungsdeck das kann man dann einfach, dann schneidet man den Windows Teil halt weg oder. Kann man schon machen. #00:38:06-6#

Severin Zimmermann: Ok bestens, dann kommen wir zu Chancen und Risiken bei der Implementierung einer Meldeplattform. Mir ist bekannt, dass sie dies im OptiPish Projekt gemacht haben, so viel ich weiß war das glaube ich ein Button im Outlook, den Sie zur Verfügung gestellt haben und entsprechend im SOC Center eben die Mitarbeiter zur Verfügung gestellt haben, die die Anfragen bearbeiten. Das haben Sie auch bereits angesprochen 4 bis 5 Mitarbeiter, die damit beschäftigt waren. #00:38:41-6#

Experte 4: Ich glaube, da gibt es ein Missverständnis. Wir hatten eine Meldeplattform, aber das ist unser Servicedesk gewesen, das heißt, da kahmen dann Mails an Servicedesk@zhaw.ch, oder Anrufe beim Servicedesk. Wir haben keinen Button im Outlook drin gehabt, da wäre ich jetzt da bin ich jetzt irritiert, also ich bin mir da sogar sehr sicher, dass wir das nicht gemacht haben, weil wir im Moment überlegen diesen Button nämlich einzubauen. Also die Diskussion, die Führung wir aktuell, aber im OptiPish haben wir noch nicht gehabt. #00:38:41-6# #00:39:16-5#

Severin Zimmermann: Okay, dann hab ich vielleicht hier etwas missverstanden. Dann aber vielleicht Chancen und Risiken die sich sehen, wenn man eben solche Meldeplattform wie eben ein Button im Outlook oder sagen wir eine separate Homepage wo das gemeldet werden kann etc. sehen Sie da Chancen Risiken? #00:39:35-6#

Experte 4: Ich, sehe da in erster Linie Aufwände oder. Weil im Outlook können Mails schon relativ komfortabel als junk markiert werden. Wenn wir jetzt über einen Button, jede verdächtige Mail an den Service Desk schicken, dann generiert das einen gewissen Aufwand. Ich meine, man kann, muss dann überlegen was hat das für einen Sinn? Was erwarten wir von den von den Benutzern, wenn sie da drauf klicken? Was soll das auch auf der Seite zum Beispiel Security Monitor oder so dann auslösen? Was ist die Erwartungshaltung? Erwarten, die unsere Mitarbeitenden, wenn sie da auf den Button klicken, dass sie dann immer eine Rückmeldung bekommen irgendeine Bestätigung? Ja, das war jetzt Phishing, oder das war kein Phishing oder ist das einfach nur ein zur Kenntnisnahme, aber dann warum reicht denn der Junkfilter nicht einfach, wo man sagt OK Rechtsklick auf die Mail und Junk markieren? Also ich find das /. Ich bin noch nicht ganz überzeugt, ich weiß bei uns gibt es Bestrebungen, das umzusetzen, ich bin nicht überzeugt davon. #00:40:48-7#

Severin Zimmermann: Ok, vielen Dank. Das wäre es mit einem technischen Fragen gewesen, die nächste würde wieder das Umfeld betreffen. Sie haben hier bereits am Anfang Umfeld Aspekte genannt zu Beginn sind Ihnen vielleicht im Laufe des Interviews jetzt neue Umfeldfaktoren eingefallen, die erwähnt werden sollten, die Phishing Awareness Trainings beeinflussen können. #00:41:17-1#

Experte 4: Ja, also klar kurz zur Kultur habe ich jetzt schon bisschen was gesagt oder. Rechtliche Einflüsse natürlich Urheberrecht, Markenrecht und so, das muss berücksichtigt werden. Und ja. Also ich find wichtig zu bedenken, dass vielleicht /. Ah ja ich glaube, da können wir später auch noch dazu. Das bleibt ja, wenn ich so einen Phishing Awareness Training mache innerhalb einer Organisation, das bleibt nicht in der Organisation es geht raus! Und wir hatten das in der Vergangenheit auch, dass uns von Mitarbeitenden tatsächlich das Nationale Cybersicherheitszentrum informiert haben, über die Phishing versuche. Die sind direkt auf das NCSC gegangen und das NCSC ist dann wieder zurück gekommen zu uns und hat gefragt was macht ihr denn eigentlich? Es bleibt nicht, es bleibt nicht in der Organisation, wenn man so etwas macht. Irgendjemand geht damit nach draußen und das kann sein, dass sie damit an die Presse gehen, es kann sein, dass sie damit an die Markeninhaber gehen es kann sein, dass sie das eskalieren an so zum Beispiel Polizei oder an irgendwelcge Behörden und oder ans Cybersicherheitszentrum also ist /. Und es kann noch ganz andere Effekte haben, an die ich jetzt vielleicht ganz denke. Aber dessen muss man sich bewusst sein, wenn man das Fährt. #00:42:41-8#

Severin Zimmermann: Ja, Sie haben es angesprochen, wir werden nachher sicher nochmal auf das eingehen. Dann kommen wir zu externen Partner. Jetzt da ich mich vorhin geirrt habe, so viel ich weiß haben Sie einen externen Partner im OptiPish Projekt mit einbezogen. #00:43:03-6#

Experte 4: Ja, genau. #00:43:05-0#

Severin Zimmermann: Sehen Sie bei externen Partnern vielleicht Chancen, die sich ergeben, wenn ich mit einem externen Partner einen Phishing Awareness Training durchführe oder auch Risiken, die dadurch entstehen können? #00:43:17-5#

Experte 4: Also Vorteile sind sicher.Man kann dann von echten Szenarien, die vielleicht auch bei anderen Unternehmen schon erfolgreich waren oder gut angekommen sind, kann man profitieren kann man die wiederverwenden. Die externen Partner haben oft schon mit Markeninhabern abgeklärt, ob das ob diese einzelne Szenarien dann auch genutzt werden können, davon kann man sicher profitieren. Und man spart sich dann natürlich den ganzen Aufwand, irgendwelche Kampagnen selber zu bauen, sondern das wird bereitgestellt oder das sicherlich viele Vorteile. Ja. Nachteile sind vielleicht, dass die Partner die Organisationskultur selber nicht nicht gut kennen, aber der braucht entsprechenden Sparring-Partner intern, der das vielleicht sagt, das kann bei uns gut funktionieren, das funktioniert bei uns nicht gut. #00:44:15-5#

Severin Zimmermann: Ok, hier ergänzend. Sehen Sie vielleicht ein Risiko, da Ich sag jetzt mal der externe Partner auch sensitive Daten unter Umständen hat wie die Mail, Adresse und Namen, falls es dazu einen Dataleak kommt und dann die Daten für ein vielleicht von echten Fischen genutzt werden. #00:44:37-5#

Experte 4: Das Risiko würde ich als sehr geringe einstufen. Und selbst dann selbst wenn es /. Also (unv., #00:44:49-8#) Jetzt muss auch vorsichtig sein. es kommt drauf an, wie es implementiert ist, dann letztlich, oder. Wenn das ein vertrauenswürdiger Partner ist und wenn Benutzer dann auf eine zufällige Login Seite gelockt werden und dort ihr Passwort auch eingeben und der der Dienstleister ist kompromittiert oder Dienstleister speichert diese Eingaben von den Passwörter der Nutzer im Rahmen des Simulation, dann ist es nicht mehr akzeptabel, oder. Also passworteingaben dürfen auf keinen Fall gespeichert werden, weil die müssen komplett ignoriert werden. Ansonsten ja nur Benutzername und Emailadresse, da gibt es noch genug genug andere Datenleaks bei anderen Unternehmen passiert kontinuierlich. Das darf eigentlich für ein Unternehmen alleine kein kein großes Risiko mehr sein Heutzutage glaub ich. #00:45:40-4#

Severin Zimmermann: Sehr gut. Dann nochmals ergänzend. Wie sehen Sie das mit ausländischen Partnern im Ausland gelten vielleicht andere Rechte auch bezüglich den Markenrechten diese genannt haben oder auch Sicherheitsvorkehrungen für ihr eigenes System? #00:45:58-9#

Experte 4: Ja also ich glaube auch das der Sitz des ausländischen Partners muss über ein vergleichbares rechtliches Niveau verfügen wie die Schweiz oder also muss vergleichbar sein. Ich finde EU Ausland wäre auch noch akzeptabel, weil wir uns ja letztlich alle irgendwie an der DSGV auch orientieren. Auch was Meldepflichten angeht bei Sicherheitsvorfällen usw ist es ja ähnlich. Aber jetzt bei anderen Anbietern hätte ich da Bauchschmerzen, wenn der Anbieter irgendwie eben in Nigeria, China oder so oder im Iran sitzt, da hätte ich damit mehr Bauchschmerzen, oder in Russland. #00:46:40-4#

Severin Zimmermann: Ok, vielen Dank. Jetzt die nächste Frage betrifft die rechtlichen Aspekte hier haben sie aber schon diverse genannt, deshalb hier nur noch ergänzt die Frage, ob sie hier noch etwas ergänzen wollen oder ob das so in Ordnung ist. #00:46:58-9#

Experte 4: Nein, nein ich hab da nichts weiter zu ergänzen, eben Markenrecht, Urheberrecht gilt es zu beachten und der Datenschutz haben wir auch gerade gehabt ja. #00:47:11-4#

Severin Zimmermann: Sehr gut, jetzt sind wir beim Punkt, wo Sie vorhin erwähnt haben, mit externen Parteien, Regierungsinstitutionen, Horster, Registrar etc. die zwingend über die Durchführung eines Phishing Awareness informiert werden müssen. Wollen Sie das vielleicht noch etwas weiter erläutern, oder? #00:47:31-4#

Experte 4: Ja, also eben das Hoster registrat stimmt, ich erinnere mich jetzt auch da hatten wir einen Austausch, die sind auf uns zugekommen genau. Ja ansonsten das NCSC werden wir zukünftig auch immer informieren, wenn wir bisschen Kampagnen fahren. Switch als Betreiber des schweizerischen Hochschulen und Forschungsnetzes, die müssen auch informiert werden. Ja. #00:48:06-7#

Severin Zimmermann: Sehr gut. Wissen Sie vielleicht auch, weshalb diese Parteien informiert werden sollen? Also eben beim NCSC haben sie ja bereits gesagt, dass die, weil die sonst auf sie zukommen und fragen, was sie machen bei den anderen? #00:48:23-1#

Experte 4: Ja, die Hoster und Registrare haben damit gedroht, unsere die in der Fisch und Kampagnen genutzten Domains zu sperren also sie haben gedacht die werden nur zu Phishing zwecken verwendet und haben damit gedroht, die zusperren, wenn wir ihnen keine Rückmeldung geben. #00:48:39-5#

Severin Zimmermann: Ok, bestens, vielen Dank. Dann sind Ihnen vielleicht Meldepflichten bekannt, die im Falle eines echten Phishing vorliegen? #00:48:50-7#

Experte 4: Ja Also eigentlich ein Phishing alleine eher nicht. Aber wenn, Daten abfließen, wenn es ein Daten Leck gibt oder dann gibt es natürlich Meldepflichten, an unsere kantonale Datenschutzbeauftragte für uns jetzt in erster Linie. Wir würden aber sicherlich auch Switch und eben das NCSC informieren aber jetzt nur weil wir eine eine Phishing Mail zugestellt bekommen, wo niemand drauf klickt, da würden wir dann jetzt nicht keine keine Meldung erstatten. #00:49:29-3#

Severin Zimmermann: Sehr gut, dann wären das alle meine Fragen gewesen sind aus Ihrer Sicht noch Punkte, die wir nicht ausreichend behandelt haben oder Ergänzungen die Sie gerne anbringen wollen? #00:49:43-7#

Experte 4: Ne, ich glaub ich hab zwischendurch schon immer ein bisschen was gebracht ja. #00:49:49-3#

Severin Zimmermann: Sehr gut, dann noch eine Frage von mir. Ich werde noch weitere Interviews durchführen. Eventuell ergeben sich darin neue Aspekte, von denen ich auch gerne ihre Meinung hätte dürfte ich Sie in diesem Fall nochmals kontaktieren. #00:50:04-7#

Experte 4: Ja, sicher. #00:50:05-8#

Severin Zimmermann: Sehr gut, besten Dank dann würde ich nun die Aufzeichnung beenden.

H Transkript Experten-Interview Experte 5 und 6

Administratives		
Interview Datum	20.04.2023	
Interview-Partner	Experte 5	Experte 6
Arbeitgeber	ZHAW	
Aufnahme OK?	Ja	Ja
Anonymisierung Daten?	Ja	Ja

Severin Zimmermann: Jetzt muss ich noch kurz die Sprache Annpassen des Transkripts. Dann würde ich mit der ersten Frage beginnen und zwar, Experte 5, sind dir bekannt, die im Rahmen eines Phishinge während des Trainings entstehen können? #00:00:27-5#

Experte 5: Positive Aspekte, ja klar, also positive Aspekte können entstehen, dass die User sensibilisiert werden auf ein gewisses Verhalten, vor allem auch trainiert werden, wie man mit Phishing umgeht und Phishing-Kampagnen haben auch den Vorteil, dass man thema-basierend die richtigen E-Learnings zuweisen könnte oder kann. #00:00:58-1#

Severin Zimmermann: Ja, sehr gut. Experte 6, entstehen aus deiner Sicht auch entsprechend positive Aspekte? #00:01:03-9#

Experte 6: Also ich kann mir gut auch vorstellen, dass man ein bisschen das Interesse an Security wecken kann dadurch in Personen, also dass Personen sich eher dafür interessieren, weil sie näher an das Thema herangezogen werden und dass sie merken, dass das effektiv ein Problem sein kann und dass sie auch zum Beispiel auch in ihrem Privatleben damit Vorteile ziehen können. Sowas in die Richtung. #00:01:37-8#

Severin Zimmermann: Sehr gut, das sind sehr gute Punkte. Ich würde jetzt gerade ins Gegenteil wessen, und zwar sind euch auch negative Aspekte bekannt? #00:01:48-0#

Experte 5: Leider aus meiner Sicht mehr negativ wie positiv, weil Phishing ja sensibilisiert, klar, man muss es aber richtig gestalten. Phishing Training ist auch,

man darf es nicht missbrauchen, man muss es wirklich zum Sensibilisieren nutzen und nicht nur zum Management irgendwelche Zahlen abgeben. Es ist nämlich ganz einfach aufzubauen, dass das Management mit dem zweiten Training anschliessend zufrieden ist, indem man den Level dementsprechend anzieht. Zahlen zu produzieren ist mit Phishing was ganz was einfaches, die sind aber verfälscht. Das ist das große Problem meiner Meinung nach an dem Ganze. Auch was das Problem sein ist, je nachdem wie man Kampagnen aufzieht, kann eine Kampagne, die zu viel gefahren wird, wie könnten abstoßend wirken, sodass man den User eigentlich veregrault und mit der Zeit der Abstumpft, also es muss ein gesundes Mittelmaß gefunden werden. Und das kann man nicht irgendwie pauschalisieren. Man muss da ein Feeling aufbauen, wie es bei einem am besten funktioniert. #00:02:52-4#

Experte 6: Genau, also da kann ich dir eigentlich nur zustimmen, Experte 5. Ich kenne ja, also ich habe noch andere Kollegen, die an der ZHAW arbeiten und von denen höre ich ab und zu mal wieder, also vor allem während wir bei diesem ganzen Optifish-Projekt waren, habe ich ab und zu mal gehört, "woah" schon wieder eine Phishing-E-Mail von euch, was soll das? So Zeug ist sicher für die User nicht angenehm. Was ich noch vielleicht dazu ergänzen kann, ist auch ein wenig, wie man damit umgeht mit den /. Also nicht mit dem Resultat, sondern mit der Phishing Kampagne an sich, dass man aufpassen muss, dass wenn die Leute sowas melden, dass dann auch darauf richtig reagiert werden kann, damit die Leute dann nicht das Interesse am Melden verlieren zum Beispiel oder. Also bei uns, zum Beispiel in meiner alten Firma, bei uns die internen Prozesse waren während solchen Phishing-Angriffen nicht so gestrickt, dass man richtig darauf reagieren konnte zum Beispiel. Und das macht dan /. Das kann die Leute für uns sichern. #00:04:02-9#

Severin Zimmermann: Sehr gut. Ihr habt jetzt beide eigentlich organisatorische Aspekte genannt, wie das mit den Zahlen ist, dieses im Management zu präsentieren. Da kommen wir auch nachher noch bei den Detailfragen nochmals drauf zu. Sind euch auch technische Aspekte bekannt, die im Rahmen eines Phishing Awareness Trainings beachtet werden sollten? #00:04:26-2#

Experte 5: Klar, man muss, so Phishing Kampagnen darf man nicht oft mal rauslassen, sondern das muss gestaffelt werden. Einfaches Beispiel, dadurch entsteht Flurfunk, der ist eigentlich beim richtigen Phishing Vorfall sehr wertvoll, aber für eine Kampagne, der verhindert einen oder vermisst einem das erwartende Ergebnis. Man muss auch sicherstellen, dass der Lerneffekt durch die Kampagne durch gute E-Learnings unterstützt wird und was auch ganz wichtig ist, was ich durch viele andere Austausche gelernt habe, man muss Kampagnen vorher ankündigen, damit der Faktor des Verarschens kommt sonst gern beim User vor und soll sich darauf vorbereiten, und weis "Jawohl", da kommt was. Jetzt wird niemand gern unvorbereitet getestet, sagen wir es mal so. #00:05:21-2#

Experte 6: Ja, der eine Punkt, den ich mir noch anmerken kann, ist auch aus dem Optifish-Projekt die Legalität vom dem Ganzen. Wir hatten dort offensichtlich, ich war noch nicht so stark involviert, hatten wir das Problem, dass wir bei diesen Phishing Angriffen "naja" haben wir echte Marken verwendet und unsere Mitarbeiter haben dann diesen echten Marken Mails zukommen lassen, so von wegen, warum sie uns SPAM zusenden und das konnte dann zu legalrechtlichen Problemen führen, weil eigentlich offensichtlich ist das nicht so toll, wenn man jetzt hingeht und sagt, "jo" ich nehme jetzt das Logo von Amazon für einen Phishing-Angriff zum Beispiel. Ich glaube nicht, dass wir Amazon verwendet haben, sonst ja anyway. Also das ist sicher auch noch eine technische Applikation, die existieren kann. #00:06:20-4#

Severin Zimmermann: Sehr gut. einfach /. Oder die Aspekte, die ihr jetzt genannt habt, also sprich, das mit dem Gestaffelten, das habe ich persönlich in meiner Arbeit mehr als organisatorisch und zwar die Bestimmung des Intervals definiert, da kommen wir noch darauf ein, nicht dass ihr dann verwirrt seid, weil es jetzt bei mir organisatorisch fällt. Das bezüglich Markenrecht fällt bei mir ins Umfeld, da es dann rechtliche Aspekte sind. Vielleicht ein kurzes Beispiel, im technischen Bereich, da habe ich zum Beispiel Firewall-Regeln, die erstellt werden, damit diese Phishing-E-Mails, diese Training Phishing E-Mails auch wirklich beim End-User ankommen. Vielleicht mit diesem Input habt ihr noch technische Aspekte, die jetzt euch in den Sinn kommt. #00:07:21-2#

Experte 5: Ja, also Firewall ist jetzt vielleicht der falsche Ausdruck, das würde ich jetzt korrigieren. Es ist eher ein Whitelisting, damit die Mails mit dem gewissen Inhalt nicht blockiert werden. Es müssen auch Header und Bodies, wenn man einsetzt, zur externen Warnung zum Beispiel, die setzen wir an der ZHAW ein, die müssen natürlich in der Phishing-Mails auch berücksichtigt werden zum Beispiel. Und das Ganze, ganz wichtig ist auch, dass die Infrastruktur, also der Service-Desk vor allem, der muss auch informiert sein. #00:07:52-6#

Experte 6: Genau, also das zu dem Punkt, vielleicht wegen diesen ganzen Header und all dem Zeug. Es muss eigentlich sichergestellt werden, dass am User die E-Mail so präsentiert wird, wie ein echter Angriff auch präsentiert würde. Also, dass sie auch die Chance haben, mit allen Mitteln zu arbeiten. Also, dass die URLs, die drin sind, dass die zum Beispiel ebenfalls mit, keine Ahnung, wenn jetzt sie einen URL shorten oder intern verwenden, wir haben zum Beispiel das ganze Microsoft-Portfolio, da hast du auch die Secure-Links zum Beispiel, dass auch Secure (unv., #00:08:30-2#) verwendet werden für diese E-Mails, also in diesen E-Mails drin. Dass wirklich eine Phishing-Mail genau gleich ist wie eine Test-Mail. Und ja, wegen Firewall, klar, natürlich. Theoretisch, im Normalfall muss man sie nicht öffnen, weil es sind ja keine böseartigen Webseiten dahinter, somit müsste theoretisch auch nichts geblockiert werden. Machen wir es einfach. #00:08:55-8#

Severin Zimmermann: Sehr gut, (unv., #00:08:57-2#) #00:08:57-6#

Experte 5: ich habe es Whitelisting genannt. #00:08:59-6#

Experte 6: Ja #00:09:00-5#

Severin Zimmermann: Ja, genau, also ich nenne es in meiner Arbeit auch Whitelisting, SPAM-Filter Anpassung, gibt noch andere Aspekte, da können wir aber dann noch drauf zu. Dann jetzt so mal als Überblick, ist das aus meiner Sicht gut oder habt ihr noch Aspekte, die euch jetzt gerade einfallen, die wir jetzt noch nicht erwähnt haben? #00:09:26-4#

Experte 5: Na, ist soweit okay. #00:09:29-4#

Severin Zimmermann: Okay, sehr gut, dann werde ich zu den Detail-Fragen übergehen. Und zwar die erste /. Also jetzt behandeln wir auch wieder zuerst organisatorisch, dann technisch, dann Umfeld. Das erste, das ich als organisatorisch eingestuft habe, ist, dass es sehr oft erwähnt wird, dass Phishing Awareness Training auf die User abgestimmt sein sollte, also sprich personalisiert auf bestimmte Eigenschaften der Benutzer. Seht ihr da Chancen oder Risiken, wenn ich solche personalisierte Phishing-Simulationen durchführe? #00:10:05-3#

Experte 5: Man muss es teilweise sogar machen. Es gilt ja unterschiedliche Bedürfnisse in den Teams und dementsprechend, wenn man so Phishing Kampagnen fahren will, mit erfolgt, muss man sich auch auf die Thematiken oder auf das Umfeld von dem User, muss man sich dann einlassen. #00:10:22-3#

Experte 6: Genau das, also im Endeffekt muss, sollten solche E-Mails, Phishing-Kampagnen abgestimmt sein, auf Job zumindest. #00:10:33-4#

Experte 5: mhm (bejahend) #00:10:34-6#

Experte 6: Also Wenn ich jetzt zum Beispiel, ich bin jetzt Techniker und wenn ich jetzt eine Phishing-Mail kriege, im Sales-Portal XY ist irgendwas für dich, dann ist die successalary rate relativ tief, würde ich jetzt behaupten. Hat aber auch so seine Vorteile natürlich, wenn man auf ein bisschen alles trainiert, also dass man

nicht nur extrem spezifisch arbeitet. Aber im Endeffekt, wenn man möchte einen hohen Effekt erzielen, ist es wahrscheinlich gut, wenn man eher auf die Rolle von der Person eingeht. Ja. #00:11:12-3#

Severin Zimmermann: Sehr gut, also dann verstehe ich das richtig, dass Personalisieren macht Sinn, um einen besseren Effekt des Phishing Awareness Trainings zu erzielen. #00:11:22-1#

Experte 5: Auf alle Fälle, weil ein Fallstor oder man spricht auch immer von human factor, das heißt ganz ein banales Phishing, das erkennt ein Normal-User im Regelfall, aber man muss heutzutage mit gezielten Angriffen rechnen und dann kommen eben sogenannte personalisierte Mails und die müsste man dann eben auch erkennen, darum ist der Fokus sehr wichtig. #00:11:45-8#

Experte 6: Ja sehe ich schon auch so, also mit diesen Maßnahmen gehe ich primär halt gegen SpearPhishing-Angriffe vor eigentlich oder also mit personalisierten. Ich weiß natürlich nicht, ob es Sinn macht nur auf SpearPhishing zu trainieren oder ob es auch Sinn ergeben kann beides zu trainieren. Ich hätte jetzt behauptet, wahrscheinlich macht es Sinn, dass man auch genereller trainiert. #00:12:11-2#

Experte 5: Man darf halt auch nicht zu primitiv werden, da kann man sich den Experte 6 unterstützen, weiles ist so, dass wir heute technisch so gute Abwehrmaßnahmen haben, dass sehr wenig Phishing eigentlich durchkommt und so ganz banale Sachen im Regelfall gar nicht mehr auftauchen und durch die Banalität dann eigentlich schon wieder der Verdacht bei Usern, ey das ist eventuell ein Test. Also es ist immer zweitsteidiges Schwert. #00:12:36-3#

Experte 6: Richtig, es ist nicht ganz so eine simple Angelegenheit. Wir haben ja auch ab und zu mal erfolgreiche Phishing Angriffe bei uns, bei denen man sagen muss, "Jo" ein normaler Mensch müsste da nicht reinfahren. Und ich sage /. Also ich habe vorallem sowieso das Gefühl, dass weil halt die Sicherheitsmechanismen meistens dann versagen, wenn die E-Mails halt eben keine URLs, keine Bilder, kein Nichts behalten. Ja, das sind aber auch sehr schwierige Sachen zum Trainieren, zum Phishing Simulationen machen, weil dort geht es ja um eine direkte Interaktion mit dem Benutzer. Das heißt, der Experte 5 müsste dann Fake-E-Mails austauschen mit unseren Mitarbeitern. Ich weiß halt nicht, wie effizient das ist. Vielleicht in Zukunft mit AI-getriebenen Mitteln ein Thema. Ich weiß es nicht, aber da könnte ich mir jetzt persönlich vorstellen, dass es dort noch wie Bedarf gibt oder einen gewissen Spielraum zum Herumspielen, weil diese Angriffe genauso gefährlich sein können. #00:13:43-5#

Severin Zimmermann: Sehr gut, danke vielmas für die Ergänzungen. Jetzt vielleicht auch hier im Gegenteil. Seht ihr dann Risiken, wenn ich einen Phishing personalisiere und auf die Benutzer abstimme? #00:13:58-1#

Experte 6: Ja, Experte 5, ich habe sonst nur eigentlich, wie ich es vorhin schon gesagt habe. #00:14:10-5#

Experte 5: Ja, es ist das zweischleilige Schwert, wie er will. Jetzt könnten wir das einfach umdrehen und argumentieren andersrum. #00:14:18-0#

Experte 6: Genau so. #00:14:20-9#

Severin Zimmermann: Okay nein, dann ist das Gut, dann würde ich es dann zur nächsten Frage übergehen.Und zwar ist das ja auch das Phishing Training selbst kann sehr unterschiedlich gestaltet werden. Ich kann präventive Schulungsmaßnahmen machen, indem ich die Leute in einen Klassenraum sende oder ein Schulungsmaterial zustelle und sie sollen das absolvieren. Ich kann es eben wie auch im Optifish-Projekt als Embedded-Schulung machen, also sprich ich sendesimulierte Phishing Mails. Dann auch die Inhaltsgestaltung, sei das als Game, als Video, als Textdokumente, was auch immer. Da gibt es ganz unterschiedliche Möglichkeiten. Ich habe das alles als Schulungsbestimmungen oder Aufbau einer Schulung kategorisiert. Wie seht ihr das mit solchen Aufbau-Methoden? Sind das wichtige Punkte, die man beachten sollte? Bergen vielleicht auch Risiken oder sollte einfach ein Phishing-Awareness-Training durchgeführt werden, egal wie? #00:15:27-8#

Experte 5: Also man muss die Umstände sicher berücksichtigen und ein typisches Phishing ist, wie wir es kennen per Mail. Und davon gibt es Untervarianten, vishing also visuell. Giebt es auch smishing auch wieder eine Untervariante davon. Man darf auch nicht vergessen, ist zwar jetzt auf dem Aussterbenden, aber immer noch sehr erfolgreich. USB-Sticks auslegen, auch sehr erfolgreich. Heute noch viel gängiger QR-Codes Überkleben, auch sehr erfolgreich. Da gibt es sehr viel, ja, Handlungsraum, wo man da Phishing fahren kann. #00:16:10-7#

Experte 6: Ich glaube da gehts jetzt eher /. Also von mir aus geht es jetzt eher darum, wie solche Trainings aussehen können oder? Also so in welchem Art. #00:16:22-9#

Severin Zimmermann: Vielleicht kurz, wenn ich darf eben es geht /. Oder in meiner Frage geht es vor allem darum, gibt es Chancen oder Risiken, wenn ich eben bestimmte Methoden anwende oder eben nicht. Also wie macht es Sinn und welche Chancen und Risiken entstehen, wenn ich eben das Phishing unterschiedlich gestalte? Oder das Training, so nicht das Phishing? #00:16:45-4#

Experte 6: Genau, das Training eigentlich, ja. Was soll man dazu sagen? Ich kenne nur /. Ich bin sowieso immer sehr negativ angestellt, dementsprechend, ich kenne halt eher die negative Seite. Zum Beispiel, ich kenne es aus meiner Zeit, dass ich kurzfristig für UBS-Aufträge erledigen musste. Die haben zum Beispiel, du musst pro Monat 20 oder 30 Trainings durchlaufen und im Endeffekt hat es keinen positiven Effekt. Weil Maximum klicken die Leute einfach durch. Wenn es noch eine Prüfung gibt, dann gibt es irgendjemand, der das sowieso einigermaßen besteht, macht Screenshots von allem, verteilt die, "let's go" also. Für mich ist es extrem wichtig, wie das gestartet wird. Oder weil Leute haben meistens sowieso schon keine Lust drauf und es muss ein gewisses, es muss ein etwas Spaß machen. Es kann nicht /. Also wenn es langweilig ist, machen es die Leute sowieso nicht. Das ist ein wenig mein Gefühl. #00:17:46-8#

Experte 5: Ja. Das ist ja genau das, was wir jetzt auch bei uns anstreben wollen, dass wir das Training selber interessant gestalten. Security ist ein "trockenes Thema". Man muss es auflockern. Wie du Experte 6 gesagt hast, es muss vielleicht auch mal ein wenig Humor dazu. Es muss Gamification ist das große Wort heute. Ja Die E-Learnings, die müssen natürlich auch dementsprechend gestaltet sein. Eventuell muss man sich auch identifizieren können ja durch irgendeine Kampagne oder Design, eine Bildsprache. (unv., #00:18:23-2#) Das wollen wir kennen, dass einem vertraut wird. Und Wenn man das Ganze nochmal zurück auf Gamification geht, dann kann man die Motivation erhöhen, indem man dann vielleicht durch Punkte erspielen Preise ausschreibt. Da kriegt man dann Leute auf. Aber da haben wir jetzt noch keine Erfahrungen dazu. Das sind nur so Sachen, wo ich gelesen habe und mir so Ideen sind, wo man implementieren kann. #00:18:47-8#

Experte 6: Genau, das sind grundsätzlich Dinge, die ich immer und immer wieder höre, so Gamification. Menschen lieben Preise und zwar, es ist scheiße egal, ob das ein echter Preis ist oder ob es nur einfach ich habe mehr Punkte als du. "That's it". #00:19:03-7#

Experte 5: Und wir machen das auch nicht so einfach. Klick auf den Link und du kriegst ein iPad. Man muss es schon mit Verdiener und Genification verknüpfen. Das sind auch so die neuesten Papers, die gehen alle in die Richtung. #00:19:20-5#

Experte 6: Genau, weil sonst, wenn du zum Beispiel hingehst und sagst, "Jo", ich mache jetzt einfach irgendwie ein Training, ich nehme alle Leute, steck sie in den Raum. Ich glaube nicht, dass das extrem zielführend ist, bzw. es kann zielführend sein für Leute, die das möchten. Und herauszufinden, wer Spaß hat daran, das wäre vielleicht der nächste Challenge. #00:19:43-7#

Severin Zimmermann: Sehr gut, dann würde ich das noch einmal kurz zusammenfassen. Also Risiko ist, dass wenn ich jetzt falsch mache oder nicht auf die User richtig abstimme, dass dann die Motivation tief ist und die User sich einfach "durchklicken" und gar nicht wirklich das Training absolvieren. Und positiv ist eben oder die Chance ist, wenn ich es eben entsprechend gestalte, die Motivation entsprechend hoch ist oder höher sein kann und die User sich oder das Training auch gerne absolvieren und so wahrscheinlich ein besserer Effekt erzielt wird. #00:20:17-1#

Experte 5: Es wird dadurch auch sicherlich Interesse fürs Training erwecken ja. #00:20:23-6#

Severin Zimmermann: Sehr gut, danke. Dann Experte 5, du hast es vorhin angesprochen und zwar das Informieren der Mitarbeiter. Hier spezifisch steht es sehr in Diskussion, ob das IT-Personal informiert werden soll, wenn ich Phishing Trainings bzw. Phishing Simulationen durchführe. Wie steht ihr dem gegenüber? #00:20:46-7#

Experte 5: Nein, warum? Klar, es gibt immer technische Leute, die müssen involviert werden aufgrund von dem, dass man die Phishing Kampagne technisch schon umsetzen kann. Aber ansonsten sind das normale User wie alle anderen auch, die im entsprechenden eventuell eine andere Anforderung an die Kampagne stellen und dementsprechend auch anders behandelt werden müssen. Aber es sind ganz normale Leute in der IT. #00:21:16-9#

Experte 6: Ja, bin ich bis zu /. Also bin ich eigentlich zu 100 Prozent gleicher Meinung. Ich habe eine Anekdote aus einem Phishing Vorfall, also Test in der letzten Firma. Dort hat man gemerkt, dass es eben doch Leute gibt, die informiert sein müssen. Und das Weil ich in der Security arbeite und wir haben das auch nicht mitgekriegt. Wir haben dann eigentlich einen Phishing Vorfall bei uns bemerkt, haben angefangen, die Gegenmaßnahmen einzuleiten und zum Glück hat jemand noch Whois-Einträge überprüft und hat gemerkt, dass die E-Mail /. Also die Domain, die benutzt wurde, zum Angriffen zu Info-Guard gehört. Und dann habe ich noch das Telefon in die Hand genommen und gesagt, hey lieber CISO, seit ihr /. Verarscht Ihr uns, seid ihr uns am Angreifen, weil wenn ja, musst du jetzt sofort sagen, stopp, weil sonst werden alle Phishing Mails gelöscht, weil wir sind eigentlich ready zum alles rauswerfen. Und Also im Endeffekt, die Leute, die

informiert werden müssen, sind sicher. Es gibt ein paar und vor allem die Leute, die zum Beispiel die Macht haben, solche Kampagnen zu stoppen, die müssen unbedingt informiert sein, weil ich hätte die Flächendeckung gestoppt und dann wäre ja /. Wäre überhaupt nichts rausgekommen bei dieser Aktion. #00:22:36-8#

Experte 5: Du bist in meinen Augen auch eine technisch involvierte Person. #00:22:40-9#

Experte 6: Ich hätte jetzt gesagt, eigentlich jetzt in der ZHAW nicht, weil da wären jetzt unsere SOC Personen, aber ich bin nicht SOC. Also ich sehe mich nicht involviert. Nicht mehr. #00:22:51-4#

Experte 5: Ja okay, können wir jetzt darüber streiten. Aber was auch wichtig ist zu informieren, ist einfach auch ein Service-Desk. Die wissen nicht, was kommt, aber sie wissen, dass was kommt, damit sie sich darauf einstellen können, dass vermehrte Anfragen reinkommen. #00:23:04-7#

Experte 6: Genau. #00:23:05-8#

Severin Zimmermann: Sehr gut, dann habt ihr die Frage so beantwortet, wie ich das eigentlich auch erwartet habe, sage ich jetzt mal, oder wie ich jetzt auch von anderen Interviews bereits gehört habe. Deshalb gehe ich zur nächsten Frage, die ist vielleicht etwas schwieriger auszulegen, und zwar geht es um die Cybersicherheitskultur. Und zwar steht auch oft in Diskussion, dass die Cybersicherheitskultur ein wichtigerer Aspekt ist als das Phishing Training selbst. Es ging aus meinen Interviews oft hervor, dass das eigentlich oder dass das Phishing-Awareness-Training Teil der Cybersicherheitskultur ist. Wie steht ihr dem gegenüber? #00:23:51-7#

Experte 5: Ja, also das Phishing Training steht hinter der Kultur. Das heißt, wenn die Kultur nicht stimmt, wirst du auch mit der Awareness Kampagne Phishing Probleme haben. Also es ist sehr wichtig, dass die Gesamtkultur stimmt und die User der Kampagne positiv eigentlich schon mal entgegenwirken. Also wenn man von vornherein ein negatives Bild hat, wird man auch mit dem Phishing anschließend kein Erfolg haben. #00:24:15-7#

Experte 6: Ja, das kann ich nur bestätigen. Also aus meiner letzten Anstellung haben wir auch immer gesagt, die Kultur ist für /. Du musst Security leben, damit Security wirklich funktioniert oder. Und ich finde das aber auch extrem schwierig.

Ich weiß nicht, ob ich das Ganze zusammennehmen würde, weil ich kann mir gut vorstellen, dass Phishing Awareness trotz allem helfen kann, auch wenn die Cybersecurity Kultur nicht so hoch ist. Also ich würde jetzt nicht behaupten, dass wir eine riesige Security Kultur haben in der ZHAW. Und dennoch habe ich das Gefühl, du kannst etwas damit erreichen. Die Frage ist natürlich, wie viel? Ich persönlich sage, Kultur ist wahrscheinlich wichtiger als Phishing Awareness, aber schwierig zu sagen. Ich glaube, es geht schon ein bisschen Hand in Hand, auch wenn es ein Subpunkt von Kultur ist. #00:25:16-4#

Severin Zimmermann: Sehr gut, vielen Dank. Dann die nächste Frage. Entschuldigung, behandelt die ethischen Aspekte? Und zwar, wenn ich Phishing-Simulationen durchführe oder auch Phishing-Awareness-Training, wird oft gesagt, dass es ethisch eine Grauzone ist. Wie seht ihr das? #00:25:39-3#

Experte 6: Keine Ahnung. #00:25:45-5#

Experte 5: Ja, ethisch ist immer sehr schwierig. Also ja /. Also es gibt Themen, die lässt man momentan besser ruhen, da klopft man nicht drauf rum, da macht man den User vielleicht, der zweifelt vielleicht fast. Also es muss immer die richtige Notwendigkeit, die richtige Balance gefunden werden zwischen dem ganzen. Also man kann wie zur Phishing-Kampagne die Leute schon demotivieren, und zwar gewaltig. #00:26:14-3#

Experte 6: Ja, also ich sehe erst dann ethische Bedenken, wenn zum Beispiel hingeht, sagst du okay, ich mache eine Phishing Kampagne, du kannst hier dein Username und Passwort eingeben, Username und Passwort eingegeben, Username und Passwort wird gespeichert. Dann habe ich langsam wir ethische Bedenken. Aber sonst bin ich jetzt nicht der, der sagt, dass ich jetzt da wirklich ethische Aspekte sehe. Also ich sehe es erst dann, wenn Daten generiert werden können, die problematisch werden für die Person, die gefischt wird. Also wenn wir selber dann zum Angreifer werden anstelle von Subträgern. Aber sonst habe ich jetzt da keine große Probleme. Was man vielleicht sagen kann, häufig geht das, so Phishing Awareness sachen, geht ja auch noch ein wenig in eine ähnliche Richtung wie Passwort knacken. Bin ich da wäre ich jetzt auch eher /. Hätte ich jetzt eher ethische Bedenken. #00:27:15-3#

Experte 5: Ja, man muss schon ein wenig aufpassen. Experte 6, du kennst es selber, wir hatten bei uns auch schon Leute im Büro stehen, die sind halt sehr sensibel, schon fast paranoid. Da muss man teilweise aufpassen. Und darum ist es auch gut, wenn man weiß, welches Team, das man gerade in die Kampagne einbindet, dann kann man so etwas vielleicht über das Weiß berücksichtigen. #00:27:35-9#

Severin Zimmermann: Sehr gut, vielen Dank. Jetzt kommen wir zum Thema, das hast du vorhin auch oder ganz am Anfang bereits angesprochen, Experte 5, und zwar Klickraten. Du hast da bereits schon erwähnt, müssen sehr vorsichtig betrachtet werden. Ich habe das so vernommen, dass eben vor allem auch halt die Klickraten, ich sage jetzt mal falsch generiert werden können, indem einfach beispielsweise, dass die Phishing Simulation schwieriger gestaltet wird und so die Klickraten künstlich hochgedrückt wird. Möchtet ihr hier noch etwas ergänzen? #00:28:15-1#

Experte 5: Eigentlich ist das genau das. Also Klickrate selber, sagen wir es mal so, wenn man verantwortungsbewusst mit umgeht, kann man einen Trend erkennen, aber generell ist kein Verlass drauf und ich halte auch nicht sehr viel davon. Mir ist es sehr wichtig, dass man die Leute sensibilisiert. #00:28:36-7#

Experte 6: Ja, ich sehe das eigentlich auch so. Das Wichtigste ist eigentlich, dass das Management keine Ansprüche an das hat. Also dass du eigentlich ein Management hast, die das anordnen, die wissen, dass es egal ist. Weil Fakt ist, "Jo" du kanst jedem /. Du kannst jede Person dazukriegen, drauf zu drücken und du kannst auch solche Sachen /. Ich meine Daten sind immer extrem schwierig zu interpretieren und ich glaube, es ist wichtig, dass das Management weiss, dass die Klickkarten zum Beispiel nicht unbedingt ein guter Indikator sind. #00:29:09-7#

Experte 5: Es gibt auch sehr viele Klicks, die sind bewusst ausgelöst von User, nur weil sie interessiert, wie es weitergeht. Andere nur, um uns zu ärgern. Also von dem her kann (unv., #00:29:21-2#) man die Klickkarten nicht voll. #00:29:22-5#

Experte 6: Es ist halt nicht so zuverlässig. #00:29:26-4#

Severin Zimmermann: Sehr gut, danke. Habt ihr auch gleich meine ergänzende Frage beantwortet. Jetzt auch schon ein Thema, das wir vorhin angesprochen haben. Und zwar eben technische Sicherheitsvorkehrungen anpassen. Eben Spamfilter, Absender Whitelisting. Ja, ich denke, hier gibt es sicher Chancen und Risiken. Habt ihr auch bereits ein paar erwähnt? Habt ihr noch Erkänzungen als Chancen oder Risiken, wenn man nicht solche Maßnahmen durchführt? #00:30:01-7#

Experte 5: Ich glaube, wir haben ja bis jetzt erwähnt, was so die Risiken sind.

Oder was man berücksichtigen muss. Das war eher in dem Punkt, dass man berücksichtigt, was man bei so einer Kampagne macht. Weil die Berücksichtungen sind ja auch die Risiken ausschließlich. #00:30:24-0#

Experte 6: Ja also ich was soll ich sagen /. Also ich finde es natürlich wichtig, dass man die Ausnahmen so definiert, dass nicht versehentlich ein echter Angreiffer dann mit dieser Ausnahme was anfangen könnte. Also wenn wir jetzt zum Beispiel,"Jo" ich weiß, Firma X, die verwenden CoFans und dementsprechend weiß ich, welche E-Mail-Adressen Whitelisted sind bei denen. Weil da gibt es eine Liste, ich habe diese Liste, "bueno". Aber wenn du einigermaßen schlau bist, dann weißt du, wie man ein Whitelisting macht. Also es funktioniert nur für, wenn CoFans angreifen und nicht jemand anderes mit der gleichen E-Mail-Adresse. Oder zum Beispiel von meiner alten Firma, ich habe mir die Domäne gekauft, die sie gerne verwenden zum Angreifen. Und ich könnte jetzt zum Beispiel diese Domäne verwenden, um sie angreifen. Aber trotzdem hoffe ich, dass sie ihr Whitelisting so gebaut hat, dass ich dennoch nicht durchkomme. #00:31:17-9#

Severin Zimmermann: Sehr gut. Also ich nehme an, du sprichst hier auch Mails-Spoofing an, dass natürlich das Ausnutzen solcher Whitelistings hervorrufen kann. #00:31:31-6#

Experte 6: Genau, dass du halt eben genau dennoch das Soofing-Filter aktiv lässt, dass du sagst, jawohl, du darfst mit dieser E-Mail-Adresse kommt durch alles durch. Aber nur wenn SPF Records läuft, wenn DMARC läuft, wenn der "Usual". #00:31:47-0#

Severin Zimmermann: Sehr gut. Dann zur nächsten Frage, und zwar solche technischen Sicherheitsmaßnahmen. Ihr habt das vorhin gesagt, ihr habt relativ viele technische Sicherheitsmaßnahmen, erkennt bereits relativ viele Phishing Mails. Das kann natürlich das Problem schaffen, dass die User ein falsches Vertrauen haben in die Technik und davon ausgehen, alles was ich bekomme müsste ja legitim sein. Da es von den technischen Sicherheitsmaßnahmen bereits abgefangen werden, hätte müssen. Wie seht ihr das? Stellt das wirklich ein Risiko da oder bringt vielleicht dann das Cyber /. Das Phishing Awareness Training sogar noch Chancen oder andere Risiken? #00:32:33-9#

Experte 5: Es ist definitiv so, dass falsche Sicherheit vermittelt wird, weil wir technisch sehr gut aufgestellt sind und technisch werden wir immer besser. Das ist ja auch das Problem mit unserer Phishing Kampagne, wenn das durchgeht, dann "riechen sie schon offt den Braten", weil wieso kommt das jetzt durch. Nichtsdestotrotz ist es umso wichtiger dann eben den sogenannten Human Factor zu stabilisieren oder zu stärken, damit er dann auch sensibilisiert wird, wenn mal sowas durchkommt, dass er das bewerten kann und er dann, was dann wieder Aufgabe

von der Phishing Kampagne ist, so ein Mail, wenn er unsicher ist, auf den Button, wo er gelernt hat, zu drücken, da draufklickt und uns das zur Analyse kann schicken. #00:33:16-1#

Experte 6: Ja, also ich sehe das schon auch so. Ja /. Ja ja nein es ist halt so, je weniger du damit konfrontiert bist, desto weniger /. Also desto weniger gehst du davon aus, dass es ein Problem darstellen könnte. Plus was halt vielleicht in eine ähnliche Sparte reinfließt ist, wir sind derzeit relativ sicher gegen Angriffsversuche X und jeden Tag kommen wieder neue Ideen bei den Angreifern und dort kann es dann Tatsache sein, dass es etwas durchkommt und die werden dann vielleicht auch eher als okay bewertet, weil die Menschen dieses System auch noch nicht kennen oder. Also ich weiß es, früher, also vor X Jahren gab es mal, gab es das noch nicht so viel, zu CFO Fraud und so war noch nicht so wirklich ein "Ding" und als das aufgekommen ist, habe ich das Gefühl, war die Trefferquote um einiges höher, weil du schickst eine PDF, Achtung, Rechnung, bla bla bla, gut hat es, die sehen das, jawohl, wird bezahlt, "let's go", "that's it". Und heutzutage, weil hast du weil das vermehrt aufgetaucht ist, hast du auch eine gewisse Härte gekriegt. Du bist ein wenig vertrauter mit der Materie, du schaust ein bisschen genauer, kann man vorstellen, dass das in eine ähnliche Sparte reinfließt oder. Aber sonst, ja, es ist eigentlich das typische menschliche Ding. Sicherheit ist nicht immer ein Vorteil. Man sieht zum Beispiel aus dem Autofahren, da gab es doch mal die Studie, dass man sagt, je mehr Sicherheit eingebaut ist im Auto, je heftiger werden die Unfälle, weil die Personen sich sicherer fühlen. Wenn du jetzt aber zum Beispiel einen, keine Ahnung, ein Messer im Lenkrad hättest und du weißt, wenn du einen Unfall machst, dann bist du tot, dann fährst du vielleicht viel, viel sicherer. Dann sagst du, ich fahre jetzt nur noch 30 kmh, weil ich weiß, bis 30 kmh kann ich mich selber abstützen, dass das Messer mich nicht trifft. #00:35:21-1#

Severin Zimmermann: Sehr gut. Danke dafür. Dann die nächste Frage. Reichen eurer Meinung nach Schulungsmaßnahmen für die Sensibilisierung der Benutzer aus oder sollten technische Erweiterungen hinzugefügt werden? Hier will ich jetzt nicht auf die technischen Maßnahmen, die das Phishing schon vorher abfangen, sondern wenn etwas durchkommt, beispielsweise Warnhinweise, ein Banner im Outlook, dieses Mail kommt von extern oder wenn ich auf einen Link klicke und gibt es ja so Add-ons im Browser, die das Prüfen und Warnungen anzeigt. Wie steht ihr dem gegenüber? Seht ihr da Chancen oder Risiken? #00:36:11-7#

Experte 5: Ja also (unv., #00:36:15-9#) wie soll ich das jetzt sagen. Die Hinweise und so weiter sind sicher auch wichtig. Und Was das Thema Schulung betrifft und so weiter, das alleine bringt es nicht. Man muss ständig präsent sein. Das ist jetzt auch meine Aufgabe hier an der ZHAW, zum Awarness ständige Präsenz zu zeigen, dass man immer wieder daran erinnert wird, dass überall mal so ein Reminder auftaucht, hey, denk dran, das ist so das wichtige Element. #00:36:49-8#

Experte 6: Ja Ich sagt zum Beispiel zu Banner, ich habe da ganz klar die Einstellung, ich finde Banners useless, wil du hast /. In der ersten Woche, in der der Banner eingeführt wird, sehen die Leute den noch und danach nie wieder. Der wird ausgeblendet vom Hirn, kannst "knicken", der hat "null Impact". Das mit Link Protection bin ich tatsächlich eher der Meinung, dass es etwas bringen könnte. Also im Sinne von, wenn du einen E-Mail /. Wenn du Link hast, der geht nach intern, kriegst nichts, alles okay, geht es durch und wenn du draufklickst, der geht nach extern, dass du eine klare Meldung kriegst zuerst, hey, sei dir bewusst, du gehst jetzt aus dieser Firma raus, könnte mir persönlich jetzt, also ich habe das Gefühl, es könnte helfen, weil die Leute, keine Ahnung, du kriegst eine Mail /. Ich kriege eine Mail von Experte 5, Experte 5 schreibt mir, ich habe da was im Intranet, ich klick drauf und dann kommt die Meldung, hey, du verlässt die ZHAW. Das hätte jetzt bei mir als Person zum Beispiel eher einen Impact als in einem behinderten Banner, weil der würde ich beim Mathias /. Also wenn der Experte 5 gespoofed wird, würde ich den genauso ignorieren. Dort sehe ich effektiv Potenzial. Ich bin aber sowieso grundsätzlich der Meinung, dass Phishing muss von Technik abgefangen werden, nicht von Usern, weil Benutzer sind schlichtweg nicht, also ich auch nicht, ich bin nicht in der Lage, zu meiner guten Phishing-Mail zu erkennen. Das heißt, meine Meinung ist sowieso, die Technik muss die technischen Probleme lösen. Wie, weiß ich noch nicht ganz so genau. #00:38:28-7#

Experte 5: Immer doch ständige Präsenz. #00:38:31-0#

Experte 6: Ja also nein zum Beispiel, wir hatten heute eine Diskussion darüber, Defender for Endpoint, unsere EDR-Solution, ob man es jetzt liebt oder nicht, ist eigentlich egal, überprüft zum Beispiel, wenn du das gleiche Passwort, das du verwendest, für uns auch in der Webseite eingibst, die nicht uns gehört. Und kann man sagen, hey, coole Aktion, weil "jo", das hilft natürlich, wenn ich jetzt sehe,ja, jemand hat eine komische Mail geöffnet, da hat eine komische Link darin gehabt und hat danach in diesem komischen Link sein Passwort eingegeben, ist für uns natürlich sehr vor Interesse. Auf der anderen Seite sind das dann so Aktionen, die die User vielleicht nicht extrem gut finden, weil das bedeutet ja, sie haben ein Tool, welches das Passwort überprüft und das ist auch nicht unbedingt so schön. Ich habe noch keine echte Lösung dafür, aber ich finde, es muss technisch gelöst werden. Weil ja, die armen User haben sonst schon echt andere Probleme. #00:39:32-5#

Experte 5: Ja, die werden mit der Zeit schon blind, aber da hilft auch der Hinweis, nicht eh, du verlässt jetzt, das liest du zweimal und dann liest du nicht mehr, du weißt, da kommt was und dann ist es egal, was kommt. #00:39:43-4#

Experte 6: Genau, aber du weisst, es kommt was, wenn du die ZHAW verlässt oder wenn du deine Firma verlässt, nicht, wenn du nach intern gehst. Oder weil

wir haben bei uns zum Beispiel das Problem, das muss dann auch richtig konfiguriert sein. Bei uns, bei unseren Teams, wir haben halt Webex, wenn dort eine URL aufklickst, dann kommt immer eine Warnmeldung und das zum Beispiel ist behindert, das geht gar nicht. Also wenn ich auf unseren internen Confluence gehe über Webex, dann kommt Link, Achtung, es ist ja, Entschuldigung, natürlich, ich gehe auf eine URL, ich bin bewusst, dass der Browser aufgeht und das ist useless. Also es muss dann schon richtig gemacht werden, weil sonst, eh, wie auch immer. #00:40:22-2#

Experte 5: Gibt das unnötige Incidents. #00:40:24-7#

Experte 6: Ja, ja, ja. #00:40:26-7#

Severin Zimmermann: Also vielleicht um das noch was zusammenzufassen, es kann durchaus Sinn machen, wenn es richtig gestaltet ist und nicht nur eben jetzt, ich sage jetzt mal, bei jeder Mail oder bei jedem Aufruf immer die Meldung kommt, da man sonst blind wird von diesen Meldungen, sondern wenn es in richtigen Maßen, im richtigen Kontext gemacht wird, könnte es ein zusätzlicher Faktor sein, der den Usern hilft, Phishing erfolgreich abzuwerden. #00:40:58-7#

Experte 6: Ja du kannst dir vielleicht so vorstellen, hast vielleicht auch schon gehabt, dass mit, keine Ahnung, gehst du mit Chrome oder Firefox oder so, gehst du auf eine Webseite, die nicht gerade so 100% vertranswürdig ist und sehr, sehr selten kriegst du ein richtig rotes Bild, Achtung, Warnung, hier ist was vielleicht komisch. Also es muss einen gewissen Seltenheitsfaktor haben. Also darf nicht die (unv., #00:41:19-4#) Grenze zusammen, sonst wirst du effektiv betriebsblind. #00:41:23-2#

Severin Zimmermann: Sehr gut, danke. Dann ein etwas anderes Thema und zwar sind wir heute sehr mobil unterwegs. Also wir nutzen sehr oft auch unsere Mobile Phones, Tablets, Smartphone Smartwatches, was auch immer, zum unsere Mails zu prüfen. Das Prüfen auf diesen technischen oder mobilen, technischen Geräten funktioniert aber meist etwas anders. Also wenn ich über einen Link Hover, funktioniert das auf dem Smartphone nicht zwingend oder wenn dann anders, wie auf dem Desktop Client. Auch ist der Bildschirm viel kleiner, es ist schwerer, eine URL richtig zu identifizieren. Wie seht ihr das? Sollte diese Technik oder diese Plattformen im Schulungsmaterial integriert werden oder seht ihr da auch Risiken, wenn ich das im Schulungsmaterial integriere? #00:42:15-9#

Experte 5: Also man muss es auf alle Fälle berücksichtigen, aber der Nachteil ist, die Vielfalt ist sehr groß. Also wir haben so viele verschiedene Devices und wie

du das schon richtig erkannt hast, wenn ich jetzt auf den Desktop einen Link anklickte, also typisch eh achtet auf den Link, das ist auf dem Mobile fast nicht machbar. Darum muss man auch auf verschiedene Phishing Hinweise oder Phishing Merkmale hinweisen, dass man , ja/.Das man mit der Zeit mehrere Varianten vielleicht ausmachen kann, was so ein Phishing ausmacht. Und wir wissen ja auch nicht, wenn wir die Kampagne fahren, auf welchem Device öffnet er jetzt das Mail, also auf dem gibt es wahrscheinlich einen sehr gesunden Mix. #00:43:04-4#

Experte 6: Ja, voll dabei. Also muss unbedingt beachtet werden. Also solange die Firma zulässt, dass E-Mails auf dem Handy aufgemacht werden dürfen, muss es auch trainiert sein, weil es ist effektiv so, wie du gesagt hast, Severin, es ist so, dass auf E-Mail /. Wenn du auf links klickst auf dem Handy, dass es sehr, sehr einfach ist, die Leute so sehr zu verwirren. Du kannst zum Beispiel einfach einen Screenshot von einer guten URL hoch reinkleben auf die Webseite und dann sieht für den User alles gut aus zum Beispiel. Weil ja das sind so Dinge, die funktionieren bei Handys extrem gut und dementsprechend ist dort auch das Risiko eigentlich viel höher. #00:43:52-0#

Severin Zimmermann: Sehr gut. Also vielleicht kurz, ich kann zwar antizipieren, was daraus die Chancen sind. Ich komme ja selber auch aus der Technik und kenne das auch. Wenn ich aber vielleicht trotzdem nochmals kurz die Chancen erläutert, die entstehen, wenn ich das berücksichtige. #00:44:09-9#

Experte 5: Also die Chance ist natürlich schon, dass man, ja, die verschiedenen Umgebungen trainieren kann, weil das Gleiche verschieden aussehen kann unter Umständen. Also es wird einfach mehr Wissen vermittelt in dem Ganze. Man merkt es ja, wie du gesagt hast, so ein Mobile, wenn ich das im Hochformat habe, stellt es nur quer, sieht die Welt teilweise schon ganz anders aus. Also die Erfahrung, wo der User mitmacht mit dem Umstand, die ist natürlich auch sehr wichtig. #00:44:41-3#

Severin Zimmermann: Sehr gut, vielen Dank. Ja, einfach, dass ich das auch dann richtig in meiner Arbeit erwähne und nicht behauptet wird, ich antizipiere hier Sachen rein, die gar nicht gesagt wurden. Die nächste Frage, hier geht es um interne Meldeplattformen und zwar wird oft mit Phishing Awareness Training auch eine Meldeplattform gestaltet, wo dann, sei das ein Button im Outlook, wo ich ein Phishing melden kann oder eine Webseite, wo ich ein Phishing melden kann, seht ihr beim Erstellen und zur Verfügung stellen von solchen internen Meldeplattformen Chancen und Risiken? #00:45:26-0#

Experte 5: Also es ist (unv., #00:45:28-9#). Also meiner Meinung nach ist das keine Chance und kein Risiko. Das ist schon eine Pflicht, dass man den User

darauf hinweist, wie er so ein Mail weitergibt, damit man das richtig von den richtigen Leuten untersucht wird. Und ganz wichtig ist auch zu vermitteln dem User gegenüber wieder, dass er keine Angst davor haben muss, dass er keinen Fehler macht mit sowas, weil oft ist auch Angst dahinter, dass wir sowas melden. Und jetzt zum Beispiel mit so einem Button erleichtert man so einer Person schon wieder um einiges, um einfach so ein Mail weiterzuleiten. Also von mir aus ist das fast ein Muss, die Möglichkeit zu geben, das zu melden auf irgendwelche Art und Weise und das so einfach wie möglich. #00:46:11-7#

Experte 6: Ja, genau. Also dass es ein Muss ist, bin ich voll bei dir. Als Chance sehe genau das eigentlich, dass vielleicht, wenn wir Glück haben, mal effektiv eine böse Mail gemeldet wird, dass wir diese analysieren können, dass wir auch verstehen oder lernen können, warum das durchgekommen ist. Risiko sehe ich schon ein bisschen, aber jetzt nicht unbedingt bei uns. Also gut, ein Risiko sehe ich schon. Wir haben Spezialisten, die Mails aus dem Junkmail Ordner melden. Das generiert einfach Aufwand für uns und für nichts, weil es ist ja schon aufgefahren, dass es schlecht ist. Aber ich sehe auch noch ein echtes Risiko für vielleicht kleinere Firmen. Häufig werden solche E-Mails genommen und man sagt, okay, vielleicht ist sie bösartig, ich melde die. Und dann gehen die häufig durch automatisierte Prozesse durch, zum Beispiel durch eine Sandbox. Und ich kenne /. Also ich habe früher Kunden gehabt, die dann hingehen, ja, "Jo" wir werfen jetzt das mal in eine Sandbox rein, die eher public verfügbar ist. Und dann hat man nachträglich gemerkt, das waren interne Daten von uns. Das stand zum Beispiel, das wäre jetzt für mich ein Risiko, dass man da hingeht und versehentlich, naja, echte interne Daten, die wichtig gewesen wären, nach aussen weitergeht. Also das sehe ich als Risiko wirklich, wil das habt ihr schon gelernt. #00:47:49-0#

Experte 5: Ja bei uns Nicht. #00:47:54-9#

Experte 6: Aberist zum Beispiel könnte zum Beispiel ein Risiko sein, ich nenne es mal so. Aber sonst ist es eigentlich nicht. #00:47:58-8#

Experte 5: Aus der Aussicht ist aber so ein Button sicherlich kein Risiko. Das Risiko besteht nachher, was machbar mit den Daten, wenn falsch mit umgegangen wird. Aber das ist meiner Meinung nach wieder ein anderes Thema . #00:48:07-1#

Experte 6: Genau aber auch das könnte ein Risiko sonst könntest du auch schlecht /. Also wir als Security-Team könnten auch schlecht darauf reagieren und somit /. Und dann lösen schlechte Gefühle aus. Und somit wäre es für mich schon auch theoretisch ein Risiko. Bei uns, wie gesagt, wir versuchen nur die Chancen draußen zu ziehen. #00:48:25-3#

Severin Zimmermann: Sehr gut. Also das sind sehr interessante Punkte, die rausgekommen, also auch das mit der Sandbox habe ich so bis jetzt noch nicht gehört. Sehr interessant. Jetzt würden wir etwas auf das Umfeld eingehen. Oder ich sehe gerade die Zeit. Ihr habt ja, glaube ich, ein bisschen mehr Zeit reserviert sehe ich das /. Oder ist das immer noch so? #00:48:50-4#

Experte 5: Ein paar Minuten haben wir noch. #00:48:54-2#

Experte 6: Na ja, sicher effektiv noch Zeit, das ist kein Problem. #00:48:56-5#

Severin Zimmermann: Okay, sehr gut. Dann zu den externen Einflüssen eben vielleicht nochmals generell. Experte 6 hat schon Punkte genannt, wie rechtliche Punkte. Habt ihr sonstige externe Einflüsse, die beim Phishing Awareness Training sollen? Also sprich mit Zusammenarbeit mit externen oder solche Punkte? #00:49:22-0#

Experte 5: Ja, also du hast es erwähnt. Also wenn wir natürlich solche Payloads nutzen mit externen Anbietern, dass es da Krawall gibt, ja, das kann ein riesen Einfluss sein. Was auch ein externer Einfluss sein kann, was ich vorher schon mal kurz erwähnt habe, also auf die Kampagne selber, das sind so aktuelle Themen, wo man vielleicht nicht gerade angreifen sollte mit so einer Phishing-Kampagne, wie jetzt Ukrainekrise oder Erdbeben oder sonst irgendwas, wo man momentan vielleicht einen User noch speziell aufgrüttet damit. Also das sollte man vielleicht noch runterlassen. Ja. #00:50:03-0#

Experte 6: Ja hat Vor- und Nachteile, das ist mir schon klar. Dort könnte man jetzt sagen, dass man vielleicht dann langsam in eine ethische Grauzone reingeht. #00:50:12-5#

Experte 5: Richtig, genau. Darum hatte ich das vorher schon mal mit erwähnt, weil das geht in die Richtung. #00:50:18-3#

Experte 6: Ja, bin ich dabei. Der Vorteil ist, wenn auch dort kein Tabus ist, weil es gibt natürlich Vorteile daraus, weil ja natürlich wird mit aktuellen Anlässen gephished. Also die Angreifer, die haben da weniger moralische Probleme als wir. #00:50:37-4#

Experte 5: Es soll ein Training sein und nicht igendwie eine moralische Demoralisierung soll man natürlich unterbinden. Man muss ja natürlich auch gefasst sein, wenn es so extreme also externe Einflüsse sind, dass man vielleicht auch einen persönlich damit dann verletzen könnte. Das passiert einem beim DHL wahrscheinlich weniger. #00:50:56-7#

Experte 6: Das ist so. Ja, aber sonst fällt mir jetzt auch nichts, wirklich intelligent sein zu dem Thema. #00:51:05-3#

Severin Zimmermann: Sehr gut. Wir kommen jetzt noch auf Detailfragen in diesem Bereich zu. Vielleicht fälll euch dann /. Oder fallen euch dann noch Punkte ein. Und war jetzt in der ersten Detailfrage geht es um die Zusammenarbeit mit externen Partnern. Oft wird mit Phishing Awareness, externen Partner eingebunden, teilweise auch SaaS-Lösungen verwendet. Seht ihr hier Chancen und Risiken, wenn ich mit externen Partnern zusammenarbeite? #00:51:34-8#

Experte 5: Selbstverständlich, das Ganze muss natürlich datenschutzkonform sein. Das ist jetzt A und O. #00:51:44-0#

Experte 6: Ja, aber sonst sehe ich jetzt kein Problem mit externen Partnern also wenn die externen Partner. #00:51:50-1#

Experte 5: Sprachlichen Probleme vielleicht auch aber das ist schon wieder etwas anderes. #00:51:54-6#

Experte 6: Also weniger als wenn wir es selber machen. Also wenn ich französisch schreiben müsste, da kommt nichts dabei raus. Also ich sehe jetzt persönlich eigentlich nicht wirklich ein direktes Problem damit. Ich sehe teilweise sogar Chancen, weil eben /. Du oder keine Ahnung jetzt ein CISO könnte hingehen und sagen, ich möchte jetzt wirklich mal uns damit testen. Also wirklich nicht nur Personen damit testen, sondern zum Beispiel auch die Security-Organisation damit testen. Und da hast du eher eine Chance mit einem externen Partner, als wenn du intern jemand nimmst, der in die Security eingebunden ist. Wie eben zum Beispiel aus meiner alter Firma. Die haben das dort jeweils gar nicht gemeldet und theoretisch /. Und für sie war das dann auch ein guter Indikator. Sie haben gesehen, die Security-Organisation hätte darauf reagiert. Hatten zwar nicht mehr sehr viel mit User-Awareness zu tun, sondern eher mit einem grundsätzlichen Test gegen die Firma. Aber ansnsten. #00:52:59-9#

Experte 5: (unv., #00:52:59-9#) Externe Partner haben auch einen Erfahrungsschatz, wo man von nutzen kann. #00:53:04-0#

Experte 6: Ebene genau das kommt natürlich auch dazu. Das ist aber eigentlich immer ein Argument für Outsourcing. #00:53:10-9#

Severin Zimmermann: Sehr gut. Vielleicht aufbauend auf diese Frage habt ihr Ergänzend Punkte, wenn ich das mit ausländischen Partnerfirmen mache. Oder seht ihr das dann gleich? #00:53:24-7#

Experte 5: Das haben wir davon schon gehabt. Also es ist genau das gleiche es muss datenschutzkonform sein. Von dem her ist es eigentlich egal, wo das ist, solange die Vorgaben erfüllt und eventuell die sprachlichen Probleme abhaben aber ansonsten. #00:53:38-1#

Experte 6: Genau. Also ich kenn auch das. Wir sind halt als als ZAHW sehr stark an Datenschutz gebunden. Dementsprechend muss halt das /. Also bei uns ist eigentlich der größte Negativpunkt. Bei allen ausländischen Sachen ist immer, dass wir zuerst das noch rechtlich abklären müssen. Es geht eigentlich in die gleiche Diskussion wie zum Beispiel Cloud, also SaaS, hin. Wenn die SaaS-Applikation, die wir verwenden, in der Schweiz gehostet ist, ist es eigentlich nie ein Problem. Sobald /. Wenn es in der EU gehostet ist, müssen wir uns darum kümmern. Kommt zu Rechtsdienst, "pa-pi-pa-pum". Für uns ist es einfach schlichtweg einfacher, wenn es bei uns ist. Das ist eigentlich eher ein spezifischer ZHAW #00:54:23-6#

Severin Zimmermann: Okey sehr gut. #00:54:25-8#

Experte 5: Aber wir haben wir haben ja für unsere Softwarelösungen sowieso einen eigenen Prozess, wo das mit geprüft wird. Das heißt, wenn das bei uns läuft, ist das eigentlich in Ordnung. #00:54:34-6#

Experte 6: Genau #00:54:34-9#

Severin Zimmermann: Sehr gut. Dann auch hier nochmals ergänzend. Seht ihr hier ein erhöhtes Risiko, wenn ich mit externen Partnern arbeite, da ich sag jetzt mal, wenn bei einem externen Partner ein Data-Leak entsteht, der ja quasi nicht von euren Systemen gemanagt wird, dass dann diese Daten genutzt werden, um

echte Phishings zu prüfen? Oder solltet ihr dieses Risiko eher geringen? #00:55:04-0#

Experte 5: Ich denke, das Risiko ist gering und Risiko hat manüberall. Das kann auch mit einer eigenen Lösung passieren ja. #00:55:16-1#

Experte 6: Jah sehe ich eigenlich auch so. Es ist natürlich so, dass größere Provider immer eher von Interesse sind, zum Angreifen. Also Was weiß ich, zum Beispiel SolarWinds vor ein paar Jahren war /. Also als Angreifer würde ich tendenziell, wenn ich Aufwand betreibe, würde ich sagen, ich greife entweder die einfachen an, also grundsätzlich "Low Hanging Froot" oder ich greife etwas heftiger an, wie zum Beispiel eine Microsoft oder eine SolarWinds oder was weiß ich. Und aus dem könnte man jetzt ein Risiko spinnen. Ich persönlich sehe es aber als weniger extrem, also ich sehe es jetzt nicht als riskant. #00:55:56-5#

Severin Zimmermann: Sehr gut, danke. Jetzt die rechtlichen Aspekte. Ihr habt jetzt vorhin schon Datenschutz genannt. Experte 6 hat Marktschutzrecht genannt. Habt ihr hier noch Ergänzungen von rechtlichen Aspekten, die bei der Durchführung eines Phishing Awareness Training beachtet werden sollten? #00:56:16-7#

Experte 5: Also das ist schon aus unserer Erfahrung das, worauf man achten muss. Also mir fällt da jetzt da spontan nichts weiter. Es ist aber ganz wichtig, Datenschutz und natürlich diese Payloads, die Vorlagen, die müssen natürlich auch abgesichert sein, dass man da nicht in rechtliche bredouille kommt. #00:56:33-9#

Experte 6: Genau, es geht eigentlich wirklich um das, und eben halt, dass man schaut, dass Passwörter zum Beispiel nicht aufgezeichnet werden. Aber da sind wir eigentlich auch wieder bei Datenschutz und so weiter und so fort. Das ist jetzt nicht so. Das ist für mich schon auch primär das. #00:56:50-0#

Severin Zimmermann: Sehr gut. Dann zu externen Parteien. Sind euch externe Parteien, beispielsweise Regierungsinstitutionen, Hoster, Registrar bekannt, die zwingend informiert werden sollten, wenn ich am Phishinger während des Trainings durchführe? #00:57:05-3#

Experte 5: Ja, vor allem wenn man Payloads benutzt, die nicht zulässig sind, dann kriegt man vom NCSC ganz schnell eins "auf die Mütze". Ja, also bei uns

ist es so NCSC und wir haben noch die Switch an der Seite, die im Hochschul verbunden mit drin ist. Und viele Hochschulen sich den angebunden haben. Zwischen Stiftung, die auch Netzwerk verwaltet und so weiter. Und die analysieren auch Netzwerkverkehr. Drum informieren wir die auch. Also für uns ist Switch und NCSC sind eigentlich die zwei Institutionen, die Bescheid wissen müssen. #00:57:38-4#

Experte 6: Ja, ich weiß gar nicht, wie das ist bei, du hast jetzt so Hosts gesagt, also zum Beispiel M365, ob man dort was informieren müsste. Ich glaube nicht. Zum Beispiel bei Microsoft weiß ich zum Beispiel, wenn du Vulnerability Scanning oder so machst, dort informiert man sie im Normalfall, damit sie wissen, dass was passiert. Aber bei Phishing, das ist normalerweise so low Volume. Ich glaube jetzt nicht. #00:58:05-4#

Experte 5: Und wenn, dann schlägt es in unserer eigenen Umgebung wieder auf. #00:58:09-8#

Experte 6: Richtig. Und eben es gibt keinen echten Impact auf andere Microsoft Entities. Da sehe ich jetzt weniger ein Problem. #00:58:20-9#

Severin Zimmermann: Okay, sehr gut. Vielleicht hier auch aufbauend, weshalb sollten diese Parteien informiert werden? #00:58:28-4#

Experte 5: Ja, eben sie überwachen unseren Netzwerkverkehr. die sehen da sofort wenn was ist. #00:58:37-4#

Severin Zimmermann: Also Sie schlussendlich nicht, ich sage jetzt mal, Blocking betreiben und das Phishing unterbinden oder auf euch zukommen und nicht glücklich darüber sind oder dass es echtes Phishing gibt. #00:58:51-3#

Experte 5: Sagen wir es mal so, sie überwachen uns jetzt nicht im Detail, aber sie haben so einen Grundrauschen und wenn das ausschlägt, dann wollen die wissen warum, ja. #00:59:01-3#

Experte 6: Ja, das generiert halt auch unnötigen Aufwand. #00:59:06-3#

Experte 5: Ja auf allen seiten. #00:59:08-6#

Experte 6: Willst du verhindern. #00:59:10-6#

Severin Zimmermann: Sehr gut, dann danke. Dann auch nochmals bezüglich Meldung. Sind euch Meldepflichten bekannt, die man durchführen muss, wenn ich jetzt Opfer eines Phishing wurde? Also eines echten Phishing und nicht eines Trainings. #00:59:28-3#

Experte 5: Also als reines Phishing Opfer nein, außer es sind vertrauenswürdig und besonders zu schützende Daten betroffen. Das gibt Meldung an kantonale Datenschutze, weil dann sind Daten abgeflossen und dann wird nachgegangen. Wieso und warum? #00:59:56-3#

Experte 6: Genau, da reden wir schon von Impact. Also erst wenn wir Impact haben, dann gibt es gewisse Meldepflichten, die mir aber auch nicht wirklich bekannt sind. Ich habe zwar schon in so vielen Incident-Responses mitgearbeitet, aber ich habe mich nie um die legalrechtliche. Dafür hast du meistens andere Instanzen. #01:00:17-2#

Experte 5: Also es kamen so auf die Art und Weise bei uns Daten auch noch nicht weg, wo Meldepflichtig waren. #01:00:22-3#

Experte 6: Das weiß ich jetzt gar nicht. #01:00:25-7#

Severin Zimmermann: Das ist ja schon mal gut. Jetzt noch eine ergänzende Frage, die ist nicht in meinem Leitfaden, da diese erst in einem späteren Interview aufgetaucht ist. Experte 5, du hast es auch bereits angesprochen, und zwar Meldungen, die Users machen gegen Externe. Du hast das, glaube ich, auch im Zusammenhang mit den Brands, dass die Mitarbeiter dann diese Brands anschreiben und nachfahren und die dann natürlich nicht glücklich darüber sind. Seht ihr da, ich denke jetzt mal weniger Chancen, aber Risiken. #01:01:03-5#

Experte 5: Ja, was heißt Chancen, Risiken? Also es ist einfach so, wir haben aus dem Fehler gelernt, wir werden das nicht mehr tun. Und wir versuchen dann einfach mit Vorlagen zu arbeiten, dass wir gar nicht mal in diese Lagen reinkommen, dass wir irgendwie mit Externe in Konflikt kommen. #01:01:23-5#

Experte 6: Ja, also ich persönlich sehe es halt als, wenn ich so eine Firma wäre, also wenn ich jetzt eine Amazon oder (unv., #01:01:32-7#) DHL, UPS, das sind ja so die typischen Bananenangriffe, ich würde nicht rechtlich gegen sowas vorgehen. Weil das Problem ist, im Endeffekt, wenn wir es machen, ist es illegal, wenn es die anderen machen, interessiert es niemand, weil dort gibt es niemanden zu belangen. Und das finde ich persönlich einfach eine sehr schlechte Einstellung. Also ich würde Phishing Mails immer noch eiskalt mit allem machen, was ich kann, unter alles machen, was Sinn macht. Also zum Beispiel, wir verwenden, keine Ahnung, SAP, dann würde ich ganz klar irgendwann mal hingehen und sagen, "Jo", wir machen jetzt mal einen Test mit dem SAP-Logo drin. Aber "Jo", SAP könnte dann hingehen, oh, das ist ja Markenrecht, bla bla bla. Ich finde das einfach von solchen Firmen echt schwach überdacht, weil wir machen nur ein Training, ein echter Angriff macht damit Impact und dort können sie auch nichts tun. Aber naja. #01:02:33-9#

Experte 5: Jetzt kommen wir wieder einen Punkt zurück, zu der externe Firma. Wenn man mit externer Anbieter hat und die solche Payloads im Angebot haben, dann sind die schließlich nachher auch dafür haltbar und damit sind wir raus. Und wenn die das uns anbieten, dann können wir das natürlich auch wieder nutzen. Aber wir von uns aus selber verlassen uns eigentlich nur noch auf abgesicherte Tools. #01:02:59-5#

Severin Zimmermann: Sehr gut. Vielleicht hier jetzt auch ergänzen und zwar, wenn man jetzt beispielsweise nicht solche, ich sage jetzt mal, illegalen Vorlagen verwendet, sondern wirklich Vorlagen, die legitim sind. Seht ihr da trotzdem das Risiko, dass das extern gemeldet wird, beispielsweise strafrechtliche Behörden oder eher nicht? #01:03:27-7#

Experte 5: Auch wenn es legal ist, kann man das so gestalten, dass der User den Eindruck hat, dass käme von jemand anderem. Ich sage mal ganz vorsichtig, dann kann es schon mal passieren, dass der eine Meldung macht. Aber dass das Konsequenzen rechtlich in Ordnung hat, kann ich mir nicht verstanden. #01:03:45-9#

Experte 6: Ich hoffe es nicht. #01:03:48-6#

Experte 5: Es wäre schon ein langweiler Betrieb, wenn er nichts anderes zu tun hat. #01:03:52-9#

Experte 6: Genauso, genauso. #01:03:56-8#

Severin Zimmermann: Gut, dann danke ich euch. Jetzt hatte ich schon noch meine zwei abschließende Fragen beziehungsweise eine. Und zwar sind eurer Meinung nach jetzt noch Punkte oder Aspekte offen, die wir nicht besprochen haben, aber im Zusammenhang vom Phishing Awareness Training, also eurer Sicht wichtig ist. #01:04:17-5#

Experte 5: Also wenn ich so kurz revidiere, haben wir einen recht guten Streifzug gemacht und müsste eigentlich, meiner Meinung nach, müsste alles enthalten sein, was wichtig ist. #01:04:30-4#

Experte 6: Für mich stellt sich eher so eine umgekehrte Frage. Ich finde es immer interessanter, du hast ja schon erwähnt, Experte 5, bei Phishing redet man immer irgendwie so irgendwie komische Überbegriff und irgendwie liegt viel drin, aber irgendwie auch nicht, also mindestens zu meiner Meinung nach, oder? Also wenn wir über Phishing Simulationen reden, dann reden wir eigentlich implizit immer über E-Mails. Und ich habe eher dort vielleicht noch, damit habe ich zum Beispiel ein Problem. Ich sage, ja, vielleicht, ich weiß, ich habe schon davon gehört, dass zum Beispiel Teams verwendet werden zum Angriffestagen. Also für mich ist die Frage Phishing oder generelles Social Engineering? Weil ich finde eigentlich müsste ja, wenn man schon über das ganze Thema redet, dann müssten wir eigentlich über Social Engineering reden und nicht nur, ja, in Anführungzeichen über Phishing, weil bei Phishing redet man theoretisch über E-Mails, aber eigentlich müsste man ja damit auch alles andere meinen oder auch Phishing über SMS, über WhatsApp, über egal was, aber das sind für mich, dann irgendwie Begrifflichkeiten, ich sage es mal so. Aber sonst würde ich jetzt auch behaupten, #01:05:42-1#

Experte 5: Das sind jetzt wieder die Feinheiten. Drum gibt es Phishing mit ganz vielen Buchstaben vorne dran, wo für andere Einfallsfaktoren stehen. Genau. Aber ich denke im Allgemeinen über Phishing Kampagne wird zu 95 Prozent meinen wir darin E-Mails. #01:05:55-0#

Experte 6: Genau, richtig. Das ist auch für mich ein bisschen ein Missstand. Ich glaube zurzeit, ja, ist so, dass vieles läuft über E-Mails. Ich glaube aber auch, es wird ein Punkt kommen, an dem die Verteidiger genug gut sind zum E-Mails rausfiltrieren und dann macht es relativ schnell, wird es kippen und Angreifer werden andere Mechanismen verwenden. Man hat es zum Beispiel gesehen mit Word-Dokumente, die sind ja jetzt relativ gut gesichert worden, indem man einfach sagt, "Jo", Makros gibt es so nicht mehr wirklich. Und es ging gefühlt einen Tag und seitdem werden wir mit OneNote angegriffen. Und Das sind so Dinge, bei denen ich mich schon zum Teil frage. Aber im Endeffekt, "Jo", man versucht natürlich,

den Hauptvektor abzufangen oder zu trainieren. Aber für mich ist eigentlich wichtig, dass ein Verständnis existiert, dass ja auch Teams ist nicht vertrauenswürdig zum Beispiel. #01:06:55-3#

Experte 5: Aber das Verständnis, das sind wir am Schärfen und das Phishing ist nur ein Teil davon und das Verständnis stärken, das heißt auch die Präsenz, das habe ich schon erwähnt, dass das Thema immer aktuell gehalten wird, dass die Leute immer sensibilisiert sind und wissen, ich muss generell ein bisschen aufpassen, kann man auch machen durch andere Aktionen. #01:07:14-6#

Experte 6: Das ist eigentlich Grundsatzverständnis. Es geht nicht nur um Phishing, sondern auch Grundsatzverständnis. Vielleicht kann man da jetzt wieder von Kultur reden. Dass die Leute wissen, alles ist schlecht. Ja, sonst habe ich eigentlich auch nicht allzu viel zu sagen. #01:07:28-6#

Severin Zimmermann: Sehr gut, vielen Dank, dann werde ich die Aufzeichnung beenden.

I Transkript Experten-Interview Experte 7

Administratives	
Interview Datum	05.04.2023
Interview-Partner	Experte 7
Arbeitgeber	Datimo
Aufnahme OK?	Ja
Anonymisierung Daten?	Nein

Severin Zimmermann: So die Aufzeichnung sollte auch gestartet sein. Dann würden wir loslegen, dürfte ich dich kurz bitten mit der Position und der Funktion, die du hast vorzustellen. #00:00:24-0#

Experte 7: Selbstverständlich. Mein Name ist Experte 7 ich arbeite seit 22 Jahren bei der Optimo Service AG. Heute tätig hauptsächlich in den Bereichen Projekten und Consulting, Kundenbetreuung und übergeordnete strategische Themen innerhalb der Datimo. #00:00:50-6#

Severin Zimmermann: Sehr schön hattest du auch bereits Erfahrungen mit Phishing selbst wurdest du eventuell bereits einmal Opfer oder ähnliches? #00:00:59-6#

Experte 7: Opfer nicht, dass ich wüßte, aber ja, ich habe gewisse Erfahrungen mit mit User Awareness, da ich beteiligt war. An der Einführung dieser Services, bei der Datimo für unsere Kunden und für uns selbst natürlich. #00:01:19-2#

Severin Zimmermann: Sehr gut, du hast jetzt schon der nächsten Frage vor vorgegriffen also hast du auch bereits User Awarbess Training implementiert und aufbereitet, so wie ich das verstanden habe? Für Daten wie auch für Kunden. #00:01:33-8#

Experte 7: Genau. #00:01:37-4#

Severin Zimmermann: (unv., #00:01:37-4#) Kommen wir zum Hauptteil? Kannst

du vielleicht mal erläutern, ob dir allgemein positive Aspekte im Rahmen von Phishing Awareness Trainings bekannt sind? #00:01:55-4#

Experte 7: Ja, also ich denke positive Aspekte sind hauptsächlich die, die Schulung, die Sensibilisierung der Mitarbeiter im Umgang sei das mit Mail oder auch im Web mit. Ich erkenne links. Ich werde geschult, wie ich mit der externen Datenträger usw umgehen kann oder soll von daher.Sind sicher die positiven Aspekte sind die Schulung, die Instruktionen, die permanente Weiterbildung der Mitarbeitenden auch in Anbetracht, dass die Technologien. Wie Phishing daher kommt immer wieder neue Methoden, neue Ansätze findet und diese auf die User entsprechend (unv., #00:02:47-1#) beziehungsweise eben geschult werden können. #00:02:50-0#

Severin Zimmermann: Sehr gut. Danke und das Gegenteil sind Ihnen aber auch negativ Aspekte bekannt, welche im Rahmen eines Phishing Awareness Trainings eventuell entstehen können oder beachtet werden sollten. #00:03:06-1#

Experte 7: Ja, also mir kommen auf der technischen Seite gibt es sicher negative Aspekte, da ist relativ aufwendig ist die ganzen Systeme entsprechend zu konfigurieren, damit die Phishing Trainings auch dann beim and User ankommen und nicht durch vorgelagerte Systeme blockiert oder gefiltert werden. Dass sie ist immer wieder mal je nach Lösungen, die auf der Mail Seite implementiert ist ein größerer oder kleinerer Challenge. Aus Sicht User ist sind schon negativ Aspekte bekannt geworden. Das sind meistens Aussagen wie ist überflüssig, braucht nur viel Zeit. Meine Leute müssen arbeiten, die haben keine Zeit da halbe Stunde Stunde Schulung zu machen, das ist aber mehr. Dann sag mal eigentlich ein organisatorisches Problem und nicht das Problem der Phishing oder des Trainings selbst. #00:04:09-6#

Severin Zimmermann: Genau also du hast jetzt technische Aspekte angesprochen, wie auch leicht organisatorische wie im der Zeitbedarf. Sind von deiner Seite auch vom Umfeld her, also eventuell mit externen Firmen Aspekte bekannt, die man im Rahmen von Phishing Awareness beachten sollte. #00:04:33-4#

Experte 7: Ja, ist noch schwieriger so jetzt direkt kommt mir nichts in den Sinne, warst eventuell heikel sein könnte aber praktisch bei jedem Tool, wo ich solche Trainings machen kann implementiert ist sind diese diese Training Phishing Mails, die kommen natürlich im optisch daher von diversen Firmen bekannten, weltweit operierenden Firmen. Ob das ich sag jetzt mal rechtlich ganz sauber ist, weiß ich schlussendlich nicht. #00:05:14-2#

Severin Zimmermann: Ok, vielen Dank. #00:05:17-4#

Experte 7: Also Thema Logomissbrauch, Namensmissbrauch geht in diese Richtung. #00:05:21-1#

Severin Zimmermann: Ja also so Markenschutz etc. #00:05:24-9#

Experte 7: Genau. #00:05:24-9#

Severin Zimmermann: Sehr schön. Dann würden wir nun zu den Detailfragen kommen. Ich werde hier vor allem anfangen mit organisatorischen, wo ich ein paar Inputs geben werde für gewisse Themen, wo sie dann ihre Meinung oder ihr Wissen dazu äußern können. Anschließend folgen noch etwas technische und auch Umfeldtechnische Detailfragen. Ja, ich denke, wir legen direkt los. Und zwar ist Phishing immer oder wird Phishing sehr oft auf entsprechende Mitarbeiter abgestummen, da diese aus unterschiedlichen Faktoren, demographischen oder auch Verhaltensweisen unterschiedlich reagieren. Sollte Ihrer Meinung nach eine Abstimmung auf Personen oder beziehungsweise das Phishing Selbst Ttraining, personalisiert auf die Personen stattfinden. #00:06:38-2#

Experte 7: Ja so wenn ich jetzt die Frage richtig verstanden habe, geht es darum, ob die Phishings oder das Training nochmals nicht nach "Gießkannenprinzip" erfolgen soll, sondern nach Abteilungen oder Funktionen, Bedrohungsgrad und so weiter. Wenn das die Frage war dann ja, es gibt natürlich unterschiedliche Personenkreise, die unterschiedliche betroffen sind sei das Know How technisch vor dem Computer selbst, aber auch in ihrer Funktion also ich denke da an. Bereiche wie Personalabteilung, Finanzwesen, Geschäftsleitung. Bereiche, wo Personen Datenschutz ich sag mal Gesundheitswesen usw sicher gefährlich als nicht gefährlicher wo wo prädestiniert sind ,um gezielt angegriffen zu werden. Vergleichbar oder das Gegenteil dazu ist ich sage jetzt mal der Mitarbeiter draußen in der Produktion, der sein eher ERP System hat und die Aufträge ausliest und die Daten eingibt wenig mit sensiblen Daten zu tun hat und so weiter. Ich denke, da sollte sicher eine entsprechende Kategorisierung stattfinden, auch was Menge tief bei usw angeht vom Training selbst. #00:08:13-0#

Severin Zimmermann: Vorab also Sie haben ja da frage genau richtig verstanden. Vielleicht noch ergänzend sehen Sie Chancen oder auch Risiken, die entstehen können, wenn ich ein Phishing Awareness Training personalisiere? #00:08:32-4#

Experte 7: Ja, Chancen, das kommt auf den Betrachtungswinkel, für ich sag jetzt mal das Unternehmen kann es eine Chance sein, weil sie bei personalisierten Trainings sieht, welche Mitarbeiter explizit oder welche Mitarbeitergruppen ich sag jetzt mal sich schwerer tun mit der ganzen Materie gegenüber anderen. Das kann aus Sicht des Mitarbeiters aber ein Risiko sein, dass er ich sag jetzt mal, dass er an den "Pranger" gestellt wird, weil wenn seine Trainingsresultate nicht so gut sind wie eigentlich gewünscht also es kommt immer ein bisschen auf den Betrachter an. Von daher gibt es sicher beides. Chancen sind sicher auch aus Unternehmensicht eben das das Training die Mitarbeiter weiterbilden, sie sensibilisieren auf das Thema auch ich sag jetzt mal mit mit Insiderwissen. Einmal versuchen ein ein Phish Training durchzuführen, wo erfahrungsgemäß die Klickquote relativ hoch ist, diese wieder runter zu bekommen beziehungsweise auf ein erträgliches Niveau zu bringen. Die Chancen für den Mitarbeiter sind natürlich er lernt etwas dazu, also er kann sich weiterbilden, hat sich fortbilden, er kann das ganze. Selbstverständlich nützt ihm auch, wenn er das privat anwenden kann. Also jeder hat heute denke ich, eine Mailbox zuhause und bekommt auch zu Hause solche Mails dir lieber nicht gern hätte. #00:10:19-0#

Severin Zimmermann: Sehr gut, besten dank dann vielleicht auch das Gegenteil. Welche Chancen oder Risiken sehen Sie, wenn ich ein Phishing werden, das Training eben nicht personalisiere? #00:10:34-3#

Experte 7: Bei nicht personalisierten. Wird die /. Ist aus meiner Perspektive mehr Sonne, schwarz weiß Ansicht. Ich sehe ich sag jetzt mal, ich habe 100 Personen angeschrieben 50% , klickt auf den Links ich weiß ok 50% sind reingefallen, aber ich sehe nicht woher das die kommen, auf was sind sie reingefallen und so weiter? Also die Auswertung, die die Erkenntnisse sind aus meiner Sicht eben eher schwarz weiß zu betrachten, was sich weniger als Chance anschaue sondern mehr als Risiko. Ich weiß, ich hab ein Risiko, aber ich weiß nicht wo ich es habe. #00:11:22-4#

Severin Zimmermann: Ja, ich sehe die Frage war wahrscheinlich nicht ganz genau gestellt. Mit personalisiert war hier eher gemeint, dass es auf den User abgeschnitten ist und nicht auf Anonymisierung beruht, sondern das ist ein Training wirklich auf eine bestimmte Person zuschneide wie du das vorhin erwähnt hast, beispielsweise explizit auf die Finanzabteilung beziehungsweise eben wenn ich es nicht auf die Finanzabteilung zuschneiden. Hast du gleich mit dem noch Ergänzungen oder möchtest du das so stehen lassen? #00:12:03-4#

Experte 7: Nee, also ich eben ok, dann /.Ja, dann muss ich mich entschuldigen für die falsch verstandene Frage. Ja macht natürlich Sinn, also Chancen eben, wenn ich das so Personalisiere im Sinne von Benutzergruppen eben wie wir anfangs bereits erwähnt es gibt Bereiche, die mit sensiblen Daten umgehen, mit mit Finanzdaten usw. Die haben aus meiner Perspektive müssen die noch mehr sensibilisiert werden oder extra sensibilisiert werden, sei das von Menge, aber auch

von der Qualität der Trainings. Vergleichbar mit ich sage jetzt wieder halt der Person in der Produktion draußen. Was inhaltlich angeht, kann man natürlich maßgeschneidert mit Stellenbewerbungen mit. Sie haben Ihre Rechnung noch nicht bezahlt. Sie haben eine Gutschrift erhalten. Mit solchen Geschichten kann man natürlich punktuell besser auf die auf die Mitarbeitenden zu umgehen, weil ich sag jetzt mal wenn der lageristen Maile bekommt. Sie haben Ihre Rechnung nicht bezahlt, dann interessiert ihn das vermutlich nicht, weil er nichts damit zu tun hat. Wenn das Mail aber jemand aus der Finanzabteilung eröffnet. Ist die Chance groß, dass dort geklickt wird oder geschaut wird? Was ist an den an diesem Mail oder in diesen Informationen dran. #00:13:30-1#

Severin Zimmermann: Ok, vielen Dank. Die nächste Frage knüpft gleich etwas an und zwar geht es hier um das Schulungsmaterial selber beziehungsweise wie das Schulungsmaterial vermittelt wird. Es gibt bekanntlich mehrere Methoden. Im solche Phishing Awareness Trainings aufzubauen, beispielsweise wären hier im embedded Schulungen, wo eben wie du es auch bereits angesprochen hast, wenn jemand auf auf ein Mail klickt, dass er dann zur Schulung aufgefordert wird. Es gibt präventive Schulungen, aber auch das Schulungsmaterial selbst. Wie kann das Video als Game als Factsheet übertragen werden. Schulungen können Klassenräumen oder online stattfinden oder mittels Informationsblätter. Hier gibt es sehr viele unterschiedliche Aspekte. Auch ein Aspekt ist, ob ich meine Mitarbeiter über eine entsprechende Schulung informieren soll oder nicht. Das hat alles mit dem Aufbau einer Schulung zu tun. Sehen Sie beim Aufbau einer Schulung, wie man diese gestaltet, Chancen vielleicht in gewissen Aspekten oder Risiken, die man weiter Gestaltung beachten sollte? #00:14:56-0#

Experte 7: Ja, ich denke also der Aufbau für diese Schulungen sollte so gewählt sein, dass der Mitarbeiter oder die Mitarbeiterin ich sag mal Spaß hat an der Schulung also das ist sich damit auseinandersetzen kann, damit sie auch etwas gefordert wird. Also ich denke da entweder eben ein interaktive Schulungen oder kurze Videosequenzen, gefolgt mit mit Fragen oder so Multiplechoice einfach, wo der wo der Mitarbeiter aktiv daran teilnehmen muss, eben weil es Spaß macht, ist die Chance größer, dass sie durchgeführt wird die Schulung, weil, wenn es keinen Spaß macht oder einfach ich sag jetzt mal Informationsblätter abgegeben werden. Ich hab keine Möglichkeit zu schauen hab dass sie gelesen hab, dass sie verstanden oder ist sie einfach im Mülleimer gelandet? Von daher denke ich was sicher sehr wichtig ist ist, dass man den Fortschritt beziehungsweise die Schulung selbst messen kann, ob sie durchgeführt wird und wie sie durchgeführt wird. Das wiederum gibt an Feedback, ob die Schulung oder die Schulungen passen und gemacht wurden oder ob das Ganze einfach im "Sand verläuft". #00:16:23-6#

Severin Zimmermann: Sehr gut, besten Dank ergänzend hierzu sind Sie der Meinung, dass das IT-Personal im Rahmen einer Phishing Awareness Training, über das Training informiert werden sollte. Und wenn ja vielleicht aus welchen Gründen oder aus welchen Gründen nicht? #00:16:46-3#

Experte 7: Nein, ich also /. Iich bin der Meinung, dass IT-Personal sollte nicht informiert werden, weil auch sie gehören aus meiner Sicht zu den eher Risiko behafteten Personalbeständen oder oder ja Abteilungen. Da IT doch in der Regel mit mehr Rechten ausgestattet ist als andere Mitarbeiter, Zugriff auf Systeme haben die Mitarbeiter gar nicht haben und so weiter von daher, denke ich gehört für mich IT-Personal eigentlich zu Hochrisikogruppe dazu. Und die Information ist von daher überflüssig. Sag ich mal da sonst der Überraschungseffekt fehlt und das ganze ich sage jetzt mal, etwas lockerer angegangen wird, als wenn sie es nicht wissen. #00:17:48-4#

Severin Zimmermann: Sehr gut, besten Dank. Dann kommen wir zum nächsten Fragen und zwar ist auch in der Literatur sehr breit diskutiert die Cybersicherheitskultur im Allgemeinen. Wie sehen Sie den Einfluss bezüglich Cybersicherheitskultur? Bei Phishing Awareness Training ist hier eine umfangreiche Cybersicherheitskultur innerhalb der Unternehmung notwendig oder sollte diese genau mit dem Phishing Awareness Training geschaffen werden oder wie sehen sie das? #00:18:26-2#

Experte 7: Ich müsste nachfragen, was sie genau in der Cybersicherheitskultur verstehen. Oder was Sie damit sagen wollen? #00:18:36-7#

Severin Zimmermann: Genau da darin sind enthalten beispielsweise allgemein wie die Kultur in einem Unternehmen gegenüber Cyberbedrohungen oder allgemein Bedrohungen. Verstanden wird, wie diese gepflegt wird, wie wie das kommuniziert wird, also beispielsweise in IT-Richtlinien, dass gweisse Punkte nie erfolgen dürfen, wie beispielsweise Zutritte oder eben bei Cybersicherheit bezüglich ob User Schulungen machen sollten etc. Und hier die generelle Kultur, wie das auch gepflegt wird, allenfalls auch die Kommunikation unter den Mitarbeitern, für die Unterstützung bei, um Cyber Risiken abzuwehren. Oder ich sag jetzt mal bei einer Cybersich /. Bei einer gut gepflegten Cybersicherheitskultur fragt man auch mal den Kollegen ich habe hier ein Mail erhalten, bin mir nicht sicher. Während bei einer schlechten Cybersicherheitskultur wird das vielleicht einfach selbstständig angeschaut. #00:19:49-3#

Experte 7: Okay. Also ich denke, das eine schließt das andere nicht aus, also eine eine Cybersicherheitskultur im Unternehmen finde ich äußerst wichtig und notwendig, sofern sie auch entsprechend gelebt wird. Ich sehe halt vielfach die Problematik darin da /. Das beginnt beide ich, ich sag jetzt mal IT-Richtlinien, die eigentlich jedes Unternehmen haben soll, haben noch lange nicht alle Unternehmen und dementsprechend wird auch die Cybersicherheitskultur zu wenig oder zu intensiv gelebt, also alle wissen aus den Medien wir haben Cyberkriminelle, es kann etwas passieren, aber meine Empfindung ist, dass die meisten Unternehmen, das Ich sag jetzt mal auf die "leichte Schulter" nehmen so nach dem

Motto Wir haben ja nichts was lohnt bei uns zu zu stehlen oder zu kompromittieren. Von daher wünsche ich mir, dass diese Kultur mehr gelebt wird intensiver gelebt wird. Eben, dass seine User Awareness Training nicht als Belastung oder als Schikane betrachtet wird, sondern wirklich als wertvolle Ergänzung wertvolle Schulung, um das sich selbst und das Unternehmen weiter zu bringen und vor möglichen Attacken zu schützen. Auch bei einem Befall sieht man immer wieder die Mitarbeiter scheuen sich, das zu melden. Sie haben Angst vor Konsequenzen. Sie möchten nicht als als als "Buhmann" dargestellt werden, was in der Regel nicht der Fall ist. Aber das Ganze natürlich verschlimmert, wenn, einfach der Befall, sag ich mal erst Tage später festgestellt wird, durch andere Mitarbeiter oder durch Überwachungssysteme. Ja, wäre sicher, oder in den meisten Fällen besser händelbar wenn etwas geschieht, wenn man das so früh wie möglich weiß. Unabhängig wer das getan hat. Fehler machen alle, Menschen machen Fehler, das gehört auch zu unserer Kultur, der die Frage ist einfach wie geht man damit um? Und ich denke, da hat es noch sehr, sehr viel Potential auch in den Unternehmen, spricht von dann müßte eigentlich aus Stufe Management, Geschäftsleitung müsste da. Klares Statement kommen immer wieder kommen. Meldet euch sag mir etwas nicht gut ist es hat keine Konsequenzen es es hilft dem Unternehmen, je schneller wir dort intervenieren können, desto besser. #00:22:55-5#

Severin Zimmermann: Bestens vielen Dank. Kommen wir nun zu einem etwas anderen Aspekt. Phishing Awareness Training steht oft unter dem Aspekt über ethische Korrektheit und ethische Durchführung. Sehen Sie ethische Aspekte, welchem Rahmen des Phishing Awareness Trainings beachtet werden sollten? #00:23:24-8#

Experte 7: Ja, also ich denke die üblichen ethischen Grundsätze, wobei Ethik auch auch ein sehr flexibler Begriff ist, sollten sicher eingehalten werden, also ich denke da wenn ich ein ethische Fragen denke, dann dann kommen ja sicher Sachen wie Religion mein /. Oder ich sag mal orientierung ich sage mal politische Orientierung Ethnie usw. solche Dinge sollten vermieden werden. Beziehungsweise einfach verallgemeinert werden, damit da keine Ethische Konflikte entstehen können. Andererseits ethische Konflikte können aber auch ich sage jetzt mal entstehen, wenn ich natürlich ne Phishing Training mache und ich nutze immer immer und immer wieder Microsoft als Beispiel. Könnte im weitesten Sinne natürlich auch ethisch ausgelegt werden, dass man Microsoft immer so als "Buhmann" darstellen möchte, was definitiv natürlich nicht so gemeint ist. #00:24:41-9#

Severin Zimmermann: Sehr gut. Kommen wir zu etwas, das Ihnen sicherlich auch bekannt ist, als sie ist auch bereits ein wenig angesprochen haben im Meeting und zwar geht es um die Klickraten. Wie stehen sie gegenüber Klickraten sei das hohe Klickraten oder eben tiefe Klickraten während eines Phishing Awareness Trainings. #00:25:12-2#

Experte 7: Ja, also, ich denke die Klickrate. Eben ist eigentlich ein messbarer Spiegel, wie das Verhalten der Mitarbeiter jetzt auf diese explizite Phishing Kampagne erfolgt ist sie ist nicht mehr sie ist nicht weniger. Also hohe Klickraten zeigen in der Regel entweder ist es ein sehr, sehr gut vorbereitetes Phishing Mail gewesen oder die Mitarbeitenden sind einfach zu wenig geschult zu wenig sensibilisiert darauf und klicken jedes Mail an, "komme was wolle". Von daher hat es seine Berechtigung, diese Klickraten aber eben für mich eigentlich mehr wirklich ein Messinstrument. Was zeigt jetzt auf diese explizite Phishing Kampagne wurden so und soviel Prozent geklickt oder auch nicht, unabhängig davon eben sie sagt nichts aus über die Mitarbeitenden oder den Inhalt des Phishings, was ausschlaggebend sein kann. Also wir haben einen Test Phishing intern, wir hatten eine interne Umfrage in unserem Unternehmen und die Leute wussten die Resultate kommen irgendwo im März sollten diese Bereitstellen, ausgewertet sein. Es wurde dann so Ende Februar, Anfang März wurde Phishing Training generiert, genau mit dem Ansatz, die Resultate dieser Umfrage sein online klickrate 73%. Also wenn das clever gemacht ist, dann ist eine hoch klickrate, auch wenn die Mitarbeiter sensibilisiert sind, es kann aber auch sein, dass einfach ich sag mal bei einer tiefen Klickrate die Leute gut reagiert haben, alles einfach weggelöscht haben oder Sie haben Sie übersehen Sie haben sie ignoriert, eben es gibt so viele Aspekte. Von daher würde ich die Klickrate selbst immer mit Vorsicht genießen, immer mit Rand Daten abgleichen. #00:27:35-7#

Severin Zimmermann: Ja gut, Sie sprechen hier eine Problematik an, auf die ich auch eingehen wollte, trotzdem wollte ich noch gerne ergänzen nachfragen, und zwar über hören Instanzen wird oft die Klickrate als Verkaufsargument oder als Argumentation für Schulungsmaßnahmen verwendet. Sehen Sie hier Problematiken vielleicht auch gleich in Bezug mit den Problematiken, die sie bereits erwähnt haben. #00:28:11-1#

Experte 7: Nein, das Problematiken sehe ich nicht. Dass diese Daten oder diese Zahlen als Verkaufsargument genutzt werden, ist auch nachvollziehbar, eben weil es ist halt messbar, mann, sieht etwas oder das Management sieht etwas aber problematisch seh ich das insofern nicht, sofern man die Daten, die rauskommen entsprechend in Kontext stellt und auch entsprechend interpretiert. #00:28:44-7#

Severin Zimmermann: Wie sieht es tschuldigung? #00:28:48-0#

Experte 7: Tschuldigung, die reine Klickrate an und für sich ohne Kontext sehe ich als problematisch an, eben weil sie kann in beide Richtungen ausschlagen. Sie sagt nichts über das Verhalten aus der Mitarbeiter. #00:29:03-7#

Severin Zimmermann: Sehr gut. Wie sehen Sie das vielleicht auch wenn die Klickraten zu tief sind und allenfalls auch eine Weiterführung eines Phishing Awareness Trainings daher durch höhere Instanzen gefährdet wird. Da sie der Meinung sind es klickt ja niemand, also Wesshalb brauche ich ein Training. Sind sie vielleicht diesbezüglich noch Probleme oder Chancen, die sich ergeben können? #00:29:34-9#

Experte 7: Ja, so Probleme insofern eben das, wenn tiefe Klickraten dazu führen, dass Training einzustellen, dann wird genau diese Entscheidung zum Problem, weil ich sag jetzt mal grundsätzlich tendenziell tiefer klickraten heißt, die Mitarbeiter sind trainiert, sind geschult auf auf solche Phishing Mails und damit das so bleibt, muss das zwingend auch regelmäßig immer durchgeführt werden.Kleines Beispiel es bringt nichts, wenn ich 2 Wochen wie ein Irrer trainiere und dann das Gefühl habe jetzt hab ich meine Muskulatur aufgebaut und dann mach ich wieder 3 Jahre nichts dann sieht diese Muskulatur wieder so aus wie vorher und das ist bei bei Awareness Training dasselbe Spiel eben. Die Methoden ändern es gibt tagesaktuelle Geschichten, auf die eingegangen wird. Klassiker jetzt in der Vergangenheit die ganze Corona Geschichte da wimmelt es von Corona Mails. Jetzt aktuell ich sag jetzt mal CS bankencrash oder beinahe Crash das sind natürlich diese tagesaktuelle Dinge sind prädestiniert für solche echten Attacken und sollten auch übernommen werden im Trainings auch wieder im Zusammenhang, dass die Mitarbeiter sensibilisiert werden und wissen OK in den Medien wird jetzt Thema XY aktuell behandelt ich muss damit rechnen, dass die nächster Zeit Phishing zu diesem Thema kommen könnten.Und daher ja.Ich würde Awareness Training als wichtiger permanent repetieren Bestandteil einer Ausbildung im Unternehmen bezeichnet. #00:31:33-4#

Severin Zimmermann: Sehr gut kommen wir zum jetzt eher technischen Teil und du hast zu Beginn bereits angesprochen technische Vorkehrungen sind teilweise recht aufwendig. Sehen sie /. Oder haben Sie vielleicht noch Ergänzungen, welche zum Beispiel Spamfilter, Absender, Whitelisting etc. also weitere Aspekte und Chancen Risiken, die diese Vorkehrungen im Rahmen von Phishing Awareness herbeirufen können? #00:32:13-1#

Experte 7: Ja klar, ich denke bedingt zwar einen gewissen Aufwand, den man betreiben muss, aber ja natürlich damit eben diese Trainings beim and Enduser ankommen sind Spamfilter manipuliert worden, wurden eben Whitelistings auf DNS oder auf IP basis erstellt. Und diese diese Freischaltungen können natürlich insofern missbraucht werden, wenn ich sag jetzt mal Domain Spoofing oder Mails Spoofing einfach wenn mit /. Oder wenn Außenstehende das merken, wissen unter Umständen, dass da solche Tools im Einsatz sind und wenn sie wissen was für Tools, dann können Sie sich auch etwa "zusammenschustern", welche Maßnahmen wurden umgangen und können diese dann die ihre eigentlichen bösartigen Phishings so manipulieren. Wenn Sie ein gezielter Angriff machen wollen das sind natürlich über ich sag mal eine gefaktes Mail Adresse oder Mail Domäne reinkommen oder sich als IP ausgeben, diese nicht sind und so weiter,

ja also da bestehen definitiv gewisse Risiken und gefahren sind aber ich sag jetzt mal überschaubar man kennt sie und wenn man das mit der nötigen Sorgfalt und nicht ich sag jetzt mal in die Tageszeitung schreibt, mit welchen Tools, dass wir arbeiten sind die Chancen relativ klein. Sie sind nicht bei 0 aber sie sind relativ klein. #00:33:59-5#

Severin Zimmermann: Sehr gut, dann werde ich hier /. Die ergänzende Frage hast du auch bereits beantwortet. Dann vielleicht technische Maßnahmen sind oft sehr hilfreich für das Abwehren von echten Phishing E-Mails. Es kann aber auch dazu führen, dass Mitarbeiter ein falsches Vertrauen in die Technik erhalten und daher anfälliger für Phishing Angriffe werden, da sie der Meinung sind, dass die Technik hatte echte Angriffe schon abgewehrt und das, was ich bekomme, sind alles legitime Mails. Wie stehen Sie demgegenüber und im Rahmen von Phishing Awareness, sollte das allenfalls mit beachtet und entsprechend geschult werden, dass das nicht zwingend der Fall ist. #00:34:57-9#

Experte 7: Ja, ich denke, das ist sicher ein Fakt, der gegeben ist also das soll man, muss man den Mitarbeitern auch nicht teilen und sie das kann man gut in die Schulung einbinden. Technische Maßnahmen sind wie überall dienen als Ergänzung als als Hilfsmittel sind aber in der Regel nicht das "Maß aller Dinge", zumal sie nicht 100% funktionieren eben das ist immer so ein "Hase Igel Spiel" meistens ist der Hase oder der Igel das Unternehmen und der Hase Ich sag jetzt mal der Angreifer, dass der Hase einen Schritt voraus ist. Von daher ja unbedingt technische Maßnahmen können versagen werden versagen und der gesunde Menschenverstand ist immer einzusetzen. Vergleichbar vielleicht mit den mit den neueren Automobilen, die mit selbstfahrenden Systemen usw auch dort heißt es immer wieder, dass das Fahrzeug kann vieles spurassistenten, kollisionswarner und und und aber der Mensch als letzte Instanz muss immer Herr der Lage sein. Das das verhaltet sich am Computer genauso also es hilft, aber ich bin schlussendlich immer noch das letzte Glied, der den Klick macht oder eben nicht. #00:36:29-1#

Severin Zimmermann: Sehr schöne Umschreibung. Kommen wir zur nächsten Frage und zwar. Reichen ihrer Meinung nach Schulungsmaßnahme für die Sensibilisierung aus oder sollten technische Warnhinweise, hier will ich nicht auf die vor vorhergegangenen technischen Systeme also sprich Spamfilter etc. eingehen, sondern ein Mail dass beispielsweise durchgekommen ist, allenfalls mit einem Banner ergänzen oder im Browser entsprechende Plugins implementieren. Die zusätzliche Warnungen schaffen würden User. Sind Ihrer Meinung nach solche technischen Warnhinweise nötig oder reichen die Schulungen grundsätzlich aus? #00:37:27-5#

Experte 7: Nein, ich denke jedes Mittel, jede Methode, um die Awareness zu fördern erachte ich als sinnvoll. Eben seinen dass Warnhinweise, unabhängig in Mail oder in Browser Programm wo dan auch immer. Auch die sind ein kleines

Puzzlestück im ganzen, aber sie werden gebraucht und weglassen würde ich sie nicht einfach auch so. Ich sag mal, je besser oder je mehr die Informationsflut in Anführungszeichen besteht oder die Leute darauf hingewiesen werden, desto eher gehen Sie ins Bewußtsein über wieder vergleichbar mit mit Werbung. Wir alle kennen so nervige Werbung, wo überall hängt, im Fernsehen, im Radio gebracht wird und und und. Sie nerven zwar, aber nach 2 Monaten kann ich fragen du weißt doch ja ja, das war dann der Werbung, also die Leute, je mehr man hört, desto eher bleibt es im Gedächtnis und daher denke ich, mach das Sinn. Je nach Unternehmen würde ich auch technische Maßnahmen. Ich sag mal von daher insofern verfeinern zum Beispiel, dass man sagt Mail Attachement werden, nur ganz bestimmte oder gar keine zugelassen, innerhalb von Mails oder links werden, nur bedingt zugelassen, was man da technisch machen kann, würde ich ausschöpfen grundsätzlich. Hängt aber immer wieder vom Unternehmen, also ich sag jetzt mal eine Revisionsstelle hat ganz sicher andere Maßnahmen oder andere Anforderungen wie ich sag jetzt mal die Schreinerei um die Ecke mit mit 3 Mitarbeitern. #00:39:33-2#

Severin Zimmermann: Sehr gut. Dann kommen wir zu einen etwas anderen Bereich, und zwar Plattformen. Heute ist es üblich, mit Mobiltelefonen, Smartwatches etc. Mails zu empfangen und zu prüfen. Meistens funktionieren diese aber technisch etwas anders wie der herkömmliche Desktop. Sind Ihrer Meinung nach unterschiedliche Plattformen in einem Phishing Awareness Training zu berücksichtigen und sehen sie vielleicht auch Chancen oder Risiken, die sich ergeben, wenn ich das berücksichtige, diese Plattformen oder eben nicht? #00:40:22-0#

Experte 7: Ja, also, ich würde es ihn in insoweit berücksichtigen, dass wenn das online Schulungen sind, dass die sicher auf auf heute gängigen Geräten eben wie Smartphones, Tablets oder Notebooks Arbeitsstation im Büro, dass die von überall aus gemacht werden können selbstverständlich. Risiken seh ich insofern nicht, was das Training selbst angeht, aber im Wissen, dass auch reguläre Phishings bösartige Phishings bis an den Endbenutzer kommen. Kann es sein, beispiel mein Notebook hat Endpoint Security Software drauf geht durch ein Proxy und und und hat diverse technische Maßnahmen die das Ganze sogar vielleicht blocken. Auf mein mobile Phone hab ich das nicht, wenn ich mir dort was einfange, dann weiß ich so n Umstände nicht mal, dass ich mir was eingefangen habe und kann je nach Konstellation ich bin morgen wieder im Büro, dass mein mobile Phone verbindet sich mit dem WLAN im Büro und ja, das weitere vorgehen kann man sich dann denken, also von daher hat es Risiken aber eben wir haben auch Chancen. Die Mitarbeiter können, das müssen das nicht am Arbeitsplatz machen. Sie können das auf dem Heimweg in im Zug oder Sie können das am Sonntagnachmittag im Garten auf ihrem Tablet noch ausführen, wenn sie Lust haben man gibt den Mitarbeiter so halt die Möglichkeit, das dann zu tun, wenn er es für richtig hält und ist nicht ortsgebunden ans Unternehmen. Das als Chance! #00:42:20-3#

Severin Zimmermann: Sehr gut, vielleicht auch hier nochmals ergänzend du bist

in etwas eine andere Richtung, wie ich das angedacht habe und zwar /. Oder bringen diese Plattformen unterschiedliche Möglichkeiten für den User mit zum solche Phishing zu erkennen. Beispielsweise das Hovern über einen Link funktioniert auf dem Desktop viel einfacher, wie beispielsweise auf dem Smartphone, wo es teilweise gar nicht möglich ist oder nur schon mit sich selber in Gefahr zu bringen. Und hier die Frage, ob entsprechende Schulungen auch auf solche Plattformen angepasst werden sollten, also spricht, dass man die Schulung auch am Desktop, Mobilephone oder die Schule /. Den Schulungsinhalt auf mobilephones oder beispielsweise Smartphones auslegt. #00:43:21-2#

Experte 7: Ja, also definitiv eben wir sind heute so verletzt und so mobil unterwegs, man weiß ja nicht wer hat welche Mittel. Die meisten haben alle Mittel, die du aufgezählt hast, also Mobileohones, Desktops und Tablets von daher ja denke ich schon, dass man solche Tools und solche Trainings auch auf die ich sage jetzt mal etwas neueren Endgeräten und nicht nur auf PC Notebook beschränken sollte, eben weil du hast es beschrieben, je nach Plattform mehr oder weniger Möglichkeiten zur Verfügung stehen und ich denke auch dass muss man dem Mitarbeiter zeigen, sagen, schulen. Weil eben in der vernetzten Welt spielt das gar keine Rolle, auf welchem Endgerät ich arbeite ich kann das Problem eigentlich über so viele Stellen ins Unternehmen schleusen, von daher macht das Macht das Sinn meines /. Ich muss nicht nur in Securitas vor das Haupttor stellen, sondern auch neben die 3 Nebeneingänge und Notausgänge, weil sonst ja. Bringts nicht allzu viel. #00:44:31-9#

Severin Zimmermann: Sehr gut vielen Dank für die Ergänzungen. Kommen wir zu letzten technischen Fragen und zwar: Implementieren viele Unternehmen eine interne Meldeplattform, sei dies über einen Button im Mai Client, wo ein Phishing gemeldet werden kann, oder über eine separate Homepage oder irgendwo in einem Ticketsystem integriert. Sehen Sie Chancen oder Risiken bei der Implementierung einer internen Meldeplattform? #00:45:06-7#

Experte 7: Ja, ich hab das ganze am Anfang kurz haben angesprochen oder angeschnitten das Thema. Chancen bestehen natürlich darin eben die IT-Abteilung wird, sofern dass zeitnah gemeldet wird informiert, dass sowas im Haus ist. Gegebenenfalls weitere Schritte einleiten kann. Risiken sehe ich natürlich für den oder aus Sicht des Mitarbeitenden eben wieder diese Prangerfunktion. Man weiß, ich hab jetzt da ich sag jetzt mal "Mist gebaut" und das wissen jetzt die von der IT und das weiß mein Chef nachher und hat ich sage jetzt mal "schürt" Ängste um um um Jobsicherheit usw oder einfach "schürt" Ängste vor Repressionen. Grundsätzlich finde ich das eine gute Lösung eben hat wieder etwas mit der mit der Cyberkultur zu tun, wenn eine offene Kultur gelebt wird, dann werden die Mitarbeiten das auch melden, egal über Button über Homepage wie auch immer damit dem nachgegangen werden kann und weiteren oder allfälligen Schaden vermieden werden kann. Wo das nicht gepflegt wird, sehe ich das Risiko, dass das die Mitarbeitenden nicht machen werden, wenn sie sowas haben und sie es drauf ankommen lassen, so nach dem Motto Vielleicht merktdie.it, ja gar nicht,

dass ich jetzt hier "Mist gebaut" habe. #00:46:36-6#

Severin Zimmermann: Sehr schön. #00:46:38-4#

Experte 7: Also es bestehen somit Chancen und Risiken für beide, also für Unternehmen wie für Mitarbeitende. Die meiner Meinung nach eigentlich nicht sein dürfte eben geht wieder Richtung Kulturleben. #00:46:52-4#

Severin Zimmermann: Sehr schön ausgeführt. Jetzt greifen wir nochmal das Thema Umfeld auf. Wir hatten auch am Anfang bereits einmal kurz das Thema bezüglich externen Umfeld. Vieleicht hier hast du ergänzen jetzt nochmals externe Einflüsse, die dir bekannt sind welche bei einem Fischinger werden Is Training beachtet werden sollen oder eben Einfluss haben können. #00:47:24-5#

Experte 7: Ja, ich denke die die Umsysteme, erster Linie Mail ist ja meistens einer der Hauptpunkte eben diese diese Mail Infrastrukturen aktuell ich sag jetzt mal. Beispiel Microsoft Exchange Online ist so ein Thema, wenn es mal implementiert ist. Ist in der Regel ok. Was aber sein kann, sag jetzt mal Microsoft hat letzten Wochen ihre Spamfilterpolicy massiv verschärft, die wiederum kann dann Einfluss haben, dass diese Trainings Mail gar nicht beim Enduser ankommen, also man muss da immer up to date bleiben, das ganze auch vielleicht zwischendurch mal aussicht IT abtesten, funktionieren die Mechanismen noch so, wie sie mal implementiert wurden oder hat der Anbieter irgendwas geändert? Was sicher auch noch sein kann, ist zu prüfen, ist mir im Detail so nicht bekannt sind rechtliche Aspekte eben Markenrecht oder ich sag mal sogar strafbare Handlungen, wenn man ich sag jetzt mal ja wenn man ein Phishing macht, wo man jemand verunglimpft, oder sag mal üble Nachrede so einfach rechtliche Geschichte sag ich mal dir sicher geprüft werden müssen und immer wieder mal beachtet werden müssen. Jetzt mit Zusammenhang mit der Datenschutzrevision, die im Herbst kommt, kann auch sein, dass da noch gewisse Einflüsse neu dazu kommen, die bisher so nicht bestanden haben? #00:49:09-0#

Severin Zimmermann: Sehr gut vielen Dank für die Ergänzungen. Kommen wir zu externen Partnern. Du hast bereits Microsoft angesprochen. Jetzt möchte ich aber mehr auf Partner eingeben, die allenfalls das Phishing Awareness Training für eine Firma durchführen. Wie stehen sie gegenüber solchen externen Partnern? #00:49:35-1#

Experte 7: Grundsätzlich positiv. Also ich würde mich sicher vorab informieren ist ein etablierter Partner oder ist das irgendwie ich sag mal Fake Unternehmung bei den etablierten großen Anbietern, denke ich ist das ok die haben ihr /. Oder die

sind entsprechend ausgerüstet. Man muss schlussendlich ein gewisses Vertrauen haben, in diese Unternehmen, eben weil man ihre Systeme eigentlich ausschließt aus den ganzen überprüfungs Geschichten. Und die Gefahr besteht natürlich immer, dass ich wir diesen Partner, wenn der nicht entsprechend geschützt ist oder kompromittiert worden ist, auch mein Unternehmen kompromittiert werden kann. Das ist so eigentlich so die /. Ich sag mal, die aus meiner Sicht die die größte Gefahrenquelle, aber sie ist relativ /. Meiner Meinung nach relativ klein zu beurteilen. #00:50:38-7#

Severin Zimmermann: Sehr gut, dann habe ich hier noch eine Ergänzung. Sehen Sie Chancen und Risiken gegenüber beispielsweise externen und beziehungsweise ausländischen externen Partnern? #00:50:55-6#

Experte 7: Ich denke, bei ausländischen Partnern wird gegebenenfalls die Rechtslage anders sein. Ich meine der Anbieter muss sich grundsätzlich nur wenn Recht seines Landes rechtfertigen. Ähm, kann sein, dass ich sag jetzt mal, wenn das Ding sagt in Russland steht, wo vermutlich nicht ganz so strenge Maßnahmen oder ganz so strenge Richtlinien bestehen und wir das in der Schweiz nutzen. Könnte ich mir vorstellen das, dass eben wieder betreffend Markenrecht usw. gewisses Potential an Risiko im Sinne von Klagen oder so bestehen, aber ansonsten. Eben wenn es vertrauenswürdige Partner sind etablierte Partner sehe ich das Risiko relativ klein auch aus dem Ausland. #00:51:56-4#

Severin Zimmermann: Bestens die nächste Frage bezieht sich auf das Thema rechtliche Aspekte. Dieses hatten wir jetzt aber bereits mehrfach angesprochen darum frag ich hier nur haben Sie Ergänzungen oder wollen wir das so stehen lassen? #00:52:16-2#

Experte 7: Ja Ergänzend. Ich sag mal aus der Praxis sage ich interessiert das die wenigsten die rechtlichen Aspekte müssen aber nichtsdestotrotz beachtet werden, gegebenenfalls helfen da Nachfragen beim Datenschutzbeauftragten und oder bei einer Rechtsabteilung, Rechtsanwalt die auf solche Gebiete spezialisiert sind, kann weiterhelfen. Oder kann"Licht ins Dunkle" bringen? #00:52:46-1#

Severin Zimmermann: Sehr gut. Dann sind Ihnen externe Parteien seien das Regierungsinstitutionen, Hoster, Registrat Etc. bekannt, welche zwingend über ein Phishing Awareness Training informiert werden müssen? #00:53:06-5#

Experte 7: Nein, eigentlich so mir nicht bekannt nein. #00:53:13-5#

Severin Zimmermann: Ok. #00:53:15-3#

Experte 7: Also wenn ich, das als Schulung oder als Training einsetzen will nicht nein. Wenn ich jetzt das als als Hersteller anbiete äh, dort kann ich mir vorstellen sind Bereiche wie ISP, also Internet Dienstleister usw. wo man eventuell Rücksprache nehmen muss, einfach weil auch dort Traffic und Aktivitäten gemessen werden nicht das denn /. Ich sagen jetzt mal meinen Dienst nach dem ersten Tag blockiert wird, weil die Swisscom das Gefühl hat wir versenden hier Tausende von von von Phishing Mails. Aber so als als Endnutzer, denke ich, muss ich niemanden informieren. #00:53:59-0#

Severin Zimmermann: Sehr gut. dann vielleicht noch bei Phishing selber sind Ihnen da beispielsweise mann wird von einem Phishing befallen oder wurde angegriffen. Sind Ihnen da Meldepflichten bekannt? #00:54:16-1#

Experte 7: Pflichten noch nicht, sag ich mal. Das wird mit der neuen Datenschutzrichtlinie kommen. Es empfiehlt sich aber, wenn man Opfer einer einer Phishing Kampagne wurde, wie auch immer diese aussieht, empfiehlt sich das entsprechend zu melden. Sei das falls vorhanden Cyberversicherung sicher zeitnah aktivieren. Dann, früher hieß es Melanie heute heißt das NC National Cyber Security irgendwas vom Bund #00:54:59-1#

Severin Zimmermann: NCS #00:55:00-3#

Experte 7: NCS okay, diese empfiehlt sich sicher zu informieren, die können auch /. Weil die können in der Regel auch gut weiterhelfen. Sie selber machen nicht allzu viel, aber sie haben Partner "im Boot", die einen unterstützen können sei das Kommunikation technischer Natur und so weiter hilft es sicher, wenn diese Stelle informiert werden. Gegebenen Falles, wenn man schon ab /. Oder wenn schon absehbar ist, dass man durch einen Befall weitere Firmen seien, dass Partner, Kunden oder Lieferanten , ich sag jetzt mal kompromittiert hat, indem das die Mails von uns bekommen haben, empfiehlt sich sicher auch diese entsprechend zu informieren, über das, was vorgefallen ist und das Mails zum Beispiel an sie versendet wurden, dass sie ihre Systeme prüfen, aber anschauen könntet. #00:55:59-6#

Severin Zimmermann: Sehr schön. Dann sind wir jetzt kurz vor Ende des Interviews. Ich habe alle meine Fragen grundsätzlich gestellt, bestehen von ihrer Seite

vielleicht Ergänzungen oder Punkte, welche wir nicht ausreichend behandelt besprochen haben diese noch gerne ergänzen wollen? #00:56:22-6#

Experte 7: Ja, ich denke so ein Punkt ja, die Frage ist wo passt der rein. So meine Erfahrung was das Training angeht, in in dieser Konstellation, wie wir das jetzt besprochen haben tun sich viele Firmen schwer und sehen keinen direkten Kosten nutzen daraus. Was vielfach dazu führt, dass solche Trainings nicht durchgeführt werden. Eben weil es keinen direkten Benefit daraus resultiert oder nicht Messbar ist mindestens. Verhalten sich ein wenig wie Marketing, da weiß ich auch nicht immer genau, für was ich Geld ausgeben. Aber, da /. Oder zu diesem Aspekt fehlt mir irgendwie noch so das überzeugende Argument bei Kunden wieso, dass sie das Geld dennoch ausgeben sollen, weil je nach Unternehmensgröße kann das pro Mitarbeiter und Jahr kann das ein paar 100 Franken kosten, je nach Größe des Unternehmens sind wir dann schnell im 5 oder 6 stelligen Bereich. Aber eben das ist so die menschliche Komponente, sag ich mal und die ist noch schwierig, das dem gegenüber zu vermitteln, sofern er nicht schon sensibilisiert ist oder er auf auf den Anbieter zu gekommen ist, oder? #00:58:01-8#

Severin Zimmermann: Gut dann. Kommen wir zum letzten Punkt, und zwar werde ich noch weitere Interviews durchführen und wollte noch kurz nachfragen, ob es für Sie in Ordnung ist, dass falls da noch neue Aspekte aufkommen, die ich gerne auch ihre Meinung noch dazu hören würde, wenn ich Sie hierzu nochmals kontaktieren würde? #00:58:27-4#

Experte 7: Selbstverständlich ja. #00:58:29-8#

Severin Zimmermann: Sehr gut, dann würde ich die Aufzeichnungen nun beenden.

J Transkript Experten-Interview Experte 8

Administratives	
Interview Datum	13.04.2023
Interview-Partner	Experte 8
Arbeitgeber	UMB
Aufnahme OK?	Ja
Anonymisierung Daten?	Nein

Severin Zimmermann: Die Aufzeichnung läuft, dann als erstes dürfte ich dich bitten, dich kurz vorzustellen beziehungsweise deine Position und Funktion zu nennen? #00:00:16-2#

Experte 8: Genau mein Name ist Experte 8, ich arbeite bei der UMB seit jetzt gerade ganz neu als Teamleader Strategic Sales Consulting und darin enthalten sind die strategischen Themen und zwar die fünf Themen Cybersecurity, Modern Work, Public Cloud, SAP und das klassische Netzwerk. #00:00:42-9#

Severin Zimmermann: Sehr gut, vielleicht noch ergänzend, wie lange arbeitest du jetzt schon generell bei der UMB und jetzt die Funktion hast du gerade genannt, hast du jetzt eine neue bald, aber vorhin hast du auch als Produktmanager im Security Bereich gearbeitet so viel ich das weiss? #00:01:06-5#

Experte 8: Ja, genau, der Job nennt sich dann bei der UMB /. Ich war in diesem Team schon seit ziemlich genau zwei Jahren, also seit dem 1. März 2021 und da war ich in diesem Team, das ich nun übernommen habe, nennt sich bei der UMB dann Strategic Sales Consulting, ist aber typischerweise was du sagst, wir begleiten unsere Sales zu den strategischen Themen, das ist der Vertriebsteil und dann gibt es gleichzeitig eben auch den Serviceentwicklungs und Produktmanagement-Teil, also diese zwei Flanken werden jeweils abgedeckt in unserem Team, das Verkaufen, das Vertriebsnähe und auf der anderen Seite eben das strukturierte Product Management, Product Marketing Thema, genau. Und immer, das ist die Ergänzung, immer als ich Teammitglied war, ist, und das wird auch so bleiben, mein "Steckenpferd" oder meine Herkunft seit über 15, bald 18 Jahren ist immer Cybersecurity, also von diesen fünf Themen ist vor allem das Thema Cybersecurity das, was mich persönlich am meisten /. Da komme ich her, ist meine Leidenschaft. #00:02:19-2#

Severin Zimmermann: Sehr gut, also Cybersecurity, also dann springen wir gleich mit dem Thema zur nächsten Frag dann gehe ich mal davon aus, dass du auch bereits Erfahrungen mit Phishing hattest. Wurdest du vielleicht bereits einmal Opfer oder einer deiner Kollegen oder sonst Erfahrungen mit Phishing-Angriffen? #00:02:39-5#

Experte 8: Ja, natürlich ganz viele, ich glaube da haben wir alle schon die Erfahrungen gemacht, übrigens auch schon mit Programmen die ich /. Ich habe zehn Jahre davon bei der Swisscom gearbeitet, von diesen 18 Jahren Security und da gab es auch immer diese Phishing-Programme, da bin auch ich als in Anführungszeichen Experte logischerweise schon reingefallen, dass ich ein offiziell gesendetes Phishing-Kampagnen Mail, dass ich da reingefallen bin und geklickt habe. #00:03:11-9#

Severin Zimmermann: Okay, vielen Dank. Hast du denn auch bereits Erfahrungen mit Phishing-Awareness-Training? #00:03:18-6#

Experte 8: Ja, ist bei uns in der Firma ein Teil von unserem Angebot und Phishing ist aus meiner Sicht, ja, wenn wir, wie du sagst, Phishing-Awareness ist eine Kombination aus dem Phishing-Teil und aus dem Awareness-Teil, für mich ist Awareness der Überbegriff, also wie kann ich das Bewusstsein von einem Mitarbeiter in einer digitalen Welt beeinflussen oder stärker machen, festigen und Phishing ist eine von ganz vielen verschiedenen Disziplinen. Ich glaube jedoch auch, es ist so die Einstigsdro nicht Droge die Einstiegsthema /. Das Einstiegsthema, da gibt es aber logischerweise noch im Bereich Awareness aus meiner Sicht ganz viele weitere Themen, zum Beispiel wie arbeite ich unterwegs, wie gehe ich mit Passwörtern, wie arbeite ich im Homeoffice, welche Daten darf ich wo teilen und so weiter, da gibt es einen ganzen Blumenstrauß in diesem Awareness-Thema als Überbegriff und Phishing vermutlich das bekannteste. #00:04:31-7#

Severin Zimmermann: Ok, sehr gut, vielen Dank. Also, dass hier sehr viele Bereiche einspielen, das ist mir durchaus bekannt, einfach für dich als Hinweis in dieser Arbeit würden wir uns jetzt auf das Phishing-Awareness konzentrieren, da sonst das Spektrum etwas zu groß wäre, wenn ich alle Awareness-Themen beachten würde. Bezüglich Phishing-Awareness sind dir da positive Aspekte bekannt, die daraus resultieren können, wenn ich Phishing-Awareness durchführe? #00:05:06-1#

Experte 8: Ja, sehr viel, mit der /. Also das Wichtigste aus meiner Sicht ist, dass das eben nicht nur einmal gemacht wird, sondern dass das kontinuierlich gemacht wird, es ist wie überall, ich bringe da immer das Beispiel von alle, die schon Kinder haben, wir sind alle einmal selber Kinder gewesen und in der Schweiz

kennen wir dann das "Luege Lose Laufe" Lernprozess mit den Polizisten in der Schule und das war am Anfang, wenn ich das nur einmal gehört hätte, dann hätte ich das gewusst für eine kurze Zeit, ich würde heute aber nicht wahnsinnig talentiert über die Strasse gehen und weil ich das immer wieder gehört habe, immer wieder verstanden habe, ok, ich muss auf ganz viele "Dinge" achten, auch im Strassenverkehr, deshalb habe ich das ganz vielmals gehört und das ist bei Phishing-Awareness ziemlich genau gleich. Nur dass wir beim Polizisten vom "Luege Lose Laufe" dann irgendwann können, Phishing glaube ich müsste immer wieder passieren, aber das ist schon sehr, wir verlieren das ab und zu wieder oder auch die Phishing-Awareness Angriffe die verbessern sich, die verändern sich, die entwickeln sich weiter, deshalb ist es wichtig, dass wir auch da immer wieder Aufmerksamkeit erhöhen und das regelmässig vielleicht geprüft werden. #00:06:37-9#

Severin Zimmermann: Ok, also habe ich das richtig verstanden, es geht hauptsächlich /. Oder der Hauptvorteil ist eigentlich, dass ich die Awareness, besonders wenn ich es kontinuierlich mache, erhöhe? Oder fallen dir noch andere Punkte ein? #00:06:54-0#

Experte 8: Nein, ich glaube, dass es schon wichtig ist, dass man es im Alltag vermutlich auch sieht (unv., #00:06:59-9#). Die alte Nähe zum Tagesgeschäft ist sehr wichtig, wenn das so beispielhafte Print-Screens auf einer Powerpoint-Präsentation sind, hör zu, da hat jemand ein Mail von irgend einer Bank gekriegt, was eben Phishing wäre, dann ist das so theoretisch und das hat leider immer eine sehr grosse Distanz zu uns selber und deshalb glaube ich sehr gut, wenn es integriert oder sehr spezifisch in der eigenen Inbox ist und eben nicht einfach nur auf einer Powerpoint-Slide. #00:07:35-4#

Severin Zimmermann: Ok, vielen Dank, kennst du auch negative Aspekte, die aus Phishing Awareness resultieren können? #00:07:45-1#

Experte 8: Ja, also ob das negativ ist oder nicht negativ ist, vermutlich Interpretationsspielrahmen, es gibt natürlich auch das Risiko, dass dann aus Angst vor Phishing-Mails auch wichtige Informationen gelöscht oder nicht konsumiert werden können, das wäre jetzt eigentlich eine Information im Intranet gewesen, die für jeden Mitarbeiter wichtig wäre, das ist der Spagat in der heutigen Welt, Kommunikation per Mail ist super zentral, immer noch eine der wichtigsten Kommunikationskanäle. Und gleichzeitig lernen wir Security-Experten immer, du darfst nicht mehr klicken und du darfst nicht mehr schauen, das ist ein Risiko, das da herrscht. Ja genau, aber und dann gibt es logischerweise auch, wenn man zu viele Phishing-Awareness-Kampagnen durchführt, dann werden die entsprechenden Kollegen auch müde und dann wird einfach wie alle wenn es zu repetitiv wird, zu wiederholend, zu identisch, dann verliert es den Nutzen, also es muss schon spezifisch sein und die Menge muss gut überlegt sein. #00:09:09-2#

Severin Zimmermann: Bestens, zwei sehr gute Punkte, die du hier genannt hast. Jetzt etwas spezifischer, Phishing-Awareness-Trainings erfordern, oft auch technische Maßnahmen in Unternehmen, sind dir Aspekte bekannt, die sich positiv oder allenfalls auch negativ auswirken, wenn nicht technische Maßnahmen für die Sicherstellung, dass Phishing-Awareness durchgeführt werden kann, entstehen? #00:09:40-0#

Experte 8: Du meinst, mit technischen Maßnahmen /. Also für die Kampagnen, für das Awareness durchzuführen, die Maßnahmen? oder vielleicht machst du ein Beispiel, was du mit technischen Maßnahmen meinst. #00:09:54-2#

Severin Zimmermann: Genau, also jetzt beispielsweise, für mich gehört jetzt Phishing Simulation mit zu einem Phishing Awareness Training , das ist auch etwas am Stritten, ob man das separiert, also ist das Training nur das Training und das andere ist das Testing, in meiner Arbeit beachte ich das als das Gleiche und vor allem bei Phishing Simulationen werden oft Firewalls Ports freigeschalten, es werden AbsenderWhitelistings gemacht, das sind natürlich Punkte, die sich unter Umständen negativ auswirken können. Es gibt auch noch andere technische Maßnahmen die will ich jetzt aber nicht direkt drauf eingehen, da kommen wir ja bei den Detail Fragen noch dazu, aber sind die jetzt einfach mal so aus dem "Stehgreif" Maßnahmen bekannt, technische Maßnahmen, die negativ oder positiv sind? #00:10:49-4#

Experte 8: Was typischerweise, wie ich es kenne, oder wie wir es auch durchführen mit unseren Kunden, ich glaube sogar auch intern selber für uns als UMB, sind ohne technische Rekonfigurationen oder Ergänzungen, sondern was die Schönheit aus meiner Sicht sein könnte oder sollte ist, wenn das mit irgendeiner SaaS Lösung also Software-as-a-Service-Lösung, sprich du wirst teil von, du kaufst eine Lizenz oder eine Monats eine Jahreslizenz oder Mitgliederbeiträge, können das sein, um damit sicherzustellen, dass du typischerweise die E-Mail-Adressen von diesen Mitarbeitern erfasst, und da werden dann E-Mails verschickt, die von überall her kommen könnten, wenn eben nichts zusätzlich konfiguriert wird. das ist das Testen, da glaube ich, würde ich abraten, ich würde vermutlich nicht unbedingt oder wir machen das bei uns nicht, ich muss es so sagen, wir ergänzen keine technischen oder wie gesagt stellen irgendwelche Komponenten, Hardwarekomponenten oder Softwarekomponenten in ein Netz rein, das machen wir nicht. Und beim Simulieren oder vielleicht besser gesagt beim Schulen, das ist der zweite Teil, wenn die Mitarbeiter, bevor sie überhaupt das Mail kriegen, auf das sie möglicherweise klicken oder nicht, klicken, wenn wir dort ein Webinar oder so kleine Filmsequenzen müssen da geschaut werden und am Schluss von diesen Filmsequenzen gibt es dann eben auch einen kleinen Test oder da wird dann nicht ein Mail geschickt, sondern in diesem Webinar oder in diesem Tutorial wird dann jeweils drei Fragen gestellt, die kommen in meinem Verständnis am sinnvollsten auch aus dieser Software-as-a-Service-Plattform.

Des kann eine Learning-Plattform sein, die man extern bezieht, logischerweise gibt es auch Learning-Plattformen, die man selber betreibt, ist aber eher für die grösseren Firmen dann relevant. #00:13:15-1#

Severin Zimmermann: Okay, danke. Dann noch ergänzend oder eine andere Frage zum Umfeld und zwar du hast es gesagt, es wird oft als Software-as-a-Service bezogen, also hat man hier einen Dienstleister, der im Umfeld agiert und für das Unternehmen etwas macht, es gibt aber auch andere Umfeldfaktoren, wie Regulatoren etc., sind dir hier Aspekte bekannt, welche sich auf das Phishing Awareness Training auswirken? #00:13:48-3#

Experte 8: Ehrlich gesagt nicht, weil also ich /. mindestens weil ich überlege gerade bei unseren (unv., #00:14:00-3#) /. Ich glaube nicht weil in /. Allso Phishing Awareness Training wie in deiner Arbeit isoliert betrachte, vermute ich eher weniger, weil es ist ja nur in Anführungszeichen ein Mail, das ich zusende zustelle und dieses Zusenden von diesem Mail kann nicht reguliert werden, logischerweise gibt es Firmen, die nicht jedes E-Mail automatisch zustellen oder die dieses Mail ein wenig härter oder ein wenig weniger hart in eine Quarantäne schieben, das kann einerseits von der Firma definiert sein und andererseits kann das auch vom Hoster also Hosting-Provider definiert sein, alle diejenigen Fälle, die private E-Mail-Adressen, die Hotmail-E-Mail-Adressen und all diese privaten E-Mail-Adressen, da ist ja der Host derjenige, der entweder einen ganz harten Filter für diese Fishing-Mails einstellt oder eher ein toleranterer Filter. Aber in Firmen ist das häufig ein wenig anders, die E-Mails werden, bei uns bei der UMB gibt es punktuell auch E-Mails, die in die Quarantäne oder in den Spam-Folder gehen, aber ich würde sagen, da kommen immer noch /. Immer wieder kommen Mails eben in meine Inbox. ich glaube nicht, dass es eine regular /. Also das es reguliert allzufest reguliert werden kann oder soll, weil eben die E-Mails, die sind heute so exakt geschrieben, dass das eben /. Ich hatte gan /. (unv., #00:15:44-2#). Gibt es noch eine Sektion um Beispiele, zu nennen ich habe zwei, drei Beispiele auch privat schon erlebt? #00:15:50-5#

Severin Zimmermann: Du kannst die sehr gerne jetzt schon nennen. #00:15:53-6#

Experte 8: Ja, genau, gut. Also ein konkreter Fall war bei mir für meine /. Ich habe ein eigenes Domain, da gibt ich abe doch da läuft eine eine Website, aber vor allem, für meiene /. Damit ich meine eigene E-Mail-Adresse habe, die eben nicht @hotmail.com oder so, sondern @kaegis.net heisst, und deshalb gibt es da einen Hoster und für dieses Hosting bezahle ich logischerweise jeden Monat einen Betrag, damit die meine Website und meinen Mailserver und all das "Zeugs" betreiben und ich habe dann ein E-Mail gekriegt und da stand drauf, dass ich die Rechnung nicht bezahlt habe und ich muss das jetzt einer in Inkassofirma bezahlen, nicht mehr dem Hoster, sondern dieser Inkassofirma, weil der Hoster hat das, die ganze Mahntätigkeiten diesem in Inkassobüro übergeben. Und das Kritische

war, dass der Betrag, den ich bezahlen muss, der war richtig. Das ist ja noch ein bisschen verwirrend, weil der Betrag ist ja individuell, je nachdem, ob du ein grosses, kleines Mittelpaket hast, ist der Preis pro Monat unterschiedlich und ich hatte diesen Betrag war richtig und ich habe über "O-Scheibe" ich habe die Rechnung vergessen zu bezahlen und dann habe ich Antworten geklickt /. Ich habe nicht auf, ich bezahle sofort, auf den Button, ich bezahle sofort geklickt, sondern ich habe geantwortet und habe die Hostpoint, Info@Hostpoint das ist mein Hoster, dort als CC-Kopie mit reingenommen und habe gesagt, liebe Hostpoint und lieber inkassso, inkassogesellschaft, es tut mir leid, ich habe die Rechnung vergessen zu bezahlen, aber ich möchte die Mahngebühren nicht bezahlen. Die 10 Schweizer Franken-Mahngebühren, ich zahle heute gleich, aber könnt ihr mir bitte bestätigen, dass ich die Mahngebühren nicht bezahlen muss. Und dann hat die Hostpoint zurück reagiert, hey, passt auf, das ist eine in inkassobüro, nicht von uns. Also es war eigentlich Zufall, dass ich nicht reingefallen bin und wenn das reguliert wäre, dann könnte es sein, dass das Mail nicht zu mir gekommen wäre, ja, aber es hätte eben auch geschehen können, dass ich dann direkt bezahlt hätte. #00:18:12-7#

Severin Zimmermann: Sehr schönes Beispiel, das zeigt auch eben, dass Phischer heutzutage immer besser werden, auch individualisierte Phishing Angriffe machen. Vielleicht noch zum letzten Punkt bei den Hauptfragen, ich habe jetzt hauptsächlich aus drei Bereichen gefragt, organisatorisch, technisch, umfeld, ob dir da Aspekte bekannt sind, sind dir jetzt aus dem "Stegreif" noch Aspekte bekannt, die ich jetzt nicht erwähnt habe oder die du findest /. Die deiner Meinung nach noch wichtig sind, bevor wir zu den Detailfragen übergehen? #00:18:54-6#

Experte 8: Also ich glaube (unv., #00:18:59-7#). Habe ich schon erwähnt, aber was ich wichtig finde in einer Phishing Awareness Denkweise, dass man sich gut überlegt, dass die Awareness Kampagne oder so eine Awareness Tätikeit, dass die eben relevant für eine entsprechende Firma oder für eine entsprechende Person ist. Wie das Beispiel vorhin von Hostpoint sehr schön gezeigt hat, wenn der Betrag nicht gestimmt hätte oder wenn der Hoster ein Konkurrent gewesen wäre von meinem Hoster, dann hätte ich nie im Leben mir die Zeit genommen, ein Mail zu schreiben oder zu klicken. Das heisst, die Relevanz, die ist schon sehr zentral, weil nicht überall, aber ich glaube schon, wir Menschen sind uns heute ein bisschen mehr bewusst, dass, nein ich weiss nicht /. Zweites Beispiel ist von meiner Frau, da kam die Meldung, sie hat dein iPhone gewonnen und du kannst es abholen und logischerweise denkt jeder Mensch dann irgendwann, warum darf auch nicht ich einmal Glück haben, jetzt endlich habe ich auch mal Glück und das ist dann ein Klassiker, dass man sagt, ja jetzt habe ich auch mal Glück gehabt und das iPhone gewonnen, war dann logischerweise nichts und sie hat dann auch gemerkt, als sie das nach dem ersten Klick die Kontaktdaten angeben musste, dachte sie, oh, es ist jetzt doch ein bisschen speziell, ich gebe mal nichts ein. Aber das Konkrete und das Spezifische und das ist bei jeder Firma anders, wenn du eine Handelsunternehmung bist, sind andere Themen als wenn du Swisscom-Mitarbeiter bist und Swisscom-TV und Handy-Abos bereitstellst für Kunden, dann sind andere Themen relevant. #00:20:52-6#

Severin Zimmermann: Sehr gut, das ist eine gute Überleitung zur nächsten Frage und zwar eben, wie du gesagt hast, Personen, Firmen sind unterschiedlich, bist du der Meinung, dass auch das Phishing-Awareness-Training auf die Personen, also abgestummen werden sollte und personalisiert werden sollte? #00:21:17-1#

Experte 8: Ich also ganz der erste /. Ich glaube ja, mit der Ergänzung, dass der erste Teil, die erste Hälfte von einem Training, das ist wie überall, wenn du zum Sport gehst, wenn du zum Fussball gehst oder zu einer Sportart, die Grundregeln und die Grundmechaniken und die Grundfitness und die Bewegungsabläufe, die sind identisch bei allen Fussballspielern und schlussendlich wirds dann in der zweiten Phase wird es dann ein bisschen individueller. Erstens, wenn wir beim Sport beim Fussballbeispiel bleiben, wird es individueller, ob du Verteidiger oder Torwart oder Stürmer bist, da wird es individueller. Und noch individueller wird es, wenn du ein paar Zentimeter kleiner bist, musst du ganz andere Themen, dann übst du vielleicht ein bisschen mehr Sprungkraft. Jedoch, wenn du lange Beine hast, dann bist du eher ein bisschen schlaxig unterwegs und dann musst du an deiner Feinmotorik trainieren. Und deshalb glaube ich, die erste Hälfte, die soll einheitlich sein für alle Bereiche. Es gibt Grundregeln im Phishingbereich, im Phishing Awareness, die gelten vermutlich auf der ganzen Welt, die sind aber nur die halbe Wahrheit. Aber 50 Prozent der Wahrheit sind da enthalten und die zweiten 50 Prozent, die sind vermutlich ein bisschen spezifischer. So führen wir, by the way, auch, wenn wir als UMB für unsere Kundenkampagnen durchführen, dann ist die Plattform immer die gleiche. Die Mail Templates, die wir da zur Verfügung haben, die sind immer gleich. Da profitieren wir von Einheit, von Skaleneffekten und von Effizienz. Und gleichzeitig müssen wir ein entsprechendes Tuning, wir nennen das dann bei uns Tuning durchführen, damit wir eben eine belastbare Aussage kriegen. #00:23:14-7#

Severin Zimmermann: Also für dich ist es zweiteilig, zuerst Grundregeln und dann trotzdem Personalisieren. Siehst du Chancen und Risiken, die sich durch die Personalisierung von Phishing Awareness Trainings ergeben? #00:23:29-3#

Experte 8: Ja, gleichzeitig Chancen und Risiken, je nachdem, weil je personalisierter ich das mache, desto künstlicher werde ich die Klickrate erhöhen, dass die Leute reinfallen. Das kann irreführend sein, weil das wird dann sehr perfide wir hatten bei der Swisscom, kann ich mich erinnern, da hatten wir so eine Internetkampagne und da ging es um Swisscom TV und als Swisscom Mitarbeiter hattest du die Chance, bei Swisscom TV sogenannte Friendly Tester zu sein. Das heißt, du hattest dann immer die neueste Swisscom TV Box gekriegt, die neuesten Software Updates, wenn es irgendwelche Verbesserungen gibt. Dafür musstest du aber an einem Programm teilnehmen, um Feedback zu geben. Du musstest zuhause dieses Swisscom TV Box versuchen und testen und "Tatüttata" und dann Feedbacks ausfüllen. Und an einem Tag kam ein E-Mail und das besagte dann, dass wir im Swisscom /. Dear Friendly TV Tester, es gibt neu die

Funktion, dass wir Netflix direkt im Swisscom TV integrieren, damit du nicht mehr da die Fernbedienung wechseln und solche Sachen machen musst. Wäre das für dich einen Nutzen oder wäre das kein Nutzen? Bitte stimme hier ab. Wenn du so spezifische Fragen stellst in einer Phishing Kampagne, dann gehen die Klickraten hoch. Das waren dann 70-80% von allen Mitarbeitern haben geklickt.Jetzt ist die Frage, ist das wirklich repräsentativ? Die 80% Klickrate, ist das repräsentativ oder nicht? Und das ist das Risiko, dass du bei zu spezifischen, exakten, irreführenden Fragen eine zu dramatische Sicht kriegst. Und auf der anderen Seite ist, wenn du zu generisch bleibst, dann ist die Klickrate zu tief. Dann sieht es ja jeder, wenn du da mit schlechter Schrift und komischen Logos, dann klicken halt nur noch 20%. Und das ist die Chance und das Risiko beim Tuning oder beim generisch bleiben. Und die «Flughöhe» /. Die richtige «Flughöhe» zu finden ist, da braucht es vermutlich auch ein bisschen Begleitung von einem Experten, der sagt, ich würde nicht zu spezifisch werden, weil sonst geht die Klickrate zu hoch. Ich würde aber auch nicht zu "doof" bleiben, dass das ja jeder sieht. Es gibt immer irgendwelche, die klicken übrigens, aber die Klickrate kann schon nach unten gehen. #00:26:02-2#

Severin Zimmermann: Okay, sehr gut. Wir kommen später noch auf Klickrate zu sprechen. Ich würde es aber jetzt weiter mit den Fragen machen, bevor wir zur Klickrate kommen. Und zwar ist der Aufbau eines Phishing Trainings, das kann sehr unterschiedlich sein. Es gibt Embedded Trainings, wo die User geschult werden, wenn sie auf einem Maikl klicken oder auch präventive Schulungsmaßnahmen, wo sie eine Schulung zur Verfügung gestellt bekommen oder an einem Seminar teilnehmen müssen. Der Inhalt kann sehr unterschiedlich sein, sein das Gamification-Varianten, Videos, Fact Sheets und so weiter. Es kann im Klassenraum oder als Online-Schulung, als Flyer ausgetragen werden. Und ebenfalls ein Thema ist die Information an die Mitarbeiter. Sollten diese vorinformiert werden oder nicht? Das sind sehr viele Aspekte, die beachtet werden müssen. Wie ist deine Meinung nach dazu? Sollten solche unterschiedlichen Varianten in Betracht gezogen werden? Oder ist es einfach wichtig, dass ich ein Fishing Awareness mache, egal wie, wo und wann? #00:27:25-4#

Experte 8: Gute und sehr umfangreiche Frage logischerweise. Schlussendlich ist es nicht richtig und falsch sondern /. Also Ich kann erzählen vielleicht auch, wie das bei uns in unseren Kundengesprächen jeweils läuft. Die Frage kommt bei uns schlägt bei uns täglich auf. Das Kunden, die bei uns IT-Dienstleistungen beziehen, sagen, wie ist das jetzt mit Phishing? Was wir häufig sehen, ist, dass wir zuerst eine generische Schulung durchführen. Dann gibt es die Firmen, da sind die meisten Mitarbeiter im Gebäude, die arbeiten physisch vor Ort und sind alle da. Dann empfiehlt sich, diese Schulung über den Mittag zu machen Zum Beispiel mit Ich nehme Sandwiches mit und dann erzähle ich ganz generisch in 15-30 Minuten hört zu das sind die Anzeichen, die ein Phishing Mail ausmachen. Dann ist das eine physische Schulung. Da gibt auch andere Organisationen, die sagen, und das ist häufig auch die Frage erzählt mir mal einen Alltag bei euch in der Firma sind viele vor Ort. Nehmt Ihr zuerst einen Telefonhörer in die Hand oder schreibt zuerst ein Mail, was eure Kultur ist. Und je nach Kultur einer Firma

ist dann eben ein anderes Schulungskonzept korrekt. Und wie gesagt Schulungskonzept klingt jetzt so gross, und so umfangreich und so teuer. Das muss es nicht sein. Das kann eben auch zum Beispiel bei der UMB giebts ein Studio. Wir zeichnen da regelmässig kleine Filme auf. Und da könnte man auch so eine Aufzeichnung vom IT-Leiter machen. Ich erzähle euch jetzt kurz in 10 Minuten darüber, auf was ihr achten müsst. Bitte schaut den Absender an, Bitte fährt mit der Maus über die E-Mail-Adresse und schaut, was da wirklich für eine E-Mail-Adresse "aufpoppt" zum Beispiel. Und Dann halt so die 5 Tipps /. Dann kannst du diesen Film allen versenden und sagen ihr müsst den ansehen. Das kannst du nur nicht kontrollieren. Dann kommt der letzte Schritt vielleicht. Ich kann eben auch das mit einer Learning-Plattform machen. Da werden dann alle Mitarbeiter mit der E-Mail-Adresse erfasst und die werden dann zugeteilt. Das ist ein Pflichtfilm, den du schauen musst oder ein Pflichtwebinar oder wie das dann auch heisst. Und dann wird geprüft, wer das geschaut hat, in welcher Zeiteinheit und dort gibt es dann auch noch Schönheiten und Funktionen und Features. Muss man nur den Film schauen oder muss man anschliessend noch einen Test bestehen? Ich glaube das ist wirklich, das kann man in 10 Minuten machen, mit einem Factsheet oder mit einem der interne IT-Leiter fühlt sich bei der einen Firma sehr sicher, damit das zu erzählen die 5 Themen, welche 5 Punkte sind sehr wichtig, um ein Phishing E-Mail zu entlarven oder nicht? Und andere sagen, ich will lieber eine Online-Plattform. ich glaube, wichtig ist, dass man zuerst einmal Wissenstransfer betreibt. Also ich das Wissen, das man heute weiss eben diese ich sag jetzt 5 Faktoren, um das Fishing-E-Mail zu entlarven, diese sind auf der ganzen Welt identisch mehr oder weniger Schriftart, Sprache, Absender-E-Mail-Adresse und irgendwelche solcher Themen sind sehr /. Oder schlechte Logo- und Bildqualitäten in der Autosignatur, Autosignatur ist auch noch etwas, das sehr häufig geprüft werden kann und irreführend ist. Also das ist der ganz wichtige Teil aus meiner sicht, der sehr reduziert machen kann /. Gemacht werden kann am Schluss aber eben auch sehr strukturiert und kontrolliert gemacht werden kann. Jeder Mitarbeiter, muss es angesehen haben. #00:31:53-4#

Severin Zimmermann: Sehr gut, danke. Du hast vorhin die Kultur angesprochen. Das ist auch wieder ein sehr guter Übergang zur nächsten Frage. Und zwar geht es um die Cybersicherheitskultur. Wie reagieren Mitarbeiter auf Sicherheitsvorfälle. Wie ist ihre Einstellung gegenüber Sicherheit. Fragen Sie lieber einmal nach, bevor Sie auf einen mail /. Oder auf Link in einem Mail klicken. Oder sind Sie auf sich alleine gestellt oder haben das Gefühl, Sie sind auf sich alleine gestellt. Ist deiner Meinung nach die Cybersicherheitskultur wichtig für Phishing Awareness Trainings? Oder vielleicht sogar entscheidend im Aufbau der Cybersicherheitskultur? #00:32:42-0#

Experte 8: Sie hat sicher einen Einfluss. Was wir häufig sehen, ist, dass die Angst, dass Mitarbeiter auf diese Mails klicken, die ist berechtigt. Weil wir sind Menschen aus Fleisch und Blut mit Emotionen und wenn das Mail eine Emotion in mir auslöst, dann klicke ich. Wenn ich jetzt in die Ferien will und dann kommt ein Mail von den Malediven, dann ist die Wahrscheinlichkeit viel grösser, dass ich klicke, als wenn ich je schon in den Ferien war und Malediven doof finde, dann klicke ich vermutlich sowieso nicht. Also die Angst des Klickens die ist da

und was gefährlich sein kann, wenn man diese Mitarbeiterkultur bezüglich Cybersecurity zu kompliziert, zu regelmässig und zu häufig immer wieder stresst und schult und bemüht und wieder ein Mail verschickt, eine Info an alle, bitte passt auf. Das ist wie überall, als wir alle Jungs waren und Vater und Mutter sagten, da darfst du nicht springen, da darfst du nicht springen, da darfst du nicht gehen. Irgendwann hörst du nicht mehr, weil das ärgert, das nervt. Und ich glaube, das ist sehr wichtig. Auf der einen Seite darf das nicht zu kompliziert werden, weil wenn ich das Gefühl habe, dass jeder Mitarbeiter dann versteht, was irgendwelches Threat Monitoring oder ganz komplizierte Begriffe, ja, ich muss die Bedrohungen überwachen und Anomalieerkennung und da gibt es ganz viele komplizierte Fachbegriffe. Man glaubt im ersten Schritt, das könnte helfen, um das Bewusstsein der Mitarbeiter zu steigern. Häufig ist das eben das Gegenteil der Fall, dass durch die komplexe Herangehensweise den Mitarbeitern, die sagen, dann hör zu, ich check das eh nicht, ich will nicht, das muss aus meiner Sicht sehr /. Es muss passieren wie gesagt, der Mitarbeiter muss sich bewusst werden, dass er auch für die Sicherheit verantwortlich ist. Nicht nur der IT-Leiter ist für die Sicherheit verantwortlich, sondern jeder Anwender ist für die Sicherheit verantwortlich. Aber ich muss das einsorten, ich muss das reduzieren.Du spielst mit einem Fussballprofi anders, du sprichst mit einem Fussballprofi anders über Fussball als mit deiner Schwiegermutter du über Fussball sprichst und genau das ist die richtige «Flughöhe». Ich muss die Mitarbeiter wie Amateure behandeln. #00:35:29-5#

Severin Zimmermann: Sehr gut vielen Dank. Die nächste Frage geht in eine ganz andere Richtung. Und zwar ethische Aspekte. Sind dir ethische Aspekte bekannt, welche bei der Durchführung eines Phishing Awareness Trainings beachtet werden sollten? #00:35:47-9#

Experte 8: Also du meinst jetzt vor allem unsere, die ganzen Themen, welche Begriffe oder welche Terminologien dürfen verwendet werden? Oder meinst du auch Richtung Ethical Hacking und solche Themen? #00:36:03-9#

Severin Zimmermann: Es geht zum einen um die Begriffe, aber allenfalls auch sollte hier ein Externer einbezogen werden, der das prüft, ob das ethisch so korrekt ist, ob ethische Risiken entstehen bei dem, was man hier durchführt. Solche Dinge. #00:36:25-1#

Experte 8: Ja also eben das technische das technisch ethisch /.Man spricht ja häufig von Ethical Security und Ethical Hacking und Ethical Pentest und so weiter. Und das sind all diese Themen, die sagen, wir sind die Guten und wir versuchen da etwas zu klauen. Aber wenn es uns gelungen ist, zu klauen, dann geben wir es zurück und sagen dir, hey da ich konnte dir etwas klauen. Das wird in der Umgangssprache dann also ethisch als ethnisch angeschaut. Häufig auch White Hacking oder White Pentesting genannt. Weil es eben /. Das sind die Guten, das sind die Ethnischen. Und das ist natürlich schon richtig und wichtig, das man aber

alle /. Wenn du eine Phishing Kampagne machst oder Phishing Awareness durchführst, dann bist du in Anführungszeichen automatisch oder vielleicht unterschreibbar /. Also ich kenne keine Firma, die dann sagt, ich verkaufe mich als ethisch, ich bin dein Sublieferant, du unterschreibst mit mir einen Vertrag, dass du etwas kaufst bei mir und dann höhle ich dich aus, dann werde ich dir die Kronjuwelen klauen. Das gibt es vermutlich, habe ich noch nie gehört, aber es gibt sicher solche unethischen Verhaltensweisen, dass ich mir Geld gebe, Geld geben lasse von einem Auftraggeber und dann höhle ich diesen aus. Glaube ich schon, dass es vermutlich gibt es das. Ich galube eher nicht also ich wäre ja doof, als UMB zum Beispiel wäre ich doof wenn ich das /. Das kann ich mit einem einzigen Kunden machen und dann bin ich sofort tot in diesem Bereich. Und das andere ist natürlich in der ganzen /. Wir leben heute in einer Welt, in der man sehr vorsichtig mit Kampagnen in der Wortwahl und in der Terminologie und Themen wie Diversity sind heute sehr zentral. Und das kann auch ein bisschen streng sein zum Teil und ich glaube, da ist es einfach Vorsicht zu geboten, eventuell hilft es da, dass man auch da mit einem Experten sich unterhält. Da gibt es dann schon auch «Fettnäpfchen», wenn man dann über irgendwelche Randgruppen oder irgendwelchen Themen irgendeine Plattform anspricht, die zum Shitstorm werden kann. Also es ist immer eine Gefahr, man will nicht zu spezifisch werden, aber auch trotzdem ein bisschen Dramatik auslösen und dann nimmt man die Tinder-Plattform und dann kann es ein Schuss in den Ofen sein, der halt wirklich schwierig sein könnte. Ist die Kommunikationswelt oder unsere Welt hat sich da ein bisschen auch zum Guten weiterentwickelt, dass man ein bisschen vorsichtig ist, welche Begriffe darf man anwenden und welche nicht, was ist rassistisch was ist /. Was schliesst gewisse Themen aus, aber eben unter Umständen auch ein bisschen streng. #00:39:51-7#

Severin Zimmermann: Okay, vielen Dank. Jetzt schaue ich kurz auf die Uhr und sehe, wir haben jetzt noch eine Viertelstunde. Es sind aber noch einige Fragen offen, daher meine Frage an dich, musst du nachher gleich los, dann würde ich jedenfalls gewisse Fragen nicht mehr so spezifisch stellen. #00:40:13-2#

Experte 8: Ja ich hab um /. Ich habe ein Meeting um 10.15 Uhr, also wir können noch 5 Minuten oder so länger können wir machen, ich muss mich dann noch kurz vorbereiten, wenn wir 5 nach oder so anpeilen können, wäre das gut. #00:40:26-1#

Severin Zimmermann: Sehr gut, dann werde ich jetzt klickraten, hast du bereits vorhin erwähnt, da werde ich nicht mehr weiter drauf eingehen. Technische Vorkehrungen haben wir auch bereits angesprochen, ihr selbst macht das nicht. Dann zu diesem Thema, und zwar technische Sicherheitsmaßnahmen sorgen gegenüber den /. Also jetzt technische Sicherheitsmaßnahmen, welche für die Abwehr von echten Phishing sind, sorgen oft für ein Mitarbeiter und für falsches Vertrauen, und zwar dass sie denken, die Firma hat ja Sicherheitsvorkehrungen, also das was ich bekomme ist alles richtig, kann ich ja klicken. Wie siehst du das mit den falschen Vertrauen, ist das wirklich so, birgt das Chancen und Risiken?

#00:41:21-4#

Experte 8: Ja, also heutige, moderne sogenannte Endpunkt-Schutzlösungen können tatsächlich sehr viele Phishing E-Mails erkennen, und zwar nich nur, nicht zwingend wegen dem Phishing Mail, das alleine ist ja einfach Text, aber es gibt Lösungen, die können prüfen, was hinter einem Link, der da, im Mail enthalten ist, wo die Kommunikation hingeht, und wenn man dann eben klickt, dann kann man unter Umständen sehen, a, jetzt geht eine Kommunikation auf einen Server, auf dem eben eine Phishing-Website /. Wenn die Website aussieht wie die UBS-Website, die sieht identisch genau gleich aus, ist sie aber nicht, dann wird die häufig, die Phishing-Website, die läuft auf einem Web-Server irgendwo in Nairobi oder in Moskau oder in wo auch immer, und das kann man erkennen. Da gibt es einen Schutz, aber der ist logischerweise nicht 100% nie im Leben, deshalb gibt es eben eine geteilte Verantwortung im Bereich Phishing Awareness. Die eine Verantwortung liegt tatsächlich bei der IT oder bei der Firma, bei der Organisation, die Prozesse zu definieren und technisch zu schützen, und die andere Verantwortung bleibt immer bei den Mitarbeitern, weil am Schluss, wenn er klickt, Er wird nicht /. Kommt niemand in den Knast. Aber es braucht das Bewusstsein, dass ich vorsichtig bin, mit irgendwelchen Themen zu klicken. Die Hacker werden immer exakter, immer fein /. Immer feiner in der Definition, wohin und wie kann man die Daten des Kunden kriegen. Desshalb ja viel ist geschützt, aber das ist eine falsche Sicherheit, wenn man sagt, ich kann überall klicken, die sehen das dann schon, das ist nicht der Fall. #00:43:33-2#

Severin Zimmermann: Okay, danke. Dann auch noch technisch, oft werden technische Maßnahmen oder erweiterte Maßnahmen wie Warnhinweise für den User generiert, sei das ein Button im, falsch, sei das ein Banner im Mail, wenn es von extern kommt, Warnhinweise, wenn ich auf einen Link klicke. Denkst du, die sind notwendig, oder reicht die Sensibilisierung bzw. Schulung aus? #00:44:06-1#

Experte 8: Vermutlich sowohl, als auch. Die helfen ein bisschen, die helfen logischerweise. Die Gefahr ist auch da wieder die gleiche. Wenn dann bei jedem Mail steht, achten, das ist ein externes Mail, dann liest du diesen Banner irgendwann nicht mehr. Es gibt vor allem auch der Firma oder dem IT-Leiter die Möglichkeit zu sagen, ich habe es dir doch gesagt, ich habe dich doch gewarnt, das steht doch im Mail, pass auf, das ist ein externes Mail. Das gibt vor allem einen Schutz für den mitarbeiter nein die IT-Abteilung "tschuldigung" und auf der anderen Seite ist es eben, wie gesagt, alles was repetitiv wird, was wiederholend wird, das wird irgendwann für den Konsumenten, für den User, für den Nutzer obsolet, weil es steht ja in jedem Mail. Desshalb ja, es macht Sinn, wir bei uns, bei der UMB zum Beispiel, haben keinen solchen Warnhinweis, da kann man dafür oder dagegen sein. Es gibt, glaube ich, auch nicht richtig und falsch. Was ich sehr gut finde, im Outlook, vielleicht wäre das schon die nächste Frage gewesen, im Outlook gibt es heute sogenannte Add-Ins, die man von Drittanbietern ergänzen kann, dann gibt es einen Knopf mit einem roten Dreieck drauf und wenn ich ein Mail lese, bevor ich das überhaupt anklicken muss, weil es in der Vorschau schon

gezeigt wird und du vermutest, dass das ein Phishing Mail sein könnte, dann klickst du auf dieses rote Dreieck oder auf das Ausrufezeichen, wie auch immer das aussieht und dann wird dieses Mail weitergeleitet an diese Prüfungsinstanz, sei das ein Team, sei das ein Mensch, sei das ein Tool, dass dann eben prüft, ob das wirklich ein Phishing Mail ist oder nicht. Wenn es keines war, kriegst du wieder das Mail und wenn es eines war, kriegst du eine Meldung, ja danke, du hast richtig gemeldet, Gratulation. #00:46:17-9#

Severin Zimmermann: Vielleicht, wenn ich hier gleich ergänzen darf, siehst du hier auch Risiken mit solchen, ich sage jetzt mal /. Oder ich habe die als Meldeplatformen benannt, wie der Button im Outlook, siehst du dabei Risiken, wenn man solche Meldeplatformen integriert? #00:46:36-5#

Experte 8: Ich glaube, sehr kleine Risiken. Die Plat-Serie /. Also kommt natürlich darauf an, wenn man da eine Gratisversion sich für eine Gratisversion entscheidet, dann gilt auch Datersatz, ist das Produkt gratis, bist du das Produkt, dann sind nämlich deine Daten oder deine Informationen das Produkt, deshalb bietet der Anbieter das gratis an, nicht weil er ein guter Mensch ist und etwas Gutes der Welt tun will, sondern weil er Daten sammeln will. Deshalb bezahltpflichtige Lösungen haben immer die Möglichkeit, dass du entscheiden kannst, wohin gehen die Informationen oder welche Informationen werden verschlüsselt und welche werden gesendet und dann gibt es aus meiner Sicht kein Risiko. Gratislösungen schicken dann halt weg /. Das Google-Navi ist das beste Beispiel, man hat immer das Gefühl, das sei, weil Google sagt, don't be evil, stimmt natürlich, aber die brauchen vor allem deine Geoinformationen, wo du dich befindest, wie schnell und was du tust, deshalb machen die das gratis. #00:47:50-0#

Severin Zimmermann: Okay, vielen Dank, dann die Frage, es ist heute ja üblich, dass ich Mails nicht nur auf meinem Desktop Mailclient checke, sondern auch Mobile Phones, Tablets etc., bist du der Meinung, dass diese Plattformen im Schulungsmaterial selbst auch ergänzt werden sollten und trainiert werden sollten oder siehst du da eher negative Aspekte? #00:48:19-3#

Experte 8: Also du meinst, Schulen, wenn ich unterwegs bin und ich nicht ganz jede Funktion im Outlook auf dem Mobile Device habe, sehe ich halt vielleicht nicht jede einzelne Funktion. #00:48:31-8#

Severin Zimmermann: Also ich meine zum Beispiel, das Havon über links ist ja auf dem Mobile Phone nicht gleich oder funktioniert nicht gleich wie am Desktop klein und deshalb könnte es sinnvoll sein oder könnte es aus deiner Sicht sinnvoll sein, dass ich dann das Schulungsmaterial zur Verfügung stelle, die auch Mobile Phones abdecken und sagen, wie kann ich Mails am Mobile Phone sicher prüfen? #00:48:59-7#

Experte 8: Macht sicher Sinn, auch da generisch dann halt, wenn ich unsicher bin bei einem Mail, dann kliche ich lieber eben absolut /. integrieren würde ich, weil ich glaube, je nach Firma, wenn es wirklich Firma gibt, die Mails auf den Mobile Phones nicht erlauben, dann ist es logischerweise nicht relevant, aber es ist heute fast in jeder Firma relevant, muss man schon schulen, glaube ich schon. #00:49:29-8#

Severin Zimmermann: Ok, sehr gut. Dann ihr selbst seid ja eigentlich ein externer Partner, der Unterstützung bei Phishing Awareness Trainings anbietet. Siehst du gegenüber externen Partner Chancen und Risiken, die sich ergeben können für Firmen, wenn sie mit externen Partnern zusammenarbeiten? #00:49:48-5#

Experte 8: Also Risiken ist immer das gleiche Risiko, dass du Angst hast, dass du jemanden /. Das du etwas erzählen musst, was du lieber niemandem erzählen willst. Ich in der heutigen Zeit finde das kein Risiko, im Gegenteil, das ist ein bisschen eine Schweizer DNA, dass wir lieber, wir sprechen nicht über den Lohn und wir sprechen nicht über diverse, verschiedene Themen. Und gerade im Security ist das eigentlich das grösste Risiko, dass wir das Gefühl haben, ich muss ja nicht jetzt Detail sagen, aber nichts dazu sagen ist eigentlich das grösste Risiko, dass ich sage, oh, die Security gebe ich nicht draus, die mache ich selber. Und dann hat man das arrogante Gefühl, dass man alles besser weiss, das ist gerade im Security Bereich leider nicht mehr möglich, da braucht es Experten. Und deshalb ist für mich die Begleitung durch einen externen Partner vor allem eine Chance, glaube ich. Logischerweise ein gutes Vertrauensverhältnis aufbauen mit dieser entsprechenden Partnerfirma zu überlegen, ist das jetzt eine amerikanische multinationale Firma, die keine Emotionen zu mir in der Schweiz hat, vielleicht hat man an dem Freude vielleicht auch nicht und da gibt es auch nicht richtig und falsch, aber die Vertrauensbeziehung, die finde ich wichtig. #00:51:16-9#

Severin Zimmermann: Okay, also du hast jetzt eben die amerikanische Firma angesprochen, also siehst du das eigentlich bei ausländischen Partnern einfach so, dass einem Vertrauen gegeben sein soll oder siehst du noch andere Risiken? #00:51:31-7#

Experte 8: Ja, also der Punkt ist ja auch diese Tools, die wir verwenden, schlussendlich kommen die fast alle aus amerikanisch /. Schlussendlich enden die oder werden früher oder später von amerikanischen Firmen gekauft. Das mit der Schweizer Lösung, das funktioniert ein bisschen weniger, aber, oder das ist vielleicht die "Krux" oder die Lösung, ich kann ja zu einem Schweizer Partner gehen, der meine Sprache spricht und der dieses Tool selber einsetzt und das bei 100 Kunden, bei 100 weiteren Kunden auch schon angewendet hat, dann versteht der das viel besser und die Vertrauensbeziehung muss sich ein bisschen weniger

zu dieser amerikanischen Firma aufbauen, sondern eben zur Schweizer. #00:52:17-2#

Severin Zimmermann: Okay, vielen Dank. Dann sind dir rechtliche Aspekte bekannt, die bei der Duraufführung eines Phishing Awareness Trainings beachtet werden sollten? #00:52:27-5#

Experte 8: Nicht also ich versende /. Eben ich glaube, das rechtliche Thema ist das, darf ich, wenn ich mit einer so einer /. Wenn ich das nicht über den Mittag am Mittagstisch mache, sondern wenn ich das mit einer Plattform mache, auf welcher ich die E-Mail-Adressen erfasse, dann muss ich logischerweise überlegen, was sind die Regeln oder die Vorgaben, die meine Firma oder die Industrie hat. Wenn ich eine Privatbank bin, dann muss ich das einfach geprüft haben mit dem Verantwortlichen, derjenige, der für den Datenschutz verantwortlich ist, aber typischerweise gibt es wenig oder keine Limitierungen, weil wir ja nur E-Mails, wir erfassen nur die E-Mail-Adresse und versenden E-Mails. Mehr machen wir nicht. Somit sind die Limitierungen eher wenig, eher wenig, eher reduziert vorhanden. #00:53:28-3#

Severin Zimmermann: Okay, sehr gut. Dann sind dir externe Parteien, Regierungsinstitutionen, Hosts, Registrer etc. bekannt, die informiert werden sollten, wenn ich ein Phishing Awareness Training durchführe, vor allem auch in Bezug auf Phishing Simulationen? #00:53:46-0#

Experte 8: Nein, Nein. #00:53:49-1#

Severin Zimmermann: Gut dann ist dir eine Meldepflicht bekannt, die gegeben ist, wenn ich Opfer eines Phishings wurde? #00:53:58-7#

Experte 8: Eine Meldepflicht wird im Moment in der Schweiz diskutiert. Eine Meldepflicht gibt es noch nicht, mindestens nicht in den meisten Industrien. Zum Beispiel in der Finanzwelt gibt es die FINMA, da gibt es eine Meldepflicht, aber es gibt ja das NCSC, das Nationale Zentrum für Cyber-Sicherheit, da wird im Moment sehr intensiv von Meldepflichten, von Cyber-Attacken diskutiert. eine einem /. Es wird gewünscht, dass man man sich solche /. Das man solche Dinge meldet beim NCSC, aber eine Meldepflicht gibt es nicht, giebt es noch nicht. #00:54:39-7#

Severin Zimmermann: Sehr gut, vielen Dank. Dann noch /. Oder jetzt sind wir

eigentlich schon fast am Schluss. Sind deiner Meinung nach noch Aspekte offen oder Punkte, die wir nicht besprochen haben, die du noch erwähnen möchtest? #00:54:58-0#

Experte 8: Gut also nur einer. Ich finde es sehr wichtig, dass Phishing ist ja reaktiv da mus zuest /. Ich versende zuerst ein Mail und dann schaue ich, ob die Menschen da klicken oder nicht. Ich habe da noch nicht einen proaktiven Schutz, das haben wir in einer der letzten Fragen kurz darüber gesprochen, über die technischen Schutzmassnahmen, die möglich sind. Ich glaube, reaktive oder eben diese Phishing Awareness, ich versuche den Faktor Mensch zu stärken und das darf nie als komplette Lösung betrachtet werden. Phishing Awareness ist immer eine Ergänzung im ganzen dispositiv. Ist in deiner Arbeit jetzt nicht relevant, aber glaube ich, ist wichtig, dass man das einordnet. Das ist ein LEGO-Baustein aus einem ganzen Gebäude, aus LEGO-Steinen und nicht das ganze. Das erachte ich als wichtig. Du hast auch organisation /. Wir nennen bei uns immer die drei Themen Organisation, Technik und Mensch. Das sind die drei Disziplinen, die einen Cyber-Vorfall begünstigen oder die man beeinflussen kann und soll, um einen Cyber-Vorfall zu verhindern. Jetzt sprechen wir nur über den Faktor Mensch. Klickt der Mensch darauf oder was könnte der Mensch dazu beitragen, dass es eben keinen Sicherheitsvorfall gibt? Ein Drittel der Lösung ist der Mensch und die anderen zwei Drittel sind die organisatorischen Themen, Prozesse, Regeln, Vorgaben, Datenschutz und was ist die Technik? Das ist der IT-Leiter. Nur ein Drittel des Problems ist der IT-Leiter, der die Firewall und all diese Schutzmechanismen einstellt. Die anderen zwei Drittel sind entweder die organisatorische Seite oder die menschliche Seite, also der Mitarbeiter. #00:56:58-1#

Severin Zimmermann: Sehr gut, danke für die Ergänzung sehe ich übrigens gleich. In meiner Arbeit ist jetzt nur Phishing Awareness Thema. Ich selbst komme aber auch aus der Praxis und ich weiß, dass Phishing nur ein kleiner Bereich ist. Dann meine letzte Frage. Und zwar werde ich noch weitere Interviews durchführen. Dürfte ich dich, falls da neue Aspekte aufkommen, von denen ich auch noch gerne deine Meinung hätte, nochmals kontaktieren? #00:57:27-9#

Experte 8: Sicher. #00:57:29-1#

Severin Zimmermann: Sehr Gut Danke, dann werde ich die Aufzeichnung jetzt beenden.

K Kodierung und Zuordnung Experten-Interviews

Codesystem

- Organisatorisch
  - Risikominimierung
  - Repräsentation des Security-Teams
  - Kosten und Aufwand
  - Verhalten/Eigenschaften der geschulten Mitarbeitenden
    - Eigenschaften der geschulten Mitarbeitenden
    - Verhalten der geschulten Mitarbeitenden
  - Art und Aufbau einer Schulung
    - Schulungsmethode
    - Schulungsmedium
    - Schulungsbestimmungen
    - Aktualität des Schulungsmaterials
    - Personalisierung der Schulung
    - Intervall der Schulungen
  - Normen, Richtlinien und kulturelle Aspekte
  - Ethische Aspekte
  - Aspekte der internen Rechtfertigung
- Technologisch
  - Systemlösungen
  - Technische Abwehrmassnahmen
  - Vertrauen in die Technik
  - Technische Warnhinweise
  - Unterschiedliche Plattformen
  - Interne Meldeplattform
- Umfeld
  - Einbindung externer Firmen
  - Meldungen an Externe
  - Rechtliche Aspekte

Codes

Organisatorisch

Organisatorisch — Risikominimierung

„Es ist natürlich klar, dass ein Phishing Awareness Training das Ziel hat, die Leute zu sensibilisieren. Das heißt, dass wir als Ziel immer haben sollten, dass wir Leute eigentlich schulen, richtig auf solche Phishing E-Mails zu reagieren und Phishing E-Mails auch zu erkennen und ich denke, Phishing Awareness Training kann da wirklich auch gewissen Leuten auch helfen, diese Sensibilisierung zu entwickeln“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 13)

„So the business value of the awareness is it's following first reduced risk of breach, so people know how to identify a phishing emails, they know how to identify not only fishing emails also fishing SMS or fishing phone calls, right, this is the first thing, first benefit, right.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 18)

„some there are some research that is saying ah doing a lot of fishing training can actually reduce in the way that i like um i'll call it thomas um but i think this this kind of results are quite biased so i think if you're doing it wrong you're over teaching people that already know and you're under teaching people that don't understand you're just even annoying it's scary even more that can be even worse so yeah you need to.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 34)

„Ja, am Schluss geht es ja immer um Risikominderung, oder?“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 12)

„Ja. Und natürlich geht es darum, dass das Risiko letztlich auch für die Organisation für die Hochschule jetzt in unserem Fall zu minimieren“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 10)

„Und die Person zu sensibilisieren, auf das auf das Thema Phishing die damit verbundenen Risiken und vielleicht auch auf neue Trends, also die Phisher gehen ja auch immer mit der Zeit passen ihre Kampagnen an.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 10)

„dass die User sensibilisiert werden auf ein gewisses Verhalten, vor allem auch trainiert werden, wie man mit Phishing umgeht und Phishing-Kampagnen haben auch den Vorteil, dass man thema-basierend die richtigen E-Learnings zuweisen könnte oder kann“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 2)

„Also ich kann mir gut auch vorstellen, dass man ein bisschen das Interesse an Security wecken kann dadurch in Personen, also dass Personen sich eher dafür interessieren, weil sie näher an das Thema herangezogen werden und dass sie merken, dass das effektiv ein Problem sein kann und dass sie auch zum Beispiel auch in ihrem Privatleben damit Vorteile ziehen können. Sowas in die Richtung“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 4)

„Die Chancen für den Mitarbeiter sind natürlich er lernt etwas dazu, also er kann sich weiterbilden, hat sich fortbilden, er kann das ganze. Selbstverständlich nützt ihm auch, wenn er das privat anwenden kann. Also jeder hat heute denke ich, eine Mailbox zuhause und bekommt auch zu Hause solche Mails dir lieber nicht gern hätte“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 20)

„wir verlieren das ab und zu wieder oder auch die Phishing-Awareness Angriffe die verbessern sich, die verändern sich, die entwickeln sich weiter, deshalb ist es wichtig, dass wir auch da immer wieder Aufmerksamkeit erhöhen und das regelmässig vielleicht geprüft werde“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 10)

Organisatorisch — Repräsentation des Security-Teams

„And another indirect let's say byproduct of that is that the security team has an opportunity to present themselves and their services saying hey guys we are here if you need this you come to us we are going to help you understand you we care about you and so on“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 18)

„the regular employee never exposed to any of that the regular employee never logging into the firewall the regular employee don't you know check the cables in the server room how they are connected and other (unv., #01:17:40-5#). The only part of the work that people see "the tip of the Iceberg" of the CISO that is up outside of the water that all the employees see is including the CEO is the security awareness program this is the only thing the CISO is doing that all the employees can come and feel and see and touch and lick okay it's the only thing that it's the only thing that he cooks that they eat. Okay and if this is crap if you're getting them lunch from vietnam they might not like it this is what they think about your entire work and this is what they think about your entire security this is how much they care also about the security itself. So this is super important this is why you want it to be like super on point this is why there are so many even CISO's that are completely obsessed with the aesthetics of the programs beyond the content itself and it's very hard to do it for instance“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 99)

Organisatorisch — Kosten und Aufwand

„Aber es gibt natürlich auch viele Leute, die das als Zeitverschwendung ansehen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 15)

„Und für diese Leute ist es dann insofern negativ, dass sie sich ein bisschen vor den Kopf gestoßen fühlen Oder dass sie eben das Phishing Training als Zeitverschwendung ansehen, oftmals“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 15)

„es gibt natürlich noch viele andere, auch organisatorische Aspekte Also man darf natürlich nicht unterschätzen den Aufwand, den so eine Phishing Kampagne generiert, was man auch negativ natürlich werten kann.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 17)

„Das größte Risiko, wie ich schon angesprochen habe, man generiert relativ viel Aufwand mit Phishing-Awareness. Gerade wenn man das in einer großen Firma macht, dann müssen da wirklich viele Personalressourcen eingesetzt werden“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 39)

„o the disadvantages of course wasting the employee's time and annoying them, that's the main disadvantage of that, and also yeah when if you thought if it's done especially too much then the employees can just assume everything is just phishing training and don't really understand when something really is coming their ways.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 18)

„more negative stuff is that the security team is always every security thing there are endless things to do and nobody has the time to have the people to run this program this looks always like the least important thing but also it's important but it's another thing the team has to do. And it usually also uses products that cost money so there are serious costly. And can also generate a lot of noise in the sense of you're running it and then a lot of employees are annoyed and sending you emails and questions and why is it like this why is it like that what what do you want from me and so on“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 20)

„Und das ist die Frage, wie viel Geld nimmt man in die Hand, um wie viel Risiko zu mindern?“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 12)

„es bedeutet Aufwand. Es bedeutet organisatorisch Aufwand. Es bedeutet Aufwand auf der technischen Implementationsseite, in der Betriebsseite. Inzidenz, die auftauchen. Also Inzidenzvolumen war sehr hoch bei uns“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 14)

„Eine Sache ist, denke ich, wichtig für Unternehmen, man kann so eine Phishing Awareness Kampagne mal punktuell machen, aber beiläufig ist das nicht möglich, das ist wirklich ein Job, der einen fordert, wenn man die Kampagnen durchführen möchte, das Ganze technisch aufbaut, technisch begleitet, organisatorisch begleitet, man kommt in viel Diskussion mit unterschiedlichsten Stakeholder in Unternehmen, wie gesagt, der eine fühlt sich schon beübt nach der dritten Mail, der andere legt die Zehnte einfach weg oder löst sie. Wir sind Menschen, wir sind unterschiedlich, das ist wirklich schon ein Job für eine Person, auch das Durchführen von den Awareness Trainings jetzt nicht nur online, sondern also digital, jetzt über Portal, über Quizzes, sondern wie eben schon gesagt, über wirklich Awareness Trainings auch vor Ort oder per Cam“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 85)

„Also vielleicht einfach ergänzend. Der Aufwand, um die Simulation durchzuführen, ist nicht nur die Inbetriebnahme, die Entwicklung von den Kampagnen, sondern das ist dann auch im Nachgang die Beantwortung von Anfragen dazu“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 22)

„Das sind meistens Aussagen wie ist überflüssig, braucht nur viel Zeit. Meine Leute müssen arbeiten, die haben keine Zeit da halbe Stunde Stunde Schulung zu machen, das ist aber mehr“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 10)

„wie wir das jetzt besprochen haben tun sich viele Firmen schwer und sehen keinen direkten Kosten nutzen daraus. Was vielfach dazu führt, dass solche Trainings nicht durchgeführt werden. Eben weil es keinen direkten Benefit daraus resultiert oder nicht Messbar ist mindestens.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 74)

Organisatorisch — Verhalten/ Eigenschaften der geschulten Mitarbeitenden

Organisatorisch — Verhalten/Eigenschaften der geschulten Mitarbeitenden — Eigenschaften der geschulten Mitarbeitenden

„Zum Beispiel die Human Resources Leute, Unsere Personalabteilung, muss anders adressiert werden wie Dozierende oder Studierende oder“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 26)

„ich hab das eigentlich immer eher an der Funktion im Unternehmen festgemacht“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 26)

„Es wird relativ komplex, schnell also das relativ schnell komplex, wenn man wirklich auf alle diese Kriterien und zusätzlich noch auf die Funktion eingehen will und das berücksichtigen will und das hat auch eine technische Herausforderung, weil demographischen Background da ist normalerweise in keinem ICT System, das ich kenne hinterlegt. Also wenn wir jetzt, sagen ok, da kommt jemand ist gebürtiger Nigerianer oder so hat vielleicht einen anderen Bezug zu zu Phishing als jemand aus Norwegen, oder. Die Informationen liegen uns gar nicht vor, das heißt,

wir können das praktisch gar nicht umsetzen.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 26)

„erhofft haben wir uns natürlich, dass das unsere Mitarbeitenden, wenn ein echtes Fishing reinkommt, dass sie da vorsichtiger agieren und vielleicht und wirklich zweimal schauen ist ist der Link wirklich echt ist der Absender echt und macht macht der Text der Mail überhaupt Sinn oder ruf ich lieber den Absender an und frag ihn, Ob die Mai legitim ist?“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 28)

„ja, es gibt natürlich unterschiedliche Personenkreise, die unterschiedliche betroffen sind sei das Know How technisch vor dem Computer selbst, aber auch in ihrer Funktion also ich denke da an. Bereiche wie Personalabteilung, Finanzwesen, Geschäftsleitung. Bereiche, wo Personen Datenschutz ich sag mal Gesundheitswesen usw sicher gefährlich als nicht gefährlicher wo wo prädestiniert sind ,um gezielt angegriffen zu werden. Vergleichbar oder das Gegenteil dazu ist ich sage jetzt mal der Mitarbeiter draußen in der Produktion, der sein eher ERP System hat und die Aufträge ausliest und die Daten eingibt wenig mit sensiblen Daten zu tun hat und so weiter. Ich denke, da sollte sicher eine entsprechende Kategorisierung stattfinden, auch was Menge tief bei usw angeht vom Training selbst“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 18)

Organisatorisch — Verhalten/Eigenschaften der geschulten Mitarbeitenden— Verhalten der geschulten Mitarbeitenden

„Hat man nämlich selbst, wenn man noch so viele sensibilisierte Personen hat, hat man trotzdem immer noch Personen, die einfach darauf klicken, weil sie neugierig sind, die wissen was ist Phishing. Also hat mir ein Kollege hat mir das damals gesagt hatten wir dann an Vorfall oder. Hat mir dann gesagt, ja zu Hause auf meinem privaten hätte ich nicht darauf geklickt, aber hier bei der ZAHW hab ich gedacht ich schau mal was passiert oder. Und da kann man noch soviel sensibilisieren noch soviel sensibilisieren“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 34)

Organisatorisch — Art und Aufbau einer Schulung

Organisatorisch — Art und Aufbau einer Schulung — Schulungsmethode

„wenn man diese vielen Variantenmöglichkeiten hat, das zu organisieren, kann man natürlich das Training an die Zielgruppe anpassen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 31)

„Aber es gibt natürlich auch Chancen, wenn man das in einem größeren Rahmen macht, dass man sagt, man stellt den Leuten ein Training zu fügen, die das zum Beispiel machen wollen. Also ich sehe hier, wie die Chancen sind, dass man die Zielgruppe möglichst gut abfangen kann,“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 31)

„Bei Risiken ist es natürlich so, wenn man seine Zielgruppe nicht gut kennt oder wenn es eine sehr große Zielgruppe ist, ist es natürlich schwierig zu entscheiden, welche Art von Training wählt man eigentlich. Und das ist das größte Diskurs natürlich, dass die gewählte Art des Trainings überhaupt nicht /. Also keinen Anklang bei der Userschaft findet, dass die Leute, die hier getrainiert werden, das überhaupt nicht mögen oder vielleicht auch nicht damit lernen können, weil das einfach nicht die Art von Methodik ist, die sie gewöhnt sind“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 31)

„Alle Varianten durchführen. Das ist ganz klar meine Meinung. Es muss Abwechslung rein, es darf nicht stupide werden. Also auch in der Front oder halt jetzt online mal das ganze demonstrieren, gewisse Fälle aufzeigen, was kann denn passieren, was passiert im Hintergrund vielleicht für auch die vielleicht etwas technisch versierteren Benutzer“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 29)

„Grundsätzlich versuchen wir über viele unterschiedliche Kommunikationskanäle die Informationen zu verbreiten, weil wir haben es auch mit ganz unterschiedlichen Persönlichkeiten zu tun. Der eine lernt eherr visuell, der andere eher über das was, ihm gesagt wird und /. Die Menschen haben auch ganz unterschiedliche Wahrnehmung“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 34)

„Und Ich finde es eher gut, wenn das eben über unterschiedliche Kanäle in unterschiedlicher Gestaltung zu unterschiedlichen Zeitpunkten kommt wichtig ist und das war der Punkt“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 34)

„Ja, ich denke also der Aufbau für diese Schulungen sollte so gewählt sein, dass der Mitarbeiter oder die Mitarbeiterin ich sag mal Spaß hat an der Schulung also das ist sich damit auseinandersetzen kann, damit sie auch etwas gefordert wird. Also ich denke da entweder eben ein interaktive Schulungen oder kurze Videosequenzen, gefolgt mit mit Fragen oder so Multiplechoice einfach, wo der wo der Mitarbeiter aktiv daran teilnehmen muss, eben weil es Spaß macht, ist die Chance größer, dass sie durchgeführt wird die Schulung, weil, wenn es keinen Spaß macht oder einfach ich sag jetzt mal Informationsblätter abgegeben werden“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 26)

Organisatorisch — Arten/aufbau Schulungen — Schulungsmedium

„wenn man diese vielen Variantenmöglichkeiten hat, das zu organisieren, kann man natürlich das Training an die Zielgruppe anpassen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 31)

„Aber es gibt natürlich auch Chancen, wenn man das in einem größeren Rahmen macht, dass man sagt, man stellt den Leuten ein Training zu fügen, die das zum Beispiel machen wollen. Also ich sehe hier, wie die Chancen sind, dass man die Zielgruppe möglichst gut abfangen kann“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 31)

„Bei Risiken ist es natürlich so, wenn man seine Zielgruppe nicht gut kennt oder wenn es eine sehr große Zielgruppe ist, ist es natürlich schwierig zu entscheiden, welche Art von Training wählt man eigentlich. Und das ist das größte Diskurs natürlich, dass die gewählte Art des Trainings überhaupt nicht /. Also keinen Anklang bei der Userschaft findet, dass die Leute, die hier getrainiert werden, das überhaupt nicht mögen oder vielleicht auch nicht damit lernen können, weil das einfach nicht die Art von Methodik ist, die sie gewöhnt sind.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 31)

„Alle Varianten durchführen. Das ist ganz klar meine Meinung. Es muss Abwechslung rein, es darf nicht stupide werden. Also auch in der Front oder halt jetzt online mal das ganze demonstrieren, gewisse Fälle aufzeigen, was kann denn passieren, was passiert im Hintergrund vielleicht für auch die vielleicht etwas technisch versierteren Benutzer.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 29)

„Grundsätzlich versuchen wir über viele unterschiedliche Kommunikationskanäle die Informationen zu verbreiten, weil wir haben es auch mit ganz unterschiedlichen Persönlichkeiten zu tun. Der eine lernt eherr visuell, der andere eher über das was, ihm gesagt wird und /. Die Menschen haben auch ganz unterschiedliche Wahrnehmung“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 34)

„Oder weil Leute haben meistens sowieso schon keine Lust drauf und es muss ein gewisses, es muss ein etwas Spaß machen. Es kann nicht /. Also wenn es langweilig ist, machen es die Leute sowieso nicht. Das ist ein wenig mein Gefühl“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 37)

„Das ist ja genau das, was wir jetzt auch bei uns anstreben wollen, dass wir das Training selber interessant gestalten. Security ist ein "trockenes Thema". Man muss es auflockern. Wie du Experte 6 gesagt hast, es muss vielleicht auch mal ein wenig Humor dazu. Es muss Gamification ist das große Wort heute. Ja Die E-Learnings, die müssen natürlich auch dementsprechend gestaltet sein. Eventuell muss man sich auch identifizieren können ja durch irgendeine Kampagne oder Design, eine Bildsprache“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 38)

„enau, weil sonst, wenn du zum Beispiel hingehst und sagst, "Jo", ich mache jetzt einfach irgendwie ein Training, ich nehme alle Leute, steck sie in den Raum. Ich glaube nicht, dass das extrem zielführend ist, bzw. es kann zielführend sein für Leute, die das möchten. Und herauszufinden, wer Spaß hat daran, das wäre vielleicht der nächste Challenge.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 41)

„Es wird dadurch auch sicherlich Interesse fürs Training erwecken ja“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 43)

„Ja, ich denke also der Aufbau für diese Schulungen sollte so gewählt sein, dass der Mitarbeiter oder die Mitarbeiterin ich sag mal Spaß hat an der Schulung also das ist sich damit auseinandersetzen kann, damit sie auch etwas gefordert wird. Also ich denke da entweder eben ein interaktive Schulungen oder kurze Videosequenzen, gefolgt mit mit Fragen oder so Multiplechoice einfach, wo der wo der Mitarbeiter aktiv daran teilnehmen muss, eben weil es Spaß macht, ist die Chance größer, dass sie durchgeführt wird die Schulung, weil, wenn es keinen Spaß macht oder einfach ich sag jetzt mal Informationsblätter abgegeben werden“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 26)

„Gute und sehr umfangreiche Frage logischerweise. Schlussendlich ist es nicht richtig und falsch“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 30)

„Dann gibt es die Firmen, da sind die meisten Mitarbeiter im Gebäude, die arbeiten physisch vor Ort und sind alle da. Dann empfiehlt sich, diese Schulung über den Mittag zu machen“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 30)

Organisatorisch — Art und Aufbau einer Schulung — Schulungsbestimmungen

„Es kommt natürlich darauf an, was man testen will. Ich sage jetzt natürlich, wenn man so eine Studie wie wir uns macht, dann ist es unerlässlich, dann muss man zwingendermaßen die IT informieren. Wenn man jetzt aber natürlich testen will, ob die IT selbst richtig auf solche Phishing-Attacken reagiert, in so einem Fall macht es natürlich, dass man die IT nicht darüber informiert oder dass man dann einfach sagt, man prüft, ob die internen Prozesse korrekt sind oder korrekt funktionieren und die Leute in der IT auch richtig auf eine solche Attacke reagieren können. In so einem Fall macht das eventuell Sinn, aber auch da ist es natürlich immer mit Vorsicht zu genießen, man will ja nicht die Leute vor den Kopf stoßen. Im Endeffekt, um dann eigentlich gemeinsam mit diesen Leuten einen besseren Sicherheitsstandard oder eine bessere Sicherheitskultur zu pflegen, sage ich mal“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 33)

„Der größte Risiko ist natürlich, dass die IT das eskaliert und dass es also echt einen Angriff ansieht und das kann natürlich auch dann außerhalb der Firma oder des Unternehmens kommuniziert werden. Also im Fall eines richtigen Angriffes kann es natürlich dann auch je nach Inhalt dieser Phishing Mails dazu führen, dass diese an nationale Stellen gemeldet werden oder sogar an strafrechtliche Stellen. Es ist meistens bei Phishing weniger der Fall, aber es könnte natürlich im schlimmsten Fall eskalieren, dass es auch rechtliche Folgen hat natürlich“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 35)

„Now another benefit that a security program has besides specifically, I mean the entire security program is used not only to teach phishing but not only to teach other topics of security, it can also explain and validate first that the users read and know the policies of the company, this is business value one in terms of compliance that you're compliant but you also reduce risk of people at risk not doing not following your directive and policie“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 18)

„Now because sometimes when you just give a bunch of lawyers some documents to write and then they just put it in some folder and everybody just need to read and click then sometimes you forget about it but when you really do such a program you spend so much time writing and education writing the course we have a password policy you have to follow it and you start making videos about it and writing text about it then it makes you rethink your your entire policy and you also get feedback from people feedback you wouldn't g“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 18)

„Yes you do i mean i don't think it's a legal requirement but for many companies their internal policy does not allow them to do something like that like to do phishing simulation attack without alerting the employees first but it's not like it's more like some article you have in the intranet like the next month or quater will have some phishing attack simulations so nobody“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 40)

„companies like to call teachable moment is after the user clicked the link but he shouldn't click then there is like this website and "oopsie" you clicked on the phishing link why don't you see this really cute five minutes video that or two minutes video that explains a bit about the basics of phishing or playing this game whatever but these are these are called micro learning and they are more like for reinforcement this are not this is not really the place to teach the the user about phishing because you assume /. You must assume that the user will not do any of that if he's doing it's nice but because when the user click your link it was while he was in the middle of the meeting middle of four this is not the time that we wanted to do this training. What you need to“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 42)

„Okay listen what is aware i mean the entire company should know there is a campaign running should tell them it doesn't help them really that much“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 52)

„So it's the same with phishing texting just letting know people know that oh. there is a phishing attack the next quarter there is another fish every quarter you tell them there is a phishing simulation in the next one two months so people are always alert you know they don't want to /. Tthey don't mind if they click something and then somebody in russia i don't know get something from it but if you know my colleagues are going to know about it maybe they tell my boss or i don't want to click it again it's much more important to them“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 52)

„Das zweite ist, Phishing Kampagnen, die durchzuführen, denkt man so im eigenen Unternehmen, ja, kann ich tun, kein Problem, ist ja das eigene Unternehmen, es ist abgesegnet bis oben hin.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 18)

„Einen Rückschlussziehen auf einen Endanwender kann zum Teil auch kritisch werden. Nehmen wir als Beispiel, wir haben eine Authentisierungsmaske, der gibt seine echten Credentials ein. Also hier ist auch, Klammer auf, wichtig, was man loggen darf und ob man gewisse Dinge opfusszieren sollte. Das ist auch ein wichtiges Thema“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 24)

„Also ich würde das IT-Personal per se nicht ausschließen. Die Frage ist allerdings, muss ich vielleicht doch eine Hand voll involvieren? Weil eben Incidentaufkommen, was passieren kann und so weiter. Das sind so Themen. Für uns war der Hauptfaktor mehr fernab von der ICT, der Service Desk“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 35)

„Und deshalb Service Desk schließen wir auch ungern aus, haben aber in der Vergangenheit es so gehandhabt, dass wir zumindest den Vorgesetzten informiert haben, dass da was läuft. Also falls dann irgendwie Unmut, ob der Menge oder komischen Anfragen entsteht in seinem Team, dass er dann eingreifen kann.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 35)

„kay dann also, da gibt es verschiedene Punkte zu beachten. Einer einmal ist es sicherlich, dass die angeschriebenen Adressaten, dass die vielleicht auch randomisiert sind, also einerseits /. Also die Person reden miteinander, wenn sie in einem Büro sitzen, dann reden die miteinander. Ich hab jetzt grad blöde Phishing Mail bekommen schau mal hier, das war von der Post Paketzustellung, dann weiß das der Kollege, dann bekommt der Kollege (unv., #00:08:25-4#) Kollege in sein Postfach hat es auch drin, klicke nicht mehr drauf. Das verfälscht dann letztendlich das Ergebnis und den Sinn und Zweck, sondern /. Ich finde es wichtig, dass das randomisiert wird idealerweise, wenn man das, wenn die Systeme das hergeben, dass nicht all /. Nicht mehrere Personen in einem gemeinsamen Büro zu einem dieselbe Phishing Mail bekommen, sondern dass man vielleicht mehrere Kampagnen fährt und die dann entsprechend verteilt geschickt verteilt, dass die, dass, wenn einer /. Wenn sie untereinander darüber reden dass, dass sie da das Ergebnis nicht verfälschen oder.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 18)

„ir machen das an der ZHAW so, dass wir Schlüsselpersonen informieren, also mindestens den Servicedesk, oder weil bei denen werden dann die Tickets auflaufen. Die müssen vor informiert sein auch stellen wir uns vor, es ist irgendwie Juli, die Hälfte vom Servicedesk ist in den Ferien und wir machen so eine Kampagne, dass muss in Absprache passieren, die werden sonst geflutet und können nicht mehr die wichtigen Themen bearbeiten“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 38)

„Klar, man muss, so Phishing Kampagnen darf man nicht oft mal rauslassen, sondern das muss gestaffelt werden. Einfaches Beispiel, dadurch entsteht Flurfunk, der ist eigentlich beim richtigen Phishing Vorfall sehr wertvoll, aber für eine Kampagne, der verhindert einen oder vermisst einem das erwartende Ergebnis.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 9)

„Und das Ganze, ganz wichtig ist auch, dass die Infrastruktur, also der Service-Desk vor allem, der muss auch informiert sein.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 12)

„Nein, warum? Klar, es gibt immer technische Leute, die müssen involviert werden aufgrund von dem, dass man die Phishing Kampagne technisch schon umsetzen kann. Aber ansonsten sind das normale User wie alle anderen auch, die im entsprechenden eventuell eine andere Anforderung an die Kampagne stellen und dementsprechend auch anders behandelt werden müssen. Aber es sind ganz normale Leute in der IT“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 45)

„Und Also im Endeffekt, die Leute, die informiert werden müssen, sind sicher. Es gibt ein paar und vor allem die Leute, die zum Beispiel die Macht haben, solche Kampagnen zu stoppen, die müssen unbedingt informiert sein, weil ich hätte die Flächendeckung gestoppt und dann wäre ja /. Wäre überhaupt nichts rausgekommen bei dieser Aktion“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 46)

„Aber was auch wichtig ist zu informieren, ist einfach auch ein Service-Desk. Die wissen nicht, was kommt, aber sie wissen, dass was kommt, damit sie sich darauf einstellen können, dass vermehrte Anfragen reinkommen.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 49)

„eine Chance sein, weil sie bei personalisierten Trainings sieht, welche Mitarbeiter explizit oder welche Mitarbeitergruppen ich sag jetzt mal sich schwerer tun mit der ganzen Materie gegenüber anderen.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 20)

„aus Sicht des Mitarbeiters aber ein Risiko sein, dass er ich sag jetzt mal, dass er an den "Pranger" gestellt wird, weil wenn seine Trainingsresultate nicht so gut sind wie eigentlich gewünscht also es kommt immer ein bisschen auf den Betrachter an.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 20)

„dass IT-Personal sollte nicht informiert werden, weil auch sie gehören aus meiner Sicht zu den eher Risiko behafteten Personalbeständen oder oder ja Abteilungen. Da IT doch in der Regel mit mehr Rechten ausgestattet ist als andere Mitarbeiter, Zugriff auf Systeme haben die Mitarbeiter gar nicht haben und so weiter von daher, denke ich gehört für mich IT-Personal eigentlich zu Hochrisikogruppe dazu. Und die Information ist von daher überflüssig. Sag ich mal da sonst der Überraschungseffekt fehlt und das ganze ich sage jetzt mal, etwas lockerer angegangen wird, als wenn sie es nicht wissen“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 28)

Organisatorisch — Art und Aufbau einer Schulung — Aktualität des Schulungsmaterials

„what are the the current trends in the industry right not in industry in the what are the risks to your company. For example after the war in ukraine there are a lot of phishing email shoot specific attacks that are asking you to donate for the ukraine and stuff like that so i know that poland was flooded with it and people they were like really in favor of the ukraine and it's funny because both Ukrainian and Russian hackers used it for their benefit.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 90)

„d die dritte Sache ist einfach Anstehendeereignisse, Weihnachtsferien stehen an, alles sind unter Druck, Jahresabschlüsse, solche typischen Termine. Und dann kommt doch schnell eine

Mail vom Chef, du, ich brauche ganz dringend diese Unterlagen, ich finde sie aber nicht, kannst du mal hier auf den Link klicken und schauen“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 24)

„Was war das zu Corona Zeiten haben die Phisher dann versucht, mit günstigen Schutzmasken und günstigen Desinfektionsmitteln die Leute zu /. Anzuziehen und dann als Ukraine Krieg startete haben, sie haben sie da auch Ängste geschürt und so versucht zu Phishen. Also wir müssen, wir müssen unsere Mitarbeiterinnen und hochschulangehörigen eigentlich konnte ich auch informieren über das Phishing Awareness Training Was sind eigentlich die aktuellen Bedrohungen. Die aktuellen Phishing Risiken“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 10)

„Es müssen auch Header und Bodies, wenn man einsetzt, zur externen Warnung zum Beispiel, die setzen wir an der ZHAW ein, die müssen natürlich in der Phishing-Mails auch berücksichtigt werden zum Beispiel.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 12)

„Es muss eigentlich sichergestellt werden, dass am User die E-Mail so präsentiert wird, wie ein echter Angriff auch präsentiert würde.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 13)

„Was auch ein externer Einfluss sein kann, was ich vorher schon mal kurz erwähnt habe, also auf die Kampagne selber, das sind so aktuelle Themen, wo man vielleicht nicht gerade angreifen sollte mit so einer Phishing-Kampagne, wie jetzt Ukrainekrise oder Erdbeben oder sonst irgendwas, wo man momentan vielleicht einen User noch speziell aufgrüttet damit. Also das sollte man vielleicht noch runterlassen. Ja“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 99)

„Es soll ein Training sein und nicht igendwie eine moralische Demoralisierung soll man natürlich unterbinden. Man muss ja natürlich auch gefasst sein, wenn es so extreme also externe Einflüsse sind, dass man vielleicht auch einen persönlich damit dann verletzen könnte. Das passiert einem beim DHL wahrscheinlich weniger“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 103)

„Sind sicher die positiven Aspekte sind die Schulung, die Instruktionen, die permanente Weiterbildung der Mitarbeitenden auch in Anbetracht, dass die Technologien. Wie Phishing daher kommt immer wieder neue Methoden, neue Ansätze findet und diese auf die User entsprechend (unv., #00:02:47-1#) beziehungsweise eben geschult werden können. #00:02:50-0#“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 8)

„Die Methoden ändern es gibt tagesaktuelle Geschichten, auf die eingegangen wird. Klassiker jetzt in der Vergangenheit die ganze Corona Geschichte da wimmelt es von Corona Mails. Jetzt aktuell ich sag jetzt mal CS bankencrash oder beinahe Crash das sind natürlich diese tagesaktuelle Dinge sind prädestiniert für solche echten Attacken und sollten auch übernommen werden im Trainings auch wieder im Zusammenhang, dass die Mitarbeiter sensibilisiert werden und wissen OK in den Medien wird jetzt Thema XY aktuell behandelt ich muss damit rechnen, dass die nächster Zeit Phishing zu diesem Thema kommen könnten“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 42)

Organisatorisch — Art und Aufbau einer Schulung — Personalisierung der Schulung

„Grundsätzlich wäre es natürlich insofern wünschenswert, als dass diese Leute wahrscheinlich dann durch diese sogenannten SpearPhishing-E-Mails besser geschult werden könnten. Das Problem ist aber meistens, dass es technisch und organisatorisch nicht so einfach durchführbar ist. Also im kleinen Rahmen geht das relativ gut, vielleicht wenn man die Personen kennt aber wenn man dann eine große Firma hat, ist es sehr unwahrscheinlich, dass diese E-Mails personalisiert werden können einfach aufgrund dadurch, dass die Person, die diese Trainings durchführt, diese zu lernende Person gar nicht kennt. Und In diesem Umfeld ist es sehr schwierig, eine personalisierte Training anzubieten oder eine persönliche Training durchzuführen. Wäre aber natürlich insofern wünschenswert, als dass die Leute sicherlich davon profitieren könnten“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 25)

„weil man weiss heutzutage aus der Phishing-Studien, dass man, wenn man gezielt Content versendet der auch relevant für den alltäglichen Beruf einer Person ist oder für die allgemeinen Prozesse, die diese Person oftmals benutzt, dass diese dann tendenziell eher auf diese Phishing-E-Mails darauf einfallen. Das kann man natürlich gezielt auch für Phishing-Trainings einsetzen, für Phishing Awareness und das macht insofern auch Sinn, dass man das dann wirklich personalisiert.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 27)

„ist natürlich sehr wichtig und ich würde hier klar empfehlen, dass man in einer Phishing-E-Mails-Kampagne immer auf die Zielgruppe abstimmen sollte“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 27)

„wenn man auf gewisse Zielgruppen E-Mails erstellt und diese dann sendet, dann kann es natürlich sein, dass das auch ethisch ein bisschen ein Problem ist Insofern, dass man vielleicht ein Thema aufgreift, das dann für diese Usergruppe wie sagt man /. Als unzulässiges Training angesehen wird. Das heisst, dass das Thema vielleicht nicht angemessen ist“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 29)

„der dass das dann ethisch ein bisschen verwerflich ist oder viele Leute das dann als Beleidigung auffassen. Das ist das gleiche, wenn man gezielt E-Mails an gewisse Trainingsgruppen sendet, kann es natürlich immer vorkommen, dass diese das dann als beleidigend auffassen könnten. Man muss hier sehr gezielt oder sehr vorsichtig vorgehen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 29)

„should i elaborate okay maybe i just tell you the aspect so it's important first of all that the content is relatable okay for example we had a client in saudi arabia he looked at all the /. You know in saudi arabia most of the employees of course and they're arabs but actually most of them are indians or people um or black people from africa sometimes even and they wanted the avatars the people that are that appear in the courses to be to look like them to dress like them they didn't really relate to this uh tall blonde guy in a suit or this suit or this blonde girl in mini skirts and high heels this is not how people dress in a corporate environment in saudi arabia so this is first thing relate to the culture relate to the language also translate it to the language“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 38)

„And also there should be an adjustment to the industry if you're a person working in retail you like to read stories about security related to people working in a big store not people working in procurement department somewhere or some sales people that took us on airplanes the whole time related to me. So these are the most important thing but of course also to tailor the entire programs to the real challenges and the risks of the company so yeah but this doesn't really relate to the localization um yes and also gender is also important for being able to speak to women and men.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 38)

„So if you're using a good software that can understand what is the level of every user you can also adjust sending harder or easier phishing attack simulation. And also let's say more basic education or more like fun and short education that is just reminding you the things that you already know.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 42)

„Nobody can learn anything if you just start phishing campaign by doing the test nobody learns anything you want to do some education first and then doing a test it's like when the when you drive your car and you see sometimes signs saying oh be careful there are speed cameras ahead so people are more aware and they are in general driving more securely let's say“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 52)

„Ja, gute Frage. Ich denke, man sollte erstmal generisch ausrollen und generische Kampagnen gegenüber jedem, also jeder Zielgruppe.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 24)

„Aber ja, Ich bin auch der Meinung, dass man es gezielt machen sollte. Im Sinne von einfache Kampagnen, mittelschwere Kampagnen, schwere Kampagnen, um es mal irgendwo zu klassifizieren und zu schauen, okay, der Benutzer hat jetzt siebenmal die einfachen Kampagnen kapiert, dann bringt es kaum mehr was, ihm häufig einfache Kampagnen zukommen zu lassen“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 24)

„Wenn du gestern irgendein Geschäft getätigt hast, irgendwas bestellt hast im Internet oder auch außerhalb und heute kommt eine E-Mail dazu, die einfach im Kopf den Link herstellt, dann ist die Gefahr hoch. Ah ja, das ist ja trustworthy, ich klick's einfach an. Also die Wachsamkeit und Achtsamkeit, die ist dann einfach per se mal unten und das sind so Faktoren, die sollte man schon beachten und auch spezifisch austesten. Ebenso, ich sage jetzt mal, Finanzabteilung, die bekommen andere Mails am Tag als jemand in der IT, als Techniker. Auch das ist so ein Thema, wo man wirklich individuell drauf eingehen kann“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 24)

„Man sollte es generisch behalten, immer wieder, aber auch auf Zielgruppen eingehen“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 24)

„Zum Beispiel die Human Resources Leute, Unsere Personalabteilung, muss anders adressiert werden wie Dozierende oder Studierende oder“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 26)

„ich hab das eigentlich immer eher an der Funktion im Unternehmen festgemacht. Es wird relativ komplex, schnell also das relativ schnell komplex, wenn man wirklich auf alle diese Kriterien und zusätzlich noch auf die Funktion eingehen will und das berücksichtigen will und das hat auch eine technische Herausforderung, weil demographischen Background da ist normalerweise in keinem ICT System, das ich kenne hinterlegt. Also wenn wir jetzt, sagen ok, da kommt jemand ist gebürtiger Nigerianer oder so hat vielleicht einen anderen Bezug zu zu Phishing als jemand aus Norwegen, oder. Die Informationen liegen uns gar nicht vor, das heißt, wir können das praktisch gar nicht umsetzen.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 26)

„erhofft haben wir uns natürlich, dass das unsere Mitarbeitenden, wenn ein echtes Fishing reinkommt, dass sie da vorsichtiger agieren und vielleicht und wirklich zweimal schauen ist ist der Link wirklich echt ist der Absender echt und macht macht der Text der Mail überhaupt Sinn oder ruf ich lieber den Absender an und frag ihn, Ob die Mai legitim ist?“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 28)

„Man muss es teilweise sogar machen. Es gilt ja unterschiedliche Bedürfnisse in den Teams und dementsprechend, wenn man so Phishing Kampagnen fahren will, mit erfolgt, muss man sich

auch auf die Thematiken oder auf das Umfeld von dem User, muss man sich dann einlassen“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 20)

„Genau das, also im Endeffekt muss, sollten solche E-Mails, Phishing-Kampagnen abgestimmt sein, auf Job zumindest.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 21)

„Aber im Endeffekt, wenn man möchte einen hohen Effekt erzielen, ist es wahrscheinlich gut, wenn man eher auf die Rolle von der Person eingeht“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 23)

„Auf alle Fälle, weil ein Fallstor oder man spricht auch immer von human factor, das heißt ganz ein banales Phishing, das erkennt ein Normal-User im Regelfall, aber man muss heutzutage mit gezielten Angriffen rechnen und dann kommen eben sogenannte personalisierte Mails und die müsste man dann eben auch erkennen, darum ist der Fokus sehr wichtig“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 25)

„Man darf halt auch nicht zu primitiv werden, da kann man sich den Experte 6 unterstützen, weiles ist so, dass wir heute technisch so gute Abwehrmaßnahmen haben, dass sehr wenig Phishing eigentlich durchkommt und so ganz banale Sachen im Regelfall gar nicht mehr auftauchen und durch die Banalität dann eigentlich schon wieder der Verdacht bei Usern, ey das ist eventuell ein Test.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 27)

„ja, es gibt natürlich unterschiedliche Personenkreise, die unterschiedliche betroffen sind sei das Know How technisch vor dem Computer selbst, aber auch in ihrer Funktion also ich denke da an. Bereiche wie Personalabteilung, Finanzwesen, Geschäftsleitung. Bereiche, wo Personen Datenschutz ich sag mal Gesundheitswesen usw sicher gefährlich als nicht gefährlicher wo wo prädestiniert sind ,um gezielt angegriffen zu werden. Vergleichbar oder das Gegenteil dazu ist ich sage jetzt mal der Mitarbeiter draußen in der Produktion, der sein eher ERP System hat und die Aufträge ausliest und die Daten eingibt wenig mit sensiblen Daten zu tun hat und so weiter. Ich denke, da sollte sicher eine entsprechende Kategorisierung stattfinden, auch was Menge tief bei usw angeht vom Training selbst.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 18)

„Die haben aus meiner Perspektive müssen die noch mehr sensibilisiert werden oder extra sensibilisiert werden, sei das von Menge, aber auch von der Qualität der Trainings“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 24)

„Was inhaltlich angeht, kann man natürlich maßgeschneidert mit Stellenbewerbungen mit. Sie haben Ihre Rechnung noch nicht bezahlt. Sie haben eine Gutschrift erhalten. Mit solchen Geschichten kann man natürlich punktuell besser auf die auf die Mitarbeitenden zu umgehen, weil ich sag jetzt mal wenn der lageristen Maile bekommt. Sie haben Ihre Rechnung nicht bezahlt, dann interessiert ihn das vermutlich nicht, weil er nichts damit zu tun hat. Wenn das Mail aber jemand aus der Finanzabteilung eröffnet.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 24)

„Risiko, dass dann aus Angst vor Phishing-Mails auch wichtige Informationen gelöscht oder nicht konsumiert werden können, das wäre jetzt eigentlich eine Information im Intranet gewesen, die für jeden Mitarbeiter wichtig wäre“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 14)

„ch habe dann ein E-Mail gekriegt und da stand drauf, dass ich die Rechnung nicht bezahlt habe und ich muss das jetzt einer in Inkassofirma bezahlen, nicht mehr dem Hoster, sondern dieser Inkassofirma, weil der Hoster hat das, die ganze Mahntätigkeiten diesem in Inkassobüro übergeben. Und das Kritische war, dass der Betrag, den ich bezahlen muss, der war richtig. Das ist ja noch ein bisschen verwirrend, weil der Betrag ist ja individuell, je nachdem, ob du ein grosses,

kleines Mittelpaket hast, ist der Preis pro Monat unterschiedlich und ich hatte diesen Betrag war richtig und ich habe über "O-Scheibe" ich habe die Rechnung vergessen zu bezahlen und dann habe ich Antworten geklickt /. Ich habe nicht auf, ich bezahle sofort, auf den Button, ich bezahle sofort geklickt, sondern ich habe geantwortet und habe die Hostpoint, Info@Hostpoint das ist mein Hoster, dort als CC-Kopie mit reingenommen und habe gesagt, liebe Hostpoint und lieber inkassso, inkassogesellschaft, es tut mir leid, ich habe die Rechnung vergessen zu bezahlen, aber ich möchte die Mahngebühren nicht bezahlen. Die 10 Schweizer Franken-Mahngebühren, ich zahle heute gleich, aber könnt ihr mir bitte bestätigen, dass ich die Mahngebühren nicht bezahlen muss. Und dann hat die Hostpoint zurück reagiert, hey, passt auf, das ist eine in inkassobüro, nicht von uns. Also es war eigentlich Zufall, dass ich nicht reingefallen bin und wenn das reguliert wäre, dann könnte es sein, dass das Mail nicht zu mir gekommen wäre, ja, aber es hätte eben auch geschehen können, dass ich dann direkt bezahlt hätte“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 22)

„Ich also ganz der erste /. Ich glaube ja, mit der Ergänzung, dass der erste Teil, die erste Hälfte von einem Training, das ist wie überall, wenn du zum Sport gehst, wenn du zum Fussball gehst oder zu einer Sportart, die Grundregeln und die Grundmechaniken und die Grundfitness und die Bewegungsabläufe, die sind identisch bei allen Fussballspielern und schlussendlich wirds dann in der zweiten Phase wird es dann ein bisschen individueller.“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 26)

„Ja, gleichzeitig Chancen und Risiken, je nachdem, weil je personalisierter ich das mache, desto künstlicher werde ich die Klickrate erhöhen, dass die Leute reinfallen. Das kann irreführend sein, weil das wird dann sehr perfide“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 28)

Organisatorisch — Art und Aufbau einer Schulung — Intervall der Schulungen

„Sometimes the employees already know that, but the awareness course or the awareness the whole process reminds them of that, you know, sometimes you know how to do that, so like if I give you a test you will know how to answer it completely perfectly, you'll get 100 out of 100 percent in the score, but you when you're doing your everyday job you completely forgot about this topic, so sometimes this this course is active reminder and by the way for that sake it's important to also understand and good security awareness tools to that they know to tell between let's say the slow employees still need to learn and let's say the smat employees that they already know everything they just need to be reminded, now so“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 18)

„dass die Leute genervt werden, dass sie sagen, oh nein, das ist mir jetzt wirklich to much. Hört doch bitte mal auf damit. Ich habe es kapiert.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 29)

„Das ist einfach das Thema, diese wiederkehrende Durchführung von solchen Kampagnen und auch von den Trainings ist einfach wichtig, um einfach in den Köpfen wieder bewusst zu machen, oh ja, das kann uns böse treffen“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 29)

„Genau, auch die Frequenz ist so ein bisschen Thema, wenn man nur, ich sag jetz mal dreimal im Quartal, vielleicht ist es spannend, nicht nur einmal im Monat zu machen und der Endanwender weiß dann, oh ja, ich war jetzt einmal im Monat dran, jetzt bekomme ich keine Mail

mehr, dass es auch wirklich variiert, dass es dreimal in einem Monat sein kann und dann in den nächsten beiden nicht zum Beispiel. Also auch da muss man ein bisschen Flexibilität zeigen und einfach auf das Real-World-Szenario eingehen“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 31)

„Ja, also allen voran ist das jetzt auch nach der OptiPhish Kampagne oder 288000 Mails über ein Jahr an die Hochschulangehörigen zuzusenden. Es war zuviel, das hat auch für Aggressionen geseogt bei manchen Personen und genau. Also das ist dann kontraproduktiv, oder wenn man wirklich /. Wenn plötzlich die. Die Adressaten vom Phishing Awareness Training einfach nur noch sauer sind auf Security und nichts mehr wissen wollen von Security, dann haben wir dann plötzlich ein Problem“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 12)

„Also jetzt machen wir mal eine Woche lang Phishing Awareness, sondern es muss kontinuierlich passieren, dass ist etwas, was wir deutlich feststellen. Die Leute die vergessen das wieder und zwar schneller als man denkt, oder. Innerhalb nach ein paar Wochen ist das, hat das Training keine keine Wirkung mehr, wirklich kontinuierlich bespielen wir haben das auch in der Vergangenheit schon gemacht, ist ja schon ein paar Jahre her mit Plakaten in den Departementen mit Aufstellern in den Eingangsbereichen“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 34)

„Auch was das Problem sein ist, je nachdem wie man Kampagnen aufzieht, kann eine Kampagne, die zu viel gefahren wird, wie könnten abstoßend wirken, sodass man den User eigentlich veregrault und mit der Zeit der Abstumpft, also es muss ein gesundes Mittelmaß gefunden werden“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 6)

„Die haben zum Beispiel, du musst pro Monat 20 oder 30 Trainings durchlaufen und im Endeffekt hat es keinen positiven Effekt. Weil Maximum klicken die Leute einfach durch.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 37)

„Und daher ja.Ich würde Awareness Training als wichtiger permanent repetieren Bestandteil einer Ausbildung im Unternehmen bezeichne“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 42)

„Ja, sehr viel, mit der /. Also das Wichtigste aus meiner Sicht ist, dass das eben nicht nur einmal gemacht wird, sondern dass das kontinuierlich gemacht wird“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 10)

„wenn man zu viele Phishing-Awareness-Kampagnen durchführt, dann werden die entsprechenden Kollegen auch müde und dann wird einfach wie alle wenn es zu repetitiv wird, zu wiederholend, zu identisch, dann verliert es den Nutzen, also es muss schon spezifisch sein und die Menge muss gut überlegt sein“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 14)

Organisatorisch — Normen, Richtlinien und kulturelle Aspekte

„Also meiner Meinung nach ist Phishing-Awareness ein Teil der Cybersicherheitskultur oder der Sicherheitskultur allgemein in den Unternehme“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 37)

„In solchem Rahmen macht es dann nicht Sinn, das als große Rolle zu betrachten. Es ist natürlich ein anderes Thema bei großen Firmen, bei sehr großen Firmen. Bei denen ist es für mich schon ein bisschen ein Muss, dass die Phishing-Awareness oder die allgemeine Schulung gegen

Phishing einen festen Bestandteil ihrer Sicherheitskultur ansehen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 37)

„the security awareness program is meant to design the security is meant to design the security culture and the security awareness is based on what is the current state of your security culture and what /. How do you want to change.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 56)

„Ja, ich sag mal so, Phishing Awareness Training kann natürlich zum Aufbau einer solchen Kultur beitragen“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 37)

„Ich würde gerne noch bei den organisatorischen Aspekten noch kurz ergänzen. Aus meiner Sicht muss so ein Phishing Awareness Training muss an die Organisation und die Organisationskultur auch angelehnt sein“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 14)

„Ne ich glaub für mich gehört das zusammen oder das ist es "geht Hand in Hand"“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 40)

„ch finde wenn man eine Cyber sicherheitskultur entwickelt aufbauen möchte in einem Unternehmen dann ja, dann ist Phishing Awareness Training, kann man dann auch als /. Also das kann man als Tool mit verwenden dafür oder. Ich was ich an Phishing Awareness Training da noch sehr gut finde, ist es ist ein greifbares Thema, also bis zu einem gewissen Grad. Aber die Leute können sich was drunter vorstellen, jeder hatte mal irgendwie eine Phishing Mail und das kann wieder helfen als Beispiele, so eine Cybersicherheitskultur dann auch zu schaffen“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 40)

„Also wenn die Cybersicherheitskultur gut entwickelt ist, gehen die Leute viel offener mit solchen Phishing Awareness Trainings um. Nämlich ein Risiko was auch besteht, ist je nachdem, wie die Kultur auch ausgeprägt ist, ist das Person sich überwacht fühlen oder reingelegt fühlen von denjenigen, die dieses Awareness Training machen.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 40)

„a, also das Phishing Training steht hinter der Kultur. Das heißt, wenn die Kultur nicht stimmt, wirst du auch mit der Awareness Kampagne Phishing Probleme haben. Also es ist sehr wichtig, dass die Gesamtkultur stimmt und die User der Kampagne positiv eigentlich schon mal entgegenwirken. Also wenn man von vornherein ein negatives Bild hat, wird man auch mit dem Phishing anschließend kein Erfolg haben“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 52)

„ich kann mir gut vorstellen, dass Phishing Awareness trotz allem helfen kann, auch wenn die Cybersecurity Kultur nicht so hoch ist. Also ich würde jetzt nicht behaupten, dass wir eine riesige Security Kultur haben in der ZHAW. Und dennoch habe ich das Gefühl, du kannst etwas damit erreichen. Die Frage ist natürlich, wie viel? Ich persönlich sage, Kultur ist wahrscheinlich wichtiger als Phishing Awareness, aber schwierig zu sagen. Ich glaube, es geht schon ein bisschen Hand in Hand, auch wenn es ein Subpunkt von Kultur ist.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 53)

„Also ich denke, das eine schließt das andere nicht aus, also eine eine Cybersicherheitskultur im Unternehmen finde ich äußerst wichtig und notwendig, sofern sie auch entsprechend gelebt wird“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 32)

„Es muss passieren wie gesagt, der Mitarbeiter muss sich bewusst werden, dass er auch für die Sicherheit verantwortlich ist. Nicht nur der IT-Leiter ist für die Sicherheit verantwortlich, sondern jeder Anwender ist für die Sicherheit verantwortlich.“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 32)

Organisatorisch — Ethische Aspekte

„wenn man auf gewisse Zielgruppen E-Mails erstellt und diese dann sendet, dann kann es natürlich sein, dass das auch ethisch ein bisschen ein Problem ist Insofern, dass man vielleicht ein Thema aufgreift, das dann für diese Usergruppe wie sagt man /. Als unzulässiges Training angesehen wird. Das heisst, dass das Thema vielleicht nicht angemessen ist“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 29)

„Oder dass das dann ethisch ein bisschen verwerflich ist oder viele Leute das dann als Beleidigung auffassen. Das ist das gleiche, wenn man gezielt E-Mails an gewisse Trainingsgruppen sendet, kann es natürlich immer vorkommen, dass diese das dann als beleidigend auffassen könnten. Man muss hier sehr gezielt oder sehr vorsichtig vorgehen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 29)

„Grundsätzlich kann man sagen, dass Phishing-Awareness klar eine Grauzone im ethischen Bereich ist, weil die meisten Leute, die Phishing-Awareness ausgesetzt werden, haben nicht die Möglichkeit, das zu wählen. Gerade in Firmen oder Unternehmen wird dann einfach von der IT bestimmt, dass so ein Training durchgeführt wird. Man hat oftmals keine Möglichkeit, sich dafür an- oder abzumelden“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 43)

„Yes several um. Okay first one don't make your goings feel stupid more than than you have to okay. Sometimes it's very fun especially for security people that they like to hack things to make like attacks that are almost insulting you know“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 66)

„This is all in the category of promising you like a false gift other thing that are i'm not sure if it's yeah it is ethical slash legal already um when many of the Phishing attack emails are pretending to be other companies for“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 66)

„ow when it comes to the education itself some Phishing stories they are a little bit /. Not so politically correct right i mean like they're using race they're using sexuality they're using sexism a lot of let's say fun stuff like that. So because some of them are based on real stories that happen like that but it doesn't fit in the corporate setting“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 66)

„so for the ethical point of view there is also how ethical it is from the /. There is the old data collection aspect of the fishing training simulation there is data collection things that you write in tests also your grades and also /. Yeah it's all this kind of stuff some companies can use them not in a nice way hopefully they don't but i mean this is also theoretically can be one aspect of it.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 66)

„o i mean there are several aspects right so let's say over the phishing attacks don't mess up don't insult don't be sexist don't do don't use um don't hurt other companies or other businesses.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 101)

„nd man darf einem Mitarbeiter, also den Mitarbeitern nicht das Gefühl geben, man will sie hinter das Licht führen oder sie bloß stellen. Das darf nie der Fall sein. Das muss man ganz klar vermitteln. Ansonsten, wie gesagt, spreche ich mich für die Mischform aus“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 27)

„Man muss sich bewusst machen, wie kommuniziere ich dort, dass man wirklich eine Sprache findet, die von jedem verstanden wird, aber für keinen despektierlich ist. Das ist das eine. Und

ja was noch zu beachten ist, dass man echt wirklich überlegt bei jeder Kampagne, die man macht, komme ich da mit diesem Thema einem nicht zu nah.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 39)

„Ja also. Für mich ist das wirklich wieder das Thema Fingerspitzengefühl, oder. Organisationskultur berücksichtigen aber auch natürlich generell, wo bewegen wir uns? Welche kulturellen Themen gilt es zu berücksichtigen? Und dann natürlich ja das das Übliche /. Ich mein müssen Minderheiten respektieren und ja, auch Andersdenkende respektieren und /. Aber es ist jetzt nicht wir haben jetzt keinen Leitfaden ethischen Leitfaden für Phishing Awareness oder so erstellt, sondern das ist eigentlich "common sense" und wir kennen unser kulturelles Umfeld, oder. Und das müssen wir entsprechend auch leben“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 42)

„Ja, ethisch ist immer sehr schwierig. Also ja /. Also es gibt Themen, die lässt man momentan besser ruhen, da klopft man nicht drauf rum, da macht man den User vielleicht, der zweifelt vielleicht fast. Also es muss immer die richtige Notwendigkeit, die richtige Balance gefunden werden zwischen dem ganzen. Also man kann wie zur Phishing-Kampagne die Leute schon demotivieren, und zwar gewaltig“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 56)

„Ja, also ich sehe erst dann ethische Bedenken, wenn zum Beispiel hingeht, sagst du okay, ich mache eine Phishing Kampagne, du kannst hier dein Username und Passwort eingeben, Username und Passwort eingegeben, Username und Passwort wird gespeichert. Dann habe ich langsam wir ethische Bedenken. Aber sonst bin ich jetzt nicht der, der sagt, dass ich jetzt da wirklich ethische Aspekte sehe. Also ich sehe es erst dann, wenn Daten generiert werden können, die problematisch werden für die Person, die gefischt wird“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 57)

„Es soll ein Training sein und nicht igendwie eine moralische Demoralisierung soll man natürlich unterbinden. Man muss ja natürlich auch gefasst sein, wenn es so extreme also externe Einflüsse sind, dass man vielleicht auch einen persönlich damit dann verletzen könnte. Das passiert einem beim DHL wahrscheinlich weniger“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 103)

„Ja, also ich denke die üblichen ethischen Grundsätze, wobei Ethik auch auch ein sehr flexibler Begriff ist, sollten sicher eingehalten werden, also ich denke da wenn ich ein ethische Fragen denke, dann dann kommen ja sicher Sachen wie Religion mein /. Oder ich sag mal orientierung ich sage mal politische Orientierung Ethnie usw. solche Dinge sollten vermieden werden. Beziehungsweise einfach verallgemeinert werden, damit da keine Ethische Konflikte entstehen können“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 34)

„Andererseits ethische Konflikte können aber auch ich sage jetzt mal entstehen, wenn ich natürlich ne Phishing Training mache und ich nutze immer immer und immer wieder Microsoft als Beispiel. Könnte im weitesten Sinne natürlich auch ethisch ausgelegt werden, dass man Microsoft immer so als "Buhmann" darstellen möchte, was definitiv natürlich nicht so gemeint ist“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 34)

„Und das andere ist natürlich in der ganzen /. Wir leben heute in einer Welt, in der man sehr vorsichtig mit Kampagnen in der Wortwahl und in der Terminologie und Themen wie Diversity sind heute sehr zentral. Und das kann auch ein bisschen streng sein zum Teil und ich glaube, da ist es einfach Vorsicht zu geboten, eventuell hilft es da, dass man auch da mit einem Experten sich unterhält. Da gibt es dann schon auch "Fettnäpfchen", wenn man dann über irgendwelche Randgruppen oder irgendwelchen Themen irgendeine Plattform anspricht, die zum Shitstorm werden kann. Also es ist immer eine Gefahr, man will nicht zu spezifisch werden, aber auch

trotzdem ein bisschen Dramatik auslösen“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 36)

„Ist die Kommunikationswelt oder unsere Welt hat sich da ein bisschen auch zum Guten weiterentwickelt, dass man ein bisschen vorsichtig ist, welche Begriffe darf man anwenden und welche nicht, was ist rassistisch was ist /. Was schliesst gewisse Themen aus, aber eben unter Umständen auch ein bisschen streng“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 36)

Organisatorisch — Aspekte der internen Rechtfertigung

„Also was aus technischer Sicht sicherlich auch oftmals schief gehen kann, ist natürlich wenn man Statistiken erhebt. Also wenn man eigentlich versucht herauszufinden, wie gut das Training funktioniert. Da gibt es natürlich unterschiedliche Ansätze bei den Produkten, wie sie diese Zahlen erheben und wir haben zumindest festgestellt, dass es hier auch ein großes Fehlerpotenzial vorhanden ist, Das heißt, dass wenn man diese Tools nicht wirklich überprüft oder testet, wie schon angesprochen Dann kann es natürlich sein, dass man auch falsche Zahlen erhebt also das ist noch ein wichtiger Punkt, den man sich auf der technischen Seite zumindest immer auch vor Augen haben sollte, dass man auch Fehler machen kann bei der Datenerhebung oder“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 23)

„Grundsätzlich, das Erfassen von Klickraten ist eigentlich ein Standard-Use-Case. Das macht man eigentlich, um eine Art Baseline zu haben, wie viele Leute haben diese Phishing-Emails angeklickt. Jetzt ist natürlich immer die Frage, wie man diese Klickraten verwendet.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 45)

„Verwendet man das jetzt so im Stil von, wenn jemand klickt, dann wurde er gephisht oder sagt man einfach, jemand hat geklickt, aber er hat nicht sein Passwort eingeben. Das sind zwei verschiedene Fälle. Und je nachdem, was man für ein Security-Risiko hat, ist das dann ein entscheidender oder. Weil die meisten Leute sagen eigentlich, ein Klick genügt, um gehackt zu werden.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 45)

„as andere ist natürlich, wenn man diese Klickraten als hartes Measurement verwendet für Business-Cases, also für organisatorische Entscheidungen, dann kann es natürlich sein, dass, wie schon angesprochen, diese Klickraten vielleicht nicht so genau /. Oder so genau erfasst wurden /. oder die Daten so genau erhoben werden konnten.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 45)

„Wir haben zum Beispiel während der Studie festgestellt, dass gewisse Anti-Viren oder auch gewisse Funktionalitäten von verschiedenen Email-Client, wie zum Beispiel Microsoft Preview, einen Klick auslösen können. Das heißt zum Beispiel, wenn man jetzt ein Mail im Outlook bekommen hat und Microsoft dann ein Preview dieses Link lädt, meistens so einen kleinen Screenshot der Webseite, dann hat das /. Oder hat unser System das bereits als einen Klick gewertet. Das kann natürlich dann relativ gravierende Folgen haben, wenn man dann solche Fehler nicht entdeckt oder davon ausgeht, dass diese User wirklich geklickt haben, obwohl sie eigentlich gar nicht geklickt haben zuvor oder“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 45)

„Das ist ein bisschen so schwierig einzuschätzen. Es kommt immer darauf an, wie man diese Klickraten verwendet, aber generell würde ich sagen, mit Vorsicht zu genießen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 45)

„First of all click rate has no meaning when you don't know how difficult the attack is if the click rate of a person is very low it doesn't mean that he's protected against phishing it just means that now it's the time to sending harder attacks that's the only thing it says.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 70)

„Man darf nicht alles für "bare Münzen nehmen", was dort die Datenbasis dann hergibt.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 37)

„Man muss also wirklich die Daten, die man nachher rauszieht, hinterfragen. Kann das sein? Passt das? Ja, deshalb eine gewisse Datenmenge für eine Analyse ist schon mal ein Punkt.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 43)

„Jemand hat auf den Phishing Link geklickt und ist darauf reingefallen und denkt nachher, irgendwas war doch da komisch. Komm, ich ruf's noch mal auf und guck's mir noch mal an. Das ist so eine Möglichkeit. Die andere Möglichkeit ist eben der technisch versierte, der sagt, du, ich habe das angeklickt, mir ist das bewusst, jetzt wollte ich mir noch ein bisschen Analyse machen, mach mir noch einen Spaß, schau mir noch ein bisschen rum und ruf das halt mehrfach auf. Oder jemand, der sagt, er zeigt zum Arbeitskollegen, guck mal hier, das da habe ich angeklickt, was hältst du davon? Er will es halt noch mal zeigen.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 43)

„Das Problem ist die Vergleichbarkeit. Wenn wir jetzt eine Phishing Awareness Kampagne durchführen und dann, sagen wir mal, über ein paar Monate und wir messen die Klickrate jetzt userspezifisch, oder auch Benutzergruppen spezifisch, Monat für Monat und vergleichen die. Dann werden wir vermutlich sehen, die Raten sinken. Aber wie eben gesagt, haben wir vorher fünf einfache Kampagnen gefahren und jetzt waren wir fünf schwere. Das heißt, die Vergleichbarkeit, die müsste eigentlich immer gegeben sein. Das ist schwierig. Ich denke, was man einfach machen muss, ist die Wiederholung. Also mal aussetzende Zeit lang und es dann wieder machen, um wieder das Bewusstsein zu schaffen, oh ja, da ist hier noch irgendwas“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 45)

„Genau, es ist einfach, wie ich sage mal, bewusst und auch unbewusst manipulierbar. Die Vergleichbarkeit hierherzustellen ist extrem schwer“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 49)

„Ich find Klickraten problematisch, weil ein Phishing Dienstleister, also eine Security Firma, war bei uns und hat gesagt: Problemlos, Sie können Phishing Simulationen fahren bei uns, wo 50% der der Adressaten darauf klicken werden. Jetzt kommt das aber. Es ist massiv abhängig davon, wie anspruchsvoll man da die Phishing Simulation auch macht. Also ich kann die sehr low Level machen, wo praktisch niemand hereinfällt, weil das so offensichtlich ist und ich kann die extrem anspruchsvoll machen, wo dann fast jeder drauf hereinfällt oder.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 44)

„t aber in der Praxis extrem schwer und wie gesagt, mann läuft dann das Risiko und dass, die Leute einfach nur aggressiv werden, weil man sie so viel bespielt mit Phishing Simulation. Klickraten alleine sind mit Vorsicht zu geniessen würde ich sagen. Außer man verwendet vielleicht auch identische“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 44)

„Ja, also. Wir haben das natürlich auch gemacht und das ist tatsächlich, dass worauf die, worauf das Management schaut, oder.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 46)

„Hey die Zahlen sind mit Vorsicht zu genießen und die Zahlen alleine sagen nichts darüber aus wie dringlich oder nicht dringlich jetzt tatsächlich eine Phishing Awareness Kampagne sein wird?“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 46)

„man muss es wirklich zum Sensibilisieren nutzen und nicht nur zum Management irgendwelche Zahlen abgeben. Es ist nämlich ganz einfach aufzubauen, dass das Management mit dem zweiten Training anschliessend zufrieden ist, indem man den Level dementsprechend anzieht. Zahlen zu produzieren ist mit Phishing was ganz was einfaches, die sind aber verfälscht. Das ist das große Problem meiner Meinung nach an dem Ganze“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 6)

„Eigentlich ist das genau das. Also Klickrate selber, sagen wir es mal so, wenn man verantwortungsbewusst mit umgeht, kann man einen Trend erkennen, aber generell ist kein Verlass drauf und ich halte auch nicht sehr viel davon. Mir ist es sehr wichtig, dass man die Leute sensibilisiert.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 60)

„Das Wichtigste ist eigentlich, dass das Management keine Ansprüche an das hat. Also dass du eigentlich ein Management hast, die das anordnen, die wissen, dass es egal ist. Weil Fakt ist, "Jo" du kanst jedem /. Du kannst jede Person dazukriegen, drauf zu drücken und du kannst auch solche Sachen /. Ich meine Daten sind immer extrem schwierig zu interpretieren und ich glaube, es ist wichtig, dass das Management weiss, dass die Klickkarten zum Beispiel nicht unbedingt ein guter Indikator sind“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 61)

„Es gibt auch sehr viele Klicks, die sind bewusst ausgelöst von User, nur weil sie interessiert, wie es weitergeht. Andere nur, um uns zu ärgern. Also von dem her kann (unv., #00:29:21-2#) man die Klickkarten nicht voll.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 62)

„Es ist halt nicht so zuverlässig“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 63)

„Was zeigt jetzt auf diese explizite Phishing Kampagne wurden so und soviel Prozent geklickt oder auch nicht, unabhängig davon eben sie sagt nichts aus über die Mitarbeitenden oder den Inhalt des Phishings, was ausschlaggebend sein kann.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 36)

„Von daher würde ich die Klickrate selbst immer mit Vorsicht genießen, immer mit Rand Daten abgleichen“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 36)

„Nein, das Problematiken sehe ich nicht. Dass diese Daten oder diese Zahlen als Verkaufsargument genutzt werden, ist auch nachvollziehbar, eben weil es ist halt messbar, mann, sieht etwas oder das Management sieht etwas aber problematisch seh ich das insofern nicht, sofern man die Daten, die rauskommen entsprechend in Kontext stellt und auch entsprechend interpretiert“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 38)

„die reine Klickrate an und für sich ohne Kontext sehe ich als problematisch an, eben weil sie kann in beide Richtungen ausschlagen. Sie sagt nichts über das Verhalten aus der Mitarbeiter“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 40)

„wir hatten bei der Swisscom, kann ich mich erinnern, da hatten wir so eine Internetkampagne und da ging es um Swisscom TV und als Swisscom Mitarbeiter hattest du die Chance, bei Swisscom TV sogenannte Friendly Tester zu sein. Das heißt, du hattest dann immer die neueste Swisscom TV Box gekriegt, die neuesten Software Updates, wenn es irgendwelche Verbesserungen gibt. Dafür musstest du aber an einem Programm teilnehmen, um Feedback zu geben. Du musstest zuhause dieses Swisscom TV Box versuchen und testen und "Tatüttata" und dann Feedbacks ausfüllen. Und an einem Tag kam ein E-Mail und das besagte dann, dass wir im Swisscom /. Dear Friendly TV Tester, es gibt neu die Funktion, dass wir Netflix direkt im Swisscom TV integrieren, damit du nicht mehr da die Fernbedienung wechseln und solche Sachen machen musst. Wäre das für dich einen Nutzen oder wäre das kein Nutzen? Bitte stimme

hier ab. Wenn du so spezifische Fragen stellst in einer Phishing Kampagne, dann gehen die Klickraten hoch. Das waren dann 70-80% von allen Mitarbeitern haben geklickt.Jetzt ist die Frage, ist das wirklich repräsentativ? Die 80% Klickrate, ist das repräsentativ oder nicht? Und das ist das Risiko, dass du bei zu spezifischen, exakten, irreführenden Fragen eine zu dramatische Sicht kriegs“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 28)

Technologisch

Technologisch — Systemlösungen

„es gibt natürlich sehr viele verschiedene Produkte, die Phishing Awareness anbieten Aber nicht jedes Produkt ist gleich ausgereift oder hat die gleiche Funktionalität und daher ist es natürlich wichtig, auf technischer Seite ein Produkt zu haben, bei dem man sich auch wohlfühlt und mit dem man umgehen kann“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 19)

„Weil ein falsch konfiguriertes Produkt kann natürlich dann im schlimmsten Fall dazu führen, dass man E-Mails an Personen versendet, die diese E-Mails dann vielleicht nicht erhalten sollten. Oder dass die E-Mails gar nicht bei den End-Usern oder den geschulten oder zu schulenden Personen ankommen. Also man kann natürlich auch auf der technischen Ebene relativ viel falsch machen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 19)

„Also was aus technischer Sicht sicherlich auch oftmals schief gehen kann, ist natürlich wenn man Statistiken erhebt. Also wenn man eigentlich versucht herauszufinden, wie gut das Training funktioniert. Da gibt es natürlich unterschiedliche Ansätze bei den Produkten, wie sie diese Zahlen erheben und wir haben zumindest festgestellt, dass es hier auch ein großes Fehlerpotenzial vorhanden ist, Das heißt, dass wenn man diese Tools nicht wirklich überprüft oder testet, wie schon angesprochen Dann kann es natürlich sein, dass man auch falsche Zahlen erhebt also das ist noch ein wichtiger Punkt, den man sich auf der technischen Seite zumindest immer auch vor Augen haben sollte, dass man auch Fehler machen kann bei der Datenerhebung oder“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 23)

„SaaS-Lösungen können auch manchmal kostengünstiger sein als eine On-Premise-Lösung, die man selbst hosten, betreiben, updaten, konfigurieren muss.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 53)

„you have when you're buying software advantage main advantage is that many solutions okay not many but a lot let's say you have many (unv., #00:19:22-5#) many solutions they also give you the option to install a phishing reporting button so if you /. So if the employee sees an email that he suspects is a phishing email he can press it and then it's reported to the security team and as part of the training they you teach the employee to use it and you can use it with the security operation center to build the playbook to handle this kind alerts thats the advantage“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 22)

„Aber wichtig ist, dass die Endbenutzer Erfahrung einfach ist. Es muss wirklich aus meiner Sicht ein Portal sein, wo alles zusammenläuft. Es darf keine Hürden haben, sich dort kompliziert anzumelden. Ja, dann kommt einfach der Faktor, ja jetzt habe ich keine Zeit dazu, ich habe andere Aufgaben zu erledigen. Muss also erinnert werden, bitte macht doch noch so ein Training. Und wichtig ist einfach, dass man auch Rückmeldungen für die Durchführenden gibt“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 29)

„Das Ganze als SaaS zu beziehen, ist vielleicht nicht falsch, aber man darf nicht den Fehlglauben dann annehmen. Im Unternehmen hat man keine Arbeit mehr, weil du hast ja in den Fragen vorher es auch rausgekitzelt ist.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 71)

Technologisch — Technische Abwehrmassnahmen

„Diese Chancen sind eigentlich relativ klar. Man will ja eigentlich möglichst die E-Mails an einen End-User bringen. Das heisst, man passt dieses SPAM-Filter an oder macht Whitelisting, damit diese E-Mails wirklich auch gesehen werden“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 49)

„Das Risiko ist natürlich, wenn man dieses Whitelisting oder diese SPAM-Filter falsch anpasst oder so anpasst, dass es eventuell sogar zu einer echten Attacke während der Phishinge kommen könnte, ist das Risiko dann erheblich oder relativ groß, dass die Leute diese E-Mails auch sehen und eventuell auf ein echtes Phishing reinfallen. Das kann man im Normalfall technisch aber relativ einfach minimieren, indem man einfach ein internes Whitelisting macht. Das heisst, man tut eigentlich nicht den Absender Whitelisten, sondern man sagt, ein E-Mail von diesem, speziell dem Server, der dann der meisten intern ist, wird gewhitelistet, was dann das Risiko eigentlich minimiert.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 49)

„Und das andere ist natürlich, wie du gesagt hast, wenn dann Whitelistung betrieben wird und dieser Server freigeschaltet wird, kann es sein, dass man das Whitelistung falsch macht und auch andere Dienste freigeschaltet, die man gar nicht freigeschalten will. Da muss man natürlich das Testing eigentlich wieder in den Vordergrund stellen und auch schauen, ob das wirklich so funktioniert, wie man sich das vorgestellt oder wie das konfiguriert wurde oder.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 51)

„it but this is also something that theoretically can happen um and if some malicious actor is taking over this server that is doing this fishing training theoretically can launch real attacks on your employees because it is completely whitelisted.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 22)

„yeah i mean i think i told you in the beginning like you're just opening an attack vector theoretically you're /. What you're doing you're taking a server that is usually outside and you're trusting by whitelisting access to it. So you need to be, to make sure that it's as secure as any other server you keep this kind of access“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 76)

„. Whitelisting und dann auch aufpassen, baue ich mir nicht irgendwo noch eine Hintertür jetzt da ein, das ist nicht so ganz ohne“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 51)

„Also nicht, dass man dann jetzt irgendwas tut und sagt, ja alles, was über den Kanal geht, interessiert uns nicht. Das ist jetzt Phishing, wenn man da einen Transport Mail oder so eingerichtet hat. Nein, auch das sollte man bitte monitorieren, weil Fehlkonfiguration ist nun mal einer der häufigsten Faktoren für einen Angreifer“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 51)

„teilweise vielleicht auch noch sichtbar für die Benutzenden, dann hat man kein echtes Szenario mehr und beeinflusst dann auch wieder Klickraten“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 48)

„Also ich finde das problematisch. Chancen /. Chancen hab ich jetzt /. Chancen sehe ich jetzt irgendwie nicht ich sehe mehr Risiken.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 48)

„Also ich finde es natürlich wichtig, dass man die Ausnahmen so definiert, dass nicht versehentlich ein echter Angreiffer dann mit dieser Ausnahme was anfangen könnte. Also wenn wir jetzt zum Beispiel,"Jo" ich weiß, Firma X, die verwenden CoFans und dementsprechend weiß ich, welche E-Mail-Adressen Whitelisted sind bei denen. Weil da gibt es eine Liste, ich habe diese Liste, "bueno". Aber wenn du einigermaßen schlau bist, dann weißt du, wie man ein Whitelisting macht. Also es funktioniert nur für, wenn CoFans angreifen und nicht jemand anderes mit der gleichen E-Mail-Adresse“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 66)

„Genau, dass du halt eben genau dennoch das Soofing-Filter aktiv lässt, dass du sagst, jawohl, du darfst mit dieser E-Mail-Adresse kommt durch alles durch. Aber nur wenn SPF Records läuft, wenn DMARC läuft, wenn der "Usual"“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 68)

„relativ aufwendig ist die ganzen Systeme entsprechend zu konfigurieren, damit die Phishing Trainings auch dann beim and User ankommen und nicht durch vorgelagerte Systeme blockiert oder gefiltert werden“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 10)

„bedingt zwar einen gewissen Aufwand, den man betreiben muss, aber ja natürlich damit eben diese Trainings beim and Enduser ankommen sind Spamfilter manipuliert worden, wurden eben Whitelistings auf DNS oder auf IP basis erstellt“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 44)

„Und diese diese Freischaltungen können natürlich insofern missbraucht werden, wenn ich sag jetzt mal Domain Spoofing oder Mails Spoofing einfach wenn mit /. Oder wenn Außenstehende das merken, wissen unter Umständen, dass da solche Tools im Einsatz sind und wenn sie wissen was für Tools, dann können Sie sich auch etwa "zusammenschustern", welche Maßnahmen wurden umgangen und können diese dann die ihre eigentlichen bösartigen Phishings so manipulieren. Wenn Sie ein gezielter Angriff machen wollen das sind natürlich über ich sag mal eine gefaktes Mail Adresse oder Mail Domäne reinkommen oder sich als IP ausgeben, diese nicht sind und so weiter, ja also da bestehen definitiv gewisse Risiken und gefahren sind aber ich sag jetzt mal überschaubar man kennt sie und wenn man das mit der nötigen Sorgfalt und nicht ich sag jetzt mal in die Tageszeitung schreibt, mit welchen Tools, dass wir arbeiten sind die Chancen relativ klein. Sie sind nicht bei 0 aber sie sind relativ klei“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 44)

Technologisch — Vertrauen in die Technik

„a, es ist definitiv ein Problem. Man muss realistisch sagen, dass wir heute einen Großteil der Phishing-Mails rausfiltern können. Wenn man das statistikmäßig anschaut, sind das über 99 Prozent. Das Problem ist eben, wie bei den vielen Dingen, es kommen halt immer noch Phishing-Mails durch. Es ist nicht so, als ob Phishing gelöst wäre durch die technischen Maßnahmen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 55)

„. Und ich denke schon, dass man hier auch ein bisschen das Problem hat, dass wenn die Leute nicht oder nie damit konfrontiert sind, dass sie dann eher anfällig sind für Phishing-Mails. Und

das macht das Phishing-Awareness-Training eigentlich umso effektiver, einfach ab und zu wieder mal die Leute daran zu erinnern, dass es eben doch auch mal sein kann, dass ein Phishing-Mail durchkommt.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 55)

„Another thing it can also a security program done wrong can create like any kind of security measure that is done wrong can give a false sense of security that's why“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 20)

„So if you teach if you teach people exactly where they are secure and where they are not and this is also very very important.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 78)

„Und deshalb die letzte Instanz ist immer der vor Monitor. Und nein, die technischen Maßnahmen, klar, die versucht man so weit wie möglich nach vorne zu treiben, ohne massiv False positives zu erzeugen, aber das ist keine abschließende Sicherheit.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 53)

„Ja, ich ich glaube wirklich, dass das technische Sicherheitsmaßnahmen für falsches Vertrauen sorgen. Ich hör das auch regelmäßig, oder das. Ich, weise aber trotzdem auch immer wieder darauf hin, dass die, also wenn ich Vorträge halte, auch zu dem Thema das technische Sicherheitsmaßnahmen alleine eben nicht ausreichend sind.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 50)

„Wir hatten in der Vergangenheit eine Auswertung gemacht und zwar bekommen wir in der ZAHW pro Monat etwa 4'000'000 Emails aus dem Internet zugestellt. Von den 4'000'000 werden mehr als 3'000'000 automatisch herausgefiltert. Also das sind Mails, die sind ganz offensichtlich als Phishing erkannt. Die haben irgendwie verseuchten Email Anhang oder sind irgendwie anders als schadhaft eingestuft, die werden wir werden grundsätzlich schon herausgefiltert und dann bei denen bei der Millionen oder knappen Millionen, die wir zu stellen in die Postfächer da ist natürlich immer mal wieder auch gut gemachtes Fishing dabei oder das kann durchrutschen ja“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 50)

„Es ist definitiv so, dass falsche Sicherheit vermittelt wird, weil wir technisch sehr gut aufgestellt sind und technisch werden wir immer besser. Das ist ja auch das Problem mit unserer Phishing Kampagne, wenn das durchgeht, dann "riechen sie schon offt den Braten", weil wieso kommt das jetzt durch. Nichtsdestotrotz ist es umso wichtiger dann eben den sogenannten Human Factor zu stabilisieren oder zu stärken, damit er dann auch sensibilisiert wird, wenn mal sowas durchkommt, dass er das bewerten kann und er dann, was dann wieder Aufgabe von der Phishing Kampagne ist, so ein Mail, wenn er unsicher ist, auf den Button, wo er gelernt hat, zu drücken, da draufklickt und uns das zur Analyse kann schicken“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 70)

„Ja, also ich sehe das schon auch so. Ja /. Ja ja nein es ist halt so, je weniger du damit konfrontiert bist, desto weniger /. Also desto weniger gehst du davon aus, dass es ein Problem darstellen könnte“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 71)

„Ja, ich denke, das ist sicher ein Fakt, der gegeben ist also das soll man, muss man den Mitarbeitern auch nicht teilen und sie das kann man gut in die Schulung einbinden.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 46)

„Vergleichbar vielleicht mit den mit den neueren Automobilen, die mit selbstfahrenden Systemen usw auch dort heißt es immer wieder, dass das Fahrzeug kann vieles spurassistenten, kollisionswarner und und und aber der Mensch als letzte Instanz muss immer Herr der Lage sein. Das das verhaltet sich am Computer genauso also es hilft, aber ich bin schlussendlich immer noch das letzte Glied, der den Klick macht oder eben nicht.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 46)

Technologisch — Technische Warnhinweise

„Das Problem ist natürlich auch Hinweisen wie implementiert man das technisch und wie oft werden diese Warnhinweise angezeigt. Es gab Studien zu diesem Thema. Man hat sich auch in der Wissenschaft damit und in dieser Thematik befasst und es hat sich eigentlich gezeigt, dass diese Warnhinweise nicht viel Security bringen. Die meisten Leute gewöhnen sich nach einer gewissen Zeit an diese Warnhinweise und ignorieren sie dann.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 59)

„Weil das ist so ein wenig das gleiche Problem, das man heutzutage mit vielen Warnhinweisen, ist immer, wie geht ein Benutzer mit dieser Warnung um? Was kann er überhaupt tun, wenn er so eine Warnung sieht? Und versteht ein User diese Warnung auch? Das sind so zwei Aspekte“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 59)

„Es hat sich einfach gesagt, dass es gerade bei technischen Themen eine Warnhinweise nicht viel bringt, weil die meisten User gar nicht wissen, wie sie im Falle einer Warnung reagieren müsse“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 59)

„Es bringt nur den technischen Usern etwas. Zu den generellen Usern ist es dann meistens eher ein Hindernis.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 59)

„Genau, aber wie gesagt, es kommt immer auch ein bisschen darauf an, wie man diese Warnung implementiert. Ich meine, die ZAHW hat mal einen Versuch gestartet, so wie ich weiß, dass sie alle E-Mails von extern mit einem gelben Warnbalken versehen haben. Also dann kam bei jedem E-Mail dieses E-Mails von extern. Und ich denke, gerade solche Warnhinleiten bringen dann genau gar nichts, weil die kommen dann einfach bei jedem zweiten oder dritten E-Mail, also die Häufigkeit ist sehr hoch. Und das führt dann einfach dazu, dass die Leute das ignorieren, ganz klar“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 61)

„Aber wie gesagt, wenn so eine Warnung angezeigt werden muss, dann muss eigentlich der Fall technisch bereits klar sein, dass das ein Phishing-E-Mail ist. Und nicht der User muss dann überlegen oder eigentlich wissen, was zu tun ist oder. Sondern es ist dann wirklich ein Last Line of Defense im Endeffekt“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 61)

„that that makes sense of course if you can give the person warnings in the place where then let's say in the place of the crime it's always very important especially in very /. For example you have emails that when you some companies add a notification hey be careful this email is from external sender or before you upload the file hey be careful don't upload sensitive files make sure you're just uploading. So this is not a bad thing to do i think as long as it's in a good place and not harming business it makes makes sense“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 82)

„Yes so if you add them. It really needs to be in a good place like maybe you need to see this maybe once twice a day if you see that all the time you just become blind and don't care anymore“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 84)

„Das kommt drauf an, welches Risiko, wo man mitigieren will. Also sinnhaftig könnte es sein, so eine Geschichte wie, ich haue irgendwo einen Banner rein oder einen taggenden E-Mail mit, die kam von extern. Die wurde nicht von intern versendet. Das ist immer hilfreich und ein Indikator für, hier bitte erhöhte Sensibilität, genauer hinschauen. Solche Hilfsmittel, für die spreche ich mich stark aus.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 55)

„Ja, auch die kann man natürlich als Angreifer versuchen zu faken oder dazu umgehen. Es suggeriert natürlich über die Dauer, dass das funktioniert, aber auch das kann mal aussetzen oder nicht funktionieren. Und wenn man sich immer darauf verlassen hat, dann passieren die Unfälle“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 57)

„Das Problem damit ist das bringt gar nichts. Nach einer Woche nehmen die nehmen, die mitarbeitenden das nicht mehr war diesen Banner. Die sehen das einfach nicht mehr, man wird blind dafür. Also Ich /. Die technischen Warnhinweise halte ich nicht für nachhaltig, oder. Deswegen, man muss mehr machen als so etwas auf jeden Fall“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 52)

„Man muss ständig präsent sein. Das ist jetzt auch meine Aufgabe hier an der ZHAW, zum Awarness ständige Präsenz zu zeigen, dass man immer wieder daran erinnert wird, dass überall mal so ein Reminder auftaucht, hey, denk dran, das ist so das wichtige Elemen“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 73)

„Ich sagt zum Beispiel zu Banner, ich habe da ganz klar die Einstellung, ich finde Banners useless, wil du hast /. In der ersten Woche, in der der Banner eingeführt wird, sehen die Leute den noch und danach nie wieder. Der wird ausgeblendet vom Hirn, kannst "knicken", der hat "null Impact".“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 74)

„die werden mit der Zeit schon blind, aber da hilft auch der Hinweis, nicht eh, du verlässt jetzt, das liest du zweimal und dann liest du nicht mehr, du weißt, da kommt was und dann ist es egal, was kommt.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 77)

„Also es muss einen gewissen Seltenheitsfaktor haben. Also darf nicht die (unv., #00:41:19-4#) Grenze zusammen, sonst wirst du effektiv betriebsblind“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 82)

„Nein, ich denke jedes Mittel, jede Methode, um die Awareness zu fördern erachte ich als sinnvoll.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 48)

„Ich sag mal, je besser oder je mehr die Informationsflut in Anführungszeichen besteht oder die Leute darauf hingewiesen werden, desto eher gehen Sie ins Bewußtsein über wieder vergleichbar mit mit Werbung.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 48)

„Vermutlich sowohl, als auch. Die helfen ein bisschen, die helfen logischerweise. Die Gefahr ist auch da wieder die gleiche. Wenn dann bei jedem Mail steht, achten, das ist ein externes Mail, dann liest du diesen Banner irgendwann nicht mehr. Es gibt vor allem auch der Firma oder dem IT-Leiter die Möglichkeit zu sagen, ich habe es dir doch gesagt, ich habe dich doch gewarnt, das steht doch im Mail, pass auf, das ist ein externes Mail. Das gibt vor allem einen Schutz für den mitarbeiter nein die IT-Abteilung "tschuldigung" und auf der anderen Seite ist es eben, wie gesagt, alles was repetitiv wird, was wiederholend wird, das wird irgendwann für den Konsumenten, für den User, für den Nutzer obsolet, weil es steht ja in jedem Mail“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 42)

Technologisch — Unterschiedliche Plattformen

„Und es zeigt sich schon, dass gerade Smartphones sehr häufig verwendet werden. Also es macht in jedem Fall Sinn, dass man auch Phishing Awareness eigentlich auf mobile Geräte abstimmt und auch testet, ob diese mobilen Geräte das anzeigen. Es macht auch insofern Sinn, nicht nur auf Trainingssicht, sondern auch aus Angreifersicht, weil es gab in den letzten Jahren

vermehrt Phishing-Attacken, die gezielt auf User, die mobile Devices verwenden, abgezielt wurden.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 64)

„Es bringt natürlich nichts, wenn man Leute eine Outlook-Schulung macht und ihnen zeigt, wie man im Outlook mehr oder weniger Phishing-E-Mails erkennt, aber dann niemand Outlook verwendet oder. Weil man kann dann vielleicht gewisse Grundprinzipien beibringen, wie zum Beispiel ein Phishing mal aussieht oder wie Phishing-Absender aussehen, aber oftmals ist das Design dieser Applikationen oder dieser Mail-Client so anders, dass viele Leute Probleme haben, ihr Wissen von einem Mail-Client auf den anderen zu übertragen. Also ich empfehle ganz klar, die Leute auf den Programmen zu schulen, die sie auch tagtäglich verwenden, um diese E-Mails zu öffnen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 72)

„Oder dass der Aufwand exponentiell groß ist, weil man hat eine unendliche Anzahl von verschiedenen Geräten und man muss dann halt ein bisschen schon entscheiden, welche Geräte man schulen will oder auf welchem Programm man schulen will. Und das ist natürlich heute sehr schwierig, weil mit dem ganzen Bring Your Own Device kann man natürlich dann nicht sagen, man macht eine Schulung für alle Geräte, die eine große Firma zur Verfügung stellt“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 74)

„especially small bite education should be mobile friendly because this is where people are and especially we want them to consume education in a way that is comfortable for them so they can just /. They can see it as a let's say a break from work they can take their phone just sit on the sofa and just click through it um learn another one rather than the torture that every sit in front of them of the desktop and click around“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 86)

„Unbedingt. Das ist ganz, ganz wichtig, dem Endanwender mitzugeben, welche Möglichkeiten hat er denn zu prüfen. Und den technisch weniger versierten muss man halt eben die verschiedenen Varianten aufzeigen. Und das am besten auf jeder Plattform.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 59)

„Was wir machen können ist, wir können auswerten welche Plattformen werden bei uns zu welchem Grad genutzt oder? Und dann können wir die Schulung Schulungsunterlagen entsprechend auf die am häufigsten genutzten Plattformen Email Clients etc. auch ausrichten. Ich finde das wichtig, dass die Leute sich dann auch dort wiederfinden oder mit sich damit identifizieren können.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 54)

„Ich glaub, das ist schwierig, Das ist aufwendig. Aber ich würde allen die Informationen für die am häufigsten genutzten Plattformen zur Verfügung stellen“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 56)

„Also man muss es auf alle Fälle berücksichtigen, aber der Nachteil ist, die Vielfalt ist sehr groß. Also wir haben so viele verschiedene Devices und wie du das schon richtig erkannt hast, wenn ich jetzt auf den Desktop einen Link anklickte, also typisch eh achtet auf den Link, das ist auf dem Mobile fast nicht machbar. Darum muss man auch auf verschiedene Phishing Hinweise oder Phishing Merkmale hinweisen, dass man , ja/.Das man mit der Zeit mehrere Varianten vielleicht ausmachen kann, was so ein Phishing ausmacht. Und wir wissen ja auch nicht, wenn wir die Kampagne fahren, auf welchem Device öffnet er jetzt das Mail, also auf dem gibt es wahrscheinlich einen sehr gesunden Mix“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 84)

„Ja, voll dabei. Also muss unbedingt beachtet werden. Also solange die Firma zulässt, dass E-Mails auf dem Handy aufgemacht werden dürfen, muss es auch trainiert sein, weil es ist effektiv so, wie du gesagt hast, Severin, es ist so, dass auf E-Mail /. Wenn du auf links klickst auf dem

Handy, dass es sehr, sehr einfach ist, die Leute so sehr zu verwirren.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 85)

„lso die Chance ist natürlich schon, dass man, ja, die verschiedenen Umgebungen trainieren kann, weil das Gleiche verschieden aussehen kann unter Umständen. Also es wird einfach mehr Wissen vermittelt in dem Ganze. Man merkt es ja, wie du gesagt hast, so ein Mobile, wenn ich das im Hochformat habe, stellt es nur quer, sieht die Welt teilweise schon ganz anders aus. Also die Erfahrung, wo der User mitmacht mit dem Umstand, die ist natürlich auch sehr wichtig.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 87)

„nsoweit berücksichtigen, dass wenn das online Schulungen sind, dass die sicher auf auf heute gängigen Geräten eben wie Smartphones, Tablets oder Notebooks Arbeitsstation im Büro, dass die von überall aus gemacht werden können selbstverständlich“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 50)

„Ja, also definitiv eben wir sind heute so verletzt und so mobil unterwegs, man weiß ja nicht wer hat welche Mittel. Die meisten haben alle Mittel, die du aufgezählt hast, also Mobileohones, Desktops und Tablets von daher ja denke ich schon, dass man solche Tools und solche Trainings auch auf die ich sage jetzt mal etwas neueren Endgeräten und nicht nur auf PC Notebook beschränken sollte, eben weil du hast es beschrieben, je nach Plattform mehr oder weniger Möglichkeiten zur Verfügung stehen und ich denke auch dass muss man dem Mitarbeiter zeigen, sagen, schulen. Weil eben in der vernetzten Welt spielt das gar keine Rolle, auf welchem Endgerät ich arbeite ich kann das Problem eigentlich über so viele Stellen ins Unternehmen schleusen, von daher macht das Macht das Sinn meines“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 52)

„Macht sicher Sinn, auch da generisch dann halt, wenn ich unsicher bin bei einem Mail, dann kliche ich lieber eben absolut /. integrieren würde ich, weil ich glaube, je nach Firma, wenn es wirklich Firma gibt, die Mails auf den Mobile Phones nicht erlauben, dann ist es logischerweise nicht relevant, aber es ist heute fast in jeder Firma relevant, muss man schon schulen, glaube ich schon“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 48)

Technologisch — Interne Meldeplattform

„. Und soviel ich weiß, oder soviel ich das noch im Kopf habe, haben sie wirklich zeigen können, dass das eigentlich positiv ist, um die Reaktionszeit der IT runterzubringen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 70)

„Und es macht es natürlich auch wahrscheinlich für die User einfacher, solche Dinge zu melden, wenn sie einfach einen Button haben oder wenn sie einfach eine einfache Möglichkeit haben, an das zu melden“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 70)

„das Melden generell von Phishing-E-Mails oder auch Phishing-Webseiten kann sehr hilfreich sein zur Bekämpfung dieser Webseiten, weil wenn viele Leute das melden, kann man viel schneller reagieren, als wenn eine Person gephisht wird und 100 Personen auch gephisht werden und niemand meldet oder“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 70)

„Risiko ist natürlich immer da, wenn man eine User-Base hat, die vielleicht nicht so gut im Reporting ist oder im Erkennen von Phishing-E-Mails. Das kann natürlich auch dazu führen, dass falsche E-Mails reportiert werden oder dass der Aufwand dann groß ist, um zu überprüfen, ob diese E-Mails wirklich legitim sind oder Phishing-E-Mails“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 70)

„It's very easy to collect all this information but if you're not doing anything with it you're just doing damage to yourself so you don't want to collect information you don't benefit from and once you do that you put this button and let the people click on it um it can create a lot of noise in big companies you will be bombarded with emails all the time“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 88)

„And what's the problem there are too many problems with it. Many many times people are using it as a not as a phishing button so that oh i think this is an attack i have to tell everybody about this attack no usually the case is that i don't know this is spam i don't know if it's a spam or phishing i don't care i use this people using it as a spam button okay so most of the time the stuff that they are proposing (unv., #01:05:53-3#)“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 88)

„You know for the benefits of course security operations center if they are building good playbooks good automation to filter out most of the cases then of course you can benefit from the benefits is that for example to like at least the one that we sell can use it and also others using a little better rating of the employee so for example an employee reported the phishing email part of our simulation then it gets positive points for that and is risk factor decreased um.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 88)

„Another important aspect of it first of all i mean it can help you to detect fishing attack right if you handle all the alerts correctly.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 88)

„The company third important aspect is that this button is always there so it reminds the user when he opens his mailbox there might be some phishing some email so like like an ad for that and yeah that's it i think.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 88)

„Ja, ansonsten sollte man den Endanwendern klar kommunizieren, wie sie denn beim Verdacht auf Phishing, Schlagklammer jetzt mal Spam aus, als nicht der effektive Schadensverursacher, sondern Phishing, wie sie reagieren sollen und wie sie reagieren sollen, wenn sie die Mail wirklich eindeutig als Phishing identifiziert haben. Ich glaube, dort muss man kurz und knackig den Endanwendern mitteilen und auch Möglichkeiten geben über einen Button, über ein Kontextmenü, ihnen sagen, wie machst du das in deinen, in den häufig genutzten Mail-Clients, auf den häufig genutzten Endgeräten, wie hast du da vorzugehen. Also die User schauen, dass die da vereinheitlich ist und einfach“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 65)

„Gut, wir sind jetzt relativ große Organisation, aber wir hatten nach der ersten Durchführung, da waren bei uns eigentlich 4-5 Personen 2 Wochen lang beschäftigt, nur mit den Anfragen zu diesem Phishing Mails, da die zu bearbeiten und zu beantworten, das ist nicht zu unterschätzen, oder“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 22)

„Ich, sehe da in erster Linie Aufwände oder. Weil im Outlook können Mails schon relativ komfortabel als junk markiert werden. Wenn wir jetzt über einen Button, jede verdächtige Mail an den Service Desk schicken, dann generiert das einen gewissen Aufwand. Ich meine, man kann, muss dann überlegen was hat das für einen Sinn? Was erwarten wir von den von den Benutzern, wenn sie da drauf klicken? Was soll das auch auf der Seite zum Beispiel Security Monitor oder so dann auslösen? Was ist die Erwartungshaltung? Erwarten, die unsere Mitarbeitenden, wenn sie da auf den Button klicken, dass sie dann immer eine Rückmeldung bekommen irgendeine Bestätigung? Ja, das war jetzt Phishing, oder das war kein Phishing oder ist das einfach nur ein zur Kenntnisnahme, aber dann warum reicht denn der Junkfilter nicht einfach, wo man sagt OK Rechtsklick auf die Mail und Junk markieren?“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 62)

„ass wenn die Leute sowas melden, dass dann auch darauf richtig reagiert werden kann, damit die Leute dann nicht das Interesse am Melden verlieren zum Beispiel oder.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 7)

„Also meiner Meinung nach ist das keine Chance und kein Risiko. Das ist schon eine Pflicht, dass man den User darauf hinweist, wie er so ein Mail weitergibt, damit man das richtig von den richtigen Leuten untersucht wird. Und ganz wichtig ist auch zu vermitteln dem User gegenüber wieder, dass er keine Angst davor haben muss, dass er keinen Fehler macht mit sowas, weil oft ist auch Angst dahinter, dass wir sowas melden.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 89)

„Als Chance sehe genau das eigentlich, dass vielleicht, wenn wir Glück haben, mal effektiv eine böse Mail gemeldet wird, dass wir diese analysieren können, dass wir auch verstehen oder lernen können, warum das durchgekommen ist. Risiko sehe ich schon ein bisschen, aber jetzt nicht unbedingt bei uns. Also gut, ein Risiko sehe ich schon. Wir haben Spezialisten, die Mails aus dem Junkmail Ordner melden. Das generiert einfach Aufwand für uns und für nichts, weil es ist ja schon aufgefahren, dass es schlecht ist. Aber ich sehe auch noch ein echtes Risiko für vielleicht kleinere Firmen. Häufig werden solche E-Mails genommen und man sagt, okay, vielleicht ist sie bösartig, ich melde die. Und dann gehen die häufig durch automatisierte Prozesse durch, zum Beispiel durch eine Sandbox. Und ich kenne /. Also ich habe früher Kunden gehabt, die dann hingehen, ja, "Jo" wir werfen jetzt das mal in eine Sandbox rein, die eher public verfügbar ist. Und dann hat man nachträglich gemerkt, das waren interne Daten von uns.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 90)

„Auch bei einem Befall sieht man immer wieder die Mitarbeiter scheuen sich, das zu melden. Sie haben Angst vor Konsequenzen. Sie möchten nicht als als als "Buhmann" dargestellt werden, was in der Regel nicht der Fall ist. Aber das Ganze natürlich verschlimmert, wenn, einfach der Befall, sag ich mal erst Tage später festgestellt wird, durch andere Mitarbeiter oder durch Überwachungssysteme. Ja, wäre sicher, oder in den meisten Fällen besser händelbar wenn etwas geschieht, wenn man das so früh wie möglich weiß.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 32)

„hancen bestehen natürlich darin eben die IT-Abteilung wird, sofern dass zeitnah gemeldet wird informiert, dass sowas im Haus ist. Gegebenenfalls weitere Schritte einleiten kann“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 54)

„Risiken sehe ich natürlich für den oder aus Sicht des Mitarbeitenden eben wieder diese Prangerfunktion. Man weiß, ich hab jetzt da ich sag jetzt mal "Mist gebaut" und das wissen jetzt die von der IT und das weiß mein Chef nachher und hat ich sage jetzt mal "schürt" Ängste um um um Jobsicherheit usw oder einfach "schürt" Ängste vor Repressionen“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 54)

Umfeld

Umfeld — Einbindung externer Firmen

„Bei SaaS-Lösungen ist immer das Problem oder die Frage, wie der Datenschutz geregelt wird. Weil die Daten liegen ja dann irgendwo auf einem Server in der Cloud und es ist dann immer die Frage, wer hat Zugriff darauf. Und gerade bei Phishing ist dann die Frage, auf welche Daten

haben Sie Zugriff. Meistens kann das dann relativ viele persönliche Informationen sein, gerade wenn man E-Mails schickt, die dann auch relativ persönlichen Inhalt haben. Und darum sage ich immer, bei SaaS-Lösungen ist eines der größten Risiken aus meiner Sicht, dass diese Daten abwandern oder dass diese Daten halt von anderen Leuten eingesehen werden, die man vielleicht nicht will.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 51)

„Ja, meine Chancen sind ganz klar. Man hat meistens dann eine Partnerfirma, die eigentlich für einen dieses Phishing-Training durchführt. Und es ist wie beim meisten Security-Themen, wenn man durch eine Partnerfirma, die darauf spezialisiert ist, noch ein Training durchzuführen, dann ist das Know-How meistens größer, als wenn man das in-house macht. Oftmals haben diese Leute dann mehr Erfahrung, weil sie in verschiedenen Firmen tätig sind und halt auch aus verschiedenen Firmen oder verschiedenen Unternehmen ein bisschen das Know-How entwickeln können, sage ich mal. Natürlich ist es auch die Frage ein Kostpunkt im Endeffekt.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 53)

„Weil ja, gerade im Security-Bereich haben wir nun mal einen Fachkräftemangel und da ist man wahrscheinlich dann relativ schnell froh, wenn man sehr viele Arbeitsstunden auslaken kann, gerade für solche Tasks, die eigentlich gut von einem externen Dienstleister durchführbar sind.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 53)

„jedes Land hat seine eigenen Regulierungen, wenn es um Phishing-Awareness geht. Wenn man mit ausländischen Firmen zusammenarbeitet, muss nab sich natürlich /. Oder muss die ausländische Firma sich bewusst sein, wie die Regulierungen im eigentlichen Land sind oder. Das ist schon noch wichtig, dass man da auch ein bisschen Konsens hat. Das ist vor allem dann sehr wichtig, wenn man auch internationale Partner hat, die übersehen sind, zum Beispiel aus den USA. Weil das US-Recht ist schon sehr unterschiedlich zum europäischen Recht. Gerade auf rechtlicher Ebene muss man hier sehr viel beachten. Man sollte schon immer sehr aufpassen, wenn man an so einem Phishing-Training durchführt, dass das auch den länderspeziphishen Regulationen angepasst is“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 78)

„it but this is also something that theoretically can happen um and if some malicious actor is taking over this server that is doing this fishing training theoretically can launch real attacks on your employees because it is completely whitelisted.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 22)

„On the other end you're also sending information there from your active directory you need to understand if this is something that is allowed in your country many companies in in europe will never allow their information to go to the united states about all their employees and so on so that's that's what you need aboit it.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 76)

„hey don't know what your company needs you need to tell them what are your needs what are your priorities what is your culture now where do you want it to be and how do you“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 93)

„But you need to make sure they don't have access to they don't have access, they don't collect and don't have access to more than what they have to of course that you get the service you want with all the dashboards all the reports whatever.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 93)

„Yeah i mean you want to have /. First i mean the main advantage of having let's say a partner to do your training is that this partner has a lot of experience doing other trainings for other companies like you so if he has /“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 95)

„And also another thing it's also the sense of the business culture every time you do business from people from another country like they don't delivering time in your swiss company you're curious to get your stuff on time and in some quality and there are some ethics. And let's say for example and i'm telling you as an israeli and swiss representive. When you're telling when a swiss person tells another swiss person i think you may want to consider that, it means you want that right?“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 97)

„Es bleibt immer ein sensibles Thema und ein externer Partner kann das gar nicht abschätzen. Wie sind deine Zielgruppen? Wie ticken die Leute? Wann ist es zu viel? Wann ist es zu wenig? Wann wird was überschritten? Wann ist die Schmerzgrenze erreicht? Das ist alles etwas schwierig und von daher SaaS das Ganze zu beziehen, wenn man es technisch integriert bekommt“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 71)

„a, aber die Thematik ist eine generische Thematik, die haben wir bei jeder Software, die wir irgendwo aus der Cloud beziehen oder die von einem Drittanbieter kommt, dort müssen wir einfach ganz klar die Verträge aushandeln und auch richtig darauf hinweisen, gerade wenn es schützenswerte Daten sind, personenbezogene Daten, müssen wir halt auch die Auflagen entsprechend hochlegen und auch auditieren, erfüllt der Anbieter das Ganze.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 75)

„Also Vorteile sind sicher.Man kann dann von echten Szenarien, die vielleicht auch bei anderen Unternehmen schon erfolgreich waren oder gut angekommen sind, kann man profitieren kann man die wiederverwenden. Die externen Partner haben oft schon mit Markeninhabern abgeklärt, ob das ob diese einzelne Szenarien dann auch genutzt werden können, davon kann man sicher profitieren. Und man spart sich dann natürlich den ganzen Aufwand, irgendwelche Kampagnen selber zu bauen, sondern das wird bereitgestellt oder das sicherlich viele Vorteile.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 68)

„Ja. Nachteile sind vielleicht, dass die Partner die Organisationskultur selber nicht nicht gut kennen, aber der braucht entsprechenden Sparring-Partner intern, der das vielleicht sagt, das kann bei uns gut funktionieren, das funktioniert bei uns nicht gut.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 68)

„Das Risiko würde ich als sehr geringe einstufen. Und selbst dann selbst wenn es /. Also (unv., #00:44:49-8#) Jetzt muss auch vorsichtig sein. es kommt drauf an, wie es implementiert ist, dann letztlich, oder. Wenn das ein vertrauenswürdiger Partner ist und wenn Benutzer dann auf eine zufällige Login Seite gelockt werden und dort ihr Passwort auch eingeben und der der Dienstleister ist kompromittiert oder Dienstleister speichert diese Eingaben von den Passwörter der Nutzer im Rahmen des Simulation, dann ist es nicht mehr akzeptabel, oder. Also passworteingaben dürfen auf keinen Fall gespeichert werden, weil die müssen komplett ignoriert werden.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 70)

„Ja also ich glaube auch das der Sitz des ausländischen Partners muss über ein vergleichbares rechtliches Niveau verfügen wie die Schweiz oder also muss vergleichbar sein. Ich finde EU Ausland wäre auch noch akzeptabel, weil wir uns ja letztlich alle irgendwie an der DSGV auch orientieren. Auch was Meldepflichten angeht bei Sicherheitsvorfällen usw ist es ja ähnlich. Aber jetzt bei anderen Anbietern hätte ich da Bauchschmerzen, wenn der Anbieter irgendwie eben in Nigeria, China oder so oder im Iran sitzt, da hätte ich damit mehr Bauchschmerzen, oder in Russland“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 72)

„das Ganze muss natürlich datenschutzkonform sein. Das ist jetzt A und O“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 106)

„sogar Chancen, weil eben /. Du oder keine Ahnung jetzt ein CISO könnte hingehen und sagen, ich möchte jetzt wirklich mal uns damit testen. Also wirklich nicht nur Personen damit testen,

sondern zum Beispiel auch die Security-Organisation damit testen. Und da hast du eher eine Chance mit einem externen Partner, als wenn du intern jemand nimmst, der in die Security eingebunden ist.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 109)

„Externe Partner haben auch einen Erfahrungsschatz, wo man von nutzen kann“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 110)

„Ich denke, das Risiko ist gering und Risiko hat manüberall. Das kann auch mit einer eigenen Lösung passieren ja.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 119)

„ah sehe ich eigenlich auch so. Es ist natürlich so, dass größere Provider immer eher von Interesse sind, zum Angreifen. Also Was weiß ich, zum Beispiel SolarWinds vor ein paar Jahren war /. Also als Angreifer würde ich tendenziell, wenn ich Aufwand betreibe, würde ich sagen, ich greife entweder die einfachen an, also grundsätzlich "Low Hanging Froot" oder ich greife etwas heftiger an, wie zum Beispiel eine Microsoft oder eine SolarWinds oder was weiß ich. Und aus dem könnte man jetzt ein Risiko spinnen. Ich persönlich sehe es aber als weniger extrem, also ich sehe es jetzt nicht als riskant.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 120)

„Wenn man mit externer Anbieter hat und die solche Payloads im Angebot haben, dann sind die schließlich nachher auch dafür haltbar und damit sind wir raus. Und wenn die das uns anbieten, dann können wir das natürlich auch wieder nutzen. Aber wir von uns aus selber verlassen uns eigentlich nur noch auf abgesicherte Tools“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 144)

„Man muss schlussendlich ein gewisses Vertrauen haben, in diese Unternehmen, eben weil man ihre Systeme eigentlich ausschließt aus den ganzen überprüfungs Geschichten. Und die Gefahr besteht natürlich immer, dass ich wir diesen Partner, wenn der nicht entsprechend geschützt ist oder kompromittiert worden ist, auch mein Unternehmen kompromittiert werden kann. Das ist so eigentlich so die /. Ich sag mal, die aus meiner Sicht die die größte Gefahrenquelle, aber sie ist relativ /. Meiner Meinung nach relativ klein zu beurteilen“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 60)

„bei ausländischen Partnern wird gegebenenfalls die Rechtslage anders sein. Ich meine der Anbieter muss sich grundsätzlich nur wenn Recht seines Landes rechtfertigen. Ähm, kann sein, dass ich sag jetzt mal, wenn das Ding sagt in Russland steht, wo vermutlich nicht ganz so strenge Maßnahmen oder ganz so strenge Richtlinien bestehen und wir das in der Schweiz nutzen.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 62)

„Und dann hat man das arrogante Gefühl, dass man alles besser weiss, das ist gerade im Security Bereich leider nicht mehr möglich, da braucht es Experten. Und deshalb ist für mich die Begleitung durch einen externen Partner vor allem eine Chance, glaube ich.“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 50)

„Logischerweise ein gutes Vertrauensverhältnis aufbauen mit dieser entsprechenden Partnerfirma zu überlegen, ist das jetzt eine amerikanische multinationale Firma, die keine Emotionen zu mir in der Schweiz hat, vielleicht hat man an dem Freude vielleicht auch nicht und da gibt es auch nicht richtig und falsch, aber die Vertrauensbeziehung, die finde ich wichtig.“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 50)

Umfeld — Meldungen an Externe

„Wenn man jetzt sagt extern, so ausserhalb des Unternehmens, dann ist es klar, dann kommt es ein bisschen darauf an, in welchem Land man tätig ist. In der Schweiz würde ich jetzt empfehlen, man sollte das National Cyber Security Center, also NCSC, informieren, wenn es eine grössere Phishing-Kampagne ist. Man sollte den eigenen Domain-Registrar mit ins Boot holen, weil diese Domains können natürlich auch gesperrt werden, was dann ein Phishing-Training natürlich unmöglich macht. Und eventuell, je nach Größe, sollte man die Switch also den für den Schweizer Markt tätigen, wie sagt man, Domain-Registrar, auch mit ins Boot holen oder darüber informieren, dass solche Domains registriert werden und für Trainingszwecke verwendet werden. Ansonsten kann es natürlich sein, wenn man gerade von externen E-Mails versendet, dass diese dann auch von externen geblockiert werden, dass der Domain-Registrar diese Phishing Emails oder diese Domains erkennt und auch blockiert und die E-Mails gar nicht bei den Absendern /. Also bei den Usern ankommen oder dass die Website-Links, auf die dann verwiesen werden, bereits gesperrt sind.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 76)

„Aus meiner Sicht ist es kein Zwang, es ist eine Empfehlung grundsätzlich. Wenn wir zumindest von der Schweiz reden, gibt es kein keine /. Also keine Pflicht, dass man diese Leute informiert also "zwingendermassen". Man will aber natürlich nicht unbedingt auf Konfrontationskurs mit diesen Institutionen geben. Und wie gesagt, es kann natürlich sein, wenn man diese Nicht-Vorgänge informiert, dass diese einen sozusagen blokieren das die domains (unv., #00:50:22-2#) blockiert werden. Aber meines Wissens nach ist es keine Zwingendermaßen, dass man die informieren muss. Es ist mehr eine Empfehlung“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 84)

„ist ein sehr großes Risiko, das ist uns während der Studie auch passiert. Es ist sehr wahrscheinlich, gerade wenn man einen größeren Rasen Phishing Awareness macht, ist die Wahrscheinlichkeit fast 100%, dass Leute das an ausserhalb der /. Also zumindest im technischen Bereich außerhalb der Universität bei uns melden. Und das kann natürlich dann Prozesse bei anderen Firmen auslösen, dass zum Beispiel wenn man jetzt davon ausgeht, dass ein Unternehmer eine Phishing Awareness Kampagne macht und jemand meldet das an das NCSC, kann das natürlich dann sein, dass das NCSC ihre internen Prozesse startet und natürlich die Firma informiert, dass so ein solches Phishing E-Mail gemeldet wurde. Und dann überprüft, ob die Firma eventuell gehackt wurde oder sich mit der Firma in Verbindung setzt. Und das kann natürlich dann je nachdem, was für E-Mails gesendet werden, durch auch weitreichende Folgen haben. Also es kann zum Beispiel auch sein, dass man die Firma informiert, wenn es jetzt zum Beispiel eine Branded E-Mail ist und dass dann die Firma anfängt, ihre internen Prozesse laufen zu lassen, zum Beispiel eine Warm-E-Mail herauszuhenden an ihre Kunden. Solche Dinge können möglicherweise passieren. Das ist wahrscheinlich ein sehr großes Risiko, wenn man natürlich diese Meldepflicht gegen extern macht oder wenn man sagt, okay, man muss jedes Phishing E-Mail melden“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 88)

„So one of our phishing attack templates had Melanie in it and one of the one of the employees that received the phishing attack simulation reported to melanie that we are using their logo they got really pissed. So we removed this attack anyway but i think in general if you're using any logo of any organization you should tell them“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 105)

„To be honest us we only report to the cloud provider where we /. But we do not know telling about every campaign we just tell them this is a phishing attack server don't pay attention if you see some warnings or regards from other people in the company performing it and practically besides this and the company itself that receives it nobody needs to know about.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 107)

„Ja, NCSC genau, National Security Center Swiss, oder Switzerland. Genau, dort sollte man die Kampagnen ganz klar anmelden. Es ist auch verständlich, denn viele, die irgendwo in einem Unternehmen nur temporär angestellt sind oder eben nur zu einem gewissen Beschäftigungsgrad, die leiten ihre Mails weiter, die kommen also irgendwo an, die denken, was ist das hier und melden das einfach an der offiziellen Stelle und die offizielle Stelle bewertet“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 20)

„die wir am Anfang hatten mit NCSC, dass man eben die Kampagnen anmelden soll und deren Handling über die Masse, das ist für die okay, das funktioniert. Wichtig ist einfach, dass man nicht auf Sperrlisten kommt, dass zum Beispiel auch große Provider wie dann die Switch sich auf eine DNS-Sperrliste nehmen. Da sollte man halt wirklich aufpassen“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 65)

„Ja, das hängt eher damit zusammen, wo beziehe ich denn meine Domains. Irgendwo muss ich ja meine Domain registrieren, wenn ich eine Phishing, Fremddomain oder Drittdomain durchführen will, dann macht es natürlich auch Sinn, den Hostel zu informieren. Wir verwenden diese Domains zur Durchführung von internen Phishing Kampagnen. Das ist unser Vorgehen, das sind die Zeiträume, wo das abläuft. Also wenn dort Meldungen kommen, müsst ihr nicht zwingend direkt sperren, sondern kommt auf uns zu. Wir stehen Rede und Antwort. Eine Ansprechpartner bekannt geben ist dort ganz wichtig beim Domain Registrar. Sonst ist man nämlich ruckzuck auch auf irgendwelchen Blacklisten. Und wenn das vermehrt aus dem IP Bereich kommt, IP Block kommt, kann es dann auch der IP Block drauf kommen und das wollen wir natürlich nicht“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 79)

„Und wir hatten das in der Vergangenheit auch, dass uns von Mitarbeitenden tatsächlich das Nationale Cybersicherheitszentrum informiert haben, über die Phishing versuche. Die sind direkt auf das NCSC gegangen und das NCSC ist dann wieder zurück gekommen zu uns und hat gefragt was macht ihr denn eigentlich? Es bleibt nicht, es bleibt nicht in der Organisation, wenn man so etwas macht. Irgendjemand geht damit nach draußen und das kann sein, dass sie damit an die Presse gehen, es kann sein, dass sie damit an die Markeninhaber gehen es kann sein, dass sie das eskalieren an so zum Beispiel Polizei oder an irgendwelcge Behörden und oder ans Cybersicherheitszentrum also ist /. Und es kann noch ganz andere Effekte haben, an die ich jetzt vielleicht ganz denke“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 64)

„Ja, also eben das Hoster registrat stimmt, ich erinnere mich jetzt auch da hatten wir einen Austausch, die sind auf uns zugekommen genau. Ja ansonsten das NCSC werden wir zukünftig auch immer informieren, wenn wir bisschen Kampagnen fahren. Switch als Betreiber des schweizerischen Hochschulen und Forschungsnetzes, die müssen auch informiert werden. Ja.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 76)

„Ja, die Hoster und Registrare haben damit gedroht, unsere die in der Fisch und Kampagnen genutzten Domains zu sperren also sie haben gedacht die werden nur zu Phishing zwecken verwendet und haben damit gedroht, die zusperren, wenn wir ihnen keine Rückmeldung geben“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 78)

„Ja, vor allem wenn man Payloads benutzt, die nicht zulässig sind, dann kriegt man vom NCSC ganz schnell eins "auf die Mütze". Ja, also bei uns ist es so NCSC und wir haben noch die Switch an der Seite, die im Hochschul verbunden mit drin ist. Und viele Hochschulen sich den angebunden haben. Zwischen Stiftung, die auch Netzwerk verwaltet und so weiter. Und die analysieren auch Netzwerkverkehr. Drum informieren wir die auch. Also für uns ist Switch und NCSC sind eigentlich die zwei Institutionen, die Bescheid wissen müssen.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 125)

„Ja, das generiert halt auch unnötigen Aufwand“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 133)

Umfeld —
Rechtliche Aspekte

„Oder halte eben auch, dass solche Phishing Kampagnen je nach Land speziphishe Regulierungen haben, die dann relativ schwierig umzusetzen sind teilweise.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 17)

„jedes Land hat seine eigenen Regulierungen, wenn es um Phishing-Awareness geht. Wenn man mit ausländischen Firmen zusammenarbeitet, muss nab sich natürlich /. Oder muss die ausländische Firma sich bewusst sein, wie die Regulierungen im eigentlichen Land sind oder. Das ist schon noch wichtig, dass man da auch ein bisschen Konsens hat. Das ist vor allem dann sehr wichtig, wenn man auch internationale Partner hat, die übersehen sind, zum Beispiel aus den USA. Weil das US-Recht ist schon sehr unterschiedlich zum europäischen Recht. Gerade auf rechtlicher Ebene muss man hier sehr viel beachten. Man sollte schon immer sehr aufpassen, wenn man an so einem Phishing-Training durchführt, dass das auch den länderspeziphishen Regulationen angepasst is“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 78)

„dass man sich auch bewusst ist, dass wenn man Branding von externen Partnern verwendet, dass man auch dementsprechend, wie sagt man, dementsprechend die Einwilligung dieser Partner einholen muss.“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 80)

„Dass wenn jetzt zum Beispiel eine Firma für uns Phishinge Awareness durchführt, dass sie sich bewusst sind, dass sie auch einen Teil der Verantwortung tragen oder und dass sie auch diese Verantwortung dann rechlich, falls das jetzt rechtere Folgen hätte, auch tragen oder die Verantwortung dafür übernehmen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 80)

„wird Phishing Awareness grundsätzlich als Phishing anerkannt, also auf rechtlicher Basis, wenn dies nicht offiziell gemeldet wird. Das heißt, rein theoretisch könnte man als phisher verklagt werden, wenn man Phishing Awareness in der Schweiz macht, wenn man die in dementsprechenden Fälle also (unv., #00:49:02-1#) Stellen nicht informiert, sowie auch eben wie gesagt das Branding einhaltet. Es kann sehr hohe rechtliche Konsequenzen haben, wenn man das falsch macht. Nicht zu unterschätzen“ (Experte 1 Interview-20230419_ZHAW_Aufzeichnung, Absatz 82)

„The second even more important thing is to adjust the content to the country to their laws in the country and also specifically to the policies of the company itself i've seen many companies just buying some let's say password course and just like playing it okay so i bought a video teaching you about password security but then the instruction how to set a secure password doesn't fit the company policy tell you in the video they tell you you have to have like different characters different this and in the company you can just set up six numbers and that's fine“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 38)

„example we are using /. if you're using the swiss government logo or they are available or a (unv., #00:47:56-8#) logo or fedex or i don't know or post it's not fun for post right so people thinking that /. For example if i'm sending an email to post hey dude we were at your office you missed your box click here to register it at the post website and you're just creating negativity towards their logo right. I mean it's not so many companies this is actually a gray area in in the business of security awareness and many companies do not allow that to fall.“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 66)

„Yeah another external influences is actually changing regulations right. Changing regulation uh new privacy act or for example right now suddenly i don't know the american government decided not working with the russians anymore so now we need to update our education your russian team cannot talk to them or i don't know what or you cannot hire freelancers from russia through upwork or i don't know what all this kind of stuff needs to be considered“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 90)

„If you're using external logo you must in some cases some some companies really a must but it is a legal issue we need to consider that's what you said by what do you need to consider should they use external logos or not. Any kind of promises that you're telling an employer any kinds of things that can be“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 101)

„Another aspect of course also with your clients right if you're using some names of your clients you can get your employees to do that. Another legal aspect yeah /. Okay so this is when it starts to the phishing attack to the education we told you it's it can be problematic if you have like all kinds of funny content that shouldn't be there also by the way uh also content that was copied from other places so you need to make sure that the company that is using it also the pictures and so on that we have the ability to use the content. What else?“ (Experte 2 Interview-20230412_Thrievedx_Aufzeichnung, Absatz 101)

„Dann ist man natürlich sehr geneigt dazu, Logos zu verwenden, die Hersteller draußen haben und dann begibt man sich sofort in eine rechtliche Grauzone. Da muss man also wirklich aufpassen, was man dort darf und nicht darf. Diese Abklärungen sind wichtig, Einwilligung von eventuell Einholen draußen.“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 18)

„Ja, also Risiko ist natürlich in dem Sinne Datenschutztechnik, dass man diese Seiten betrachten muss“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 27)

„Das Risiko ist nach wie vor das Thema mit Brandings, eben rechtliche Seite, wo es der Gericht stand. Ich glaube, das wäre dann so ein Thema, falls sich jemand draußen eschoffiert fühlt, hey, das spielt doch stark auf unser Branding ab und man hat /. Man geht Richtung Rechtsstreit, dann sollte man wirklich aufpassen, dass es auch vom Gerichtsstandort dann halt rechtlich dunktioniert. Die rechtlichen Abklärungen im Vorfeld, die sollte man auch nicht unterschätzen, sollte man mache“ (Experte 3 Interview_20230413_ZHAW_Aufzeichnung, Absatz 73)

„Also es gibt Unternehmen, die unterstützen das. Ich weiß zum Beispiel nicht, wie die Banken dazu stehen. Aber grundsätzlich muss auch da mit Fingerspitzengefühl vorgegangen werden und wenn man eine bekannte Marke wieder verwenden möchte in seiner Phishing Simulation, dann muss da die Einverständnis von den Markeninhabern eingeholt werden, na.“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 20)

„Ja, also klar kurz zur Kultur habe ich jetzt schon bisschen was gesagt oder. Rechtliche Einflüsse natürlich Urheberrecht, Markenrecht und so, das muss berücksichtigt werden. Und ja. Also ich find wichtig zu bedenken, dass vielleicht /. Ah ja ich glaube, da können wir später auch noch dazu. Das bleibt ja, wenn ich so einen Phishing Awareness Training mache innerhalb einer Organisation, das bleibt nicht in der Organisation es geht raus!“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 64)

„Nein, nein ich hab da nichts weiter zu ergänzen, eben Markenrecht, Urheberrecht gilt es zu beachten und der Datenschutz haben wir auch gerade gehabt ja“ (Experte 4 Interview-20230411_ZHAW_Aufzeichnung, Absatz 74)

„die Legalität vom dem Ganzen. Wir hatten dort offensichtlich, ich war noch nicht so stark involviert, hatten wir das Problem, dass wir bei diesen Phishing Angriffen "naja" haben wir echte Marken verwendet und unsere Mitarbeiter haben dann diesen echten Marken Mails zukommen

lassen, so von wegen, warum sie uns SPAM zusenden und das konnte dann zu legalrechtlichen Problemen führen, weil eigentlich offensichtlich ist das nicht so toll, wenn man jetzt hingeht und sagt, "jo" ich nehme jetzt das Logo von Amazon für einen Phishing-Angriff zum Beispiel.“ (Experte 5 und 6 Interview-20230405_ZHAW_Aufzeichnung, Absatz 10)

„Also Thema Logomissbrauch, Namensmissbrauch geht in diese Richtung“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 14)

„Was sicher auch noch sein kann, ist zu prüfen, ist mir im Detail so nicht bekannt sind rechtliche Aspekte eben Markenrecht oder ich sag mal sogar strafbare Handlungen, wenn man ich sag jetzt mal ja wenn man ein Phishing macht, wo man jemand verunglimpft, oder sag mal üble Nachrede so einfach rechtliche Geschichte sag ich mal dir sicher geprüft werden müssen und immer wieder mal beachtet werden müssen“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 58)

„bei ausländischen Partnern wird gegebenenfalls die Rechtslage anders sein. Ich meine der Anbieter muss sich grundsätzlich nur wenn Recht seines Landes rechtfertigen. Ähm, kann sein, dass ich sag jetzt mal, wenn das Ding sagt in Russland steht, wo vermutlich nicht ganz so strenge Maßnahmen oder ganz so strenge Richtlinien bestehen und wir das in der Schweiz nutzen.“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 62)

„Könnte ich mir vorstellen das, dass eben wieder betreffend Markenrecht usw. gewisses Potential an Risiko im Sinne von Klagen oder so bestehen, aber ansonsten“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 62)

„Ja Ergänzend. Ich sag mal aus der Praxis sage ich interessiert das die wenigsten die rechtlichen Aspekte müssen aber nichtsdestotrotz beachtet werden, gegebenenfalls helfen da Nachfragen beim Datenschutzbeauftragten und oder bei einer Rechtsabteilung, Rechtsanwalt die auf solche Gebiete spezialisiert sind, kann weiterhelfen. Oder kann"Licht ins Dunkle" bringen“ (Experte 7 Interview-20230405_Datimo_Aufzeichnung_1, Absatz 64)

„wenn ich das mit einer Plattform mache, auf welcher ich die E-Mail-Adressen erfasse, dann muss ich logischerweise überlegen, was sind die Regeln oder die Vorgaben, die meine Firma oder die Industrie hat“ (Experte 8 Interview-20230405_UMB_Aufzeichnung, Absatz 54)