Zürcher Hochschule
Für Angewandte Wissenschaften

School of
Management and Law

Cyberangriffe und IT-Sicherheits-massnahmen in der Schweizer Speditions- und Logistikindustrie

Standortbestimmung im Q1/2023

Erkenntnisse aus einer Masterarbeit am Institut für Wirtschaftsinformatik

Autoren
Reto Nüesch Erismann, Nico Ebert, Tim Geppert

IMPRESSUM

Herausgeber
ZHAW School of Management and Law
Stadthausstrasse 14
Postfach
8401 Winterthur
Schweiz

Institute of Business Information Technology
www.zhaw.ch/en/sml/institutes-centres/iwi/

Projektleitung, Kontakt
Tim Geppert
Tim.geppert@zhaw.ch

Publikationsdatum
Oktober 2023

Download der Publikation
https://doi.org/10.21256/zhaw-2489

Umsetzungspartner:

Überblick

Anlässlich der akuten Bedrohungslage durch Cyberattacken weltweit wurde im ersten Quartal 2023 im Rahmen einer Masterarbeit untersucht, wie sich die aktuelle Situation bezüglich Cyberangriffe und IT-Sicherheitsmassnahmen in der Schweizer Speditions- und Logistikindustrie darstellt. Das Ergebnis wurde anschliessend mit der Situation in der Schweizer Tech-Industrie (Maschinen-, Elektro- und Metall-Industrie sowie verwandte Technologiebranchen) und mit der deutschen Logistik- und Tech-Industrie verglichen.

Es zeigte sich, dass die Unternehmen der Schweizer Speditions- und Logistikindustrie ähnlich, wenn auch technisch und organisatorisch unterschiedlich ausgeprägt, auf Cyberangriffe vorbereitet sind wie die Unternehmen der Schweizer Tech-Industrie. Zudem haben die angegriffenen Unternehmen der Schweizer Speditions- und Logistikindustrie ihre IT-Sicherheitsmassnahmen nach den Angriffen nochmals deutlich verbessert.

Abschliessend wird empfohlen, das Thema Cybersicherheit auf Geschäftsleitungsebene in einem zentralen Risikomanagement zu verankern und dem Faktor Mensch künftig noch mehr Beachtung zu schenken. Insbesondere auf künstlicher Intelligenz basierende Cyberangriffe sind immer schwieriger zu erkennen, weshalb in entsprechende Sensibilisierungsmassnahmen bei den Mitarbeitenden investiert werden sollte, um die Cybersicherheit der Unternehmen zu erhöhen.

Inhaltsverzeichnis

Ziele und Umfragedesign

ZIELE DER BEFRAGUNG

Hauptziel der Befragung war es herauszufinden, wie sich die aktuelle Situation in Bezug auf Cyberangriffe und IT-Sicherheitsmassnahmen in der Schweizer Speditions- und Logistikindustrie darstellt.

VORGEHEN

Nach einer Literaturanalyse, welche die aktuelle Bedrohungslage, den Forschungsstand sowie Trends bei technischen und organisatorischen IT-Sicherheitsmassnahmen ermittelte, wurde eine darauf aufbauende quantitative Querschnittsanalyse in Form einer Online-Befragung durchgeführt. Die in der Schweizer Logistikindustrie erhobenen Daten wurden anschliessend ausgewertet und mit bestehenden Daten des Kriminologischen Forschungsinstituts Niedersachsen zur deutschen Logistik- und Tech-Industrie sowie mit Daten der Schweizer Tech-Industrie verglichen, die das Institut für Strafrecht und Kriminologie der Universität Bern im Auftrag von Swissmem erhoben hatte. Die gewonnenen Erkenntnisse wurden anschliessend in einem Fachgespräch mit Expert:innen der Schweizer Speditions- und Logistikindustrie sowie Vertretern der Fachverbände GS1 Switzerland und Swissmem diskutiert.

UMFRAGEDESIGN

Stichprobe
Die Stichprobe umfasst Unternehmen der Schweizer Speditions- und Logistikindustrie sowie Unternehmen mit relevanten Logistikfunktionen aus allen drei Sprachregionen. Die Umfrage wurde über die Industrienverbände GS1 Switzerland und Spedlogswiss publiziert.

Datenerhebung
Die Unternehmen wurden über die Fachverbände per E-Mail aufgefordert, an der Online-Umfrage teilzunehmen. Im Februar / März 2023 hatten sie rund einen Monat lang Zeit, um die gestellten Fragen zu beantworten. Ergänzend wurde der Teilnahmelink über LinkedIn geteilt.

Fragebogen
Der Fragebogen wurde auf der Basis der bestehenden Umfragen aus der Schweiz und Deutschland und mit Erkenntnissen aus der Literaturrecherche mit Fokus auf Vergleichbarkeit entwickelt.

Analyse und Auswertung
Die Umfrageergebnisse wurden aufbereitet und mit den Datensätzen der Universität Bern und des Kriminologischen Forschungsinstituts Niedersachsen verglichen.

Vorgängerstudien

Die dieser Publikation zugrunde liegende Masterarbeit orientierte sich bezüglich Forschungsdesign und gestellter Fragen stark an den im Folgenden aufgeführten Studien des Kriminologischen Forschungsinstituts Niedersachsen und des Instituts für Strafrecht und Kriminologie der Universität Bern. Beide Institute stellten ihre Umfragedaten zur Verfügung, was einen Vergleich mit der Umfrage in der Schweizer Speditions- und Logistikindustrie ermöglichte.

Cyberangriffe gegen Unternehmen in Deutschland: Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019

Arne Dreißigacker, Bennet von Skarczinski, Gina Rosa Wollinger (2020)

https://kfn.de/wp-content/uploads/Forschungsberichte/FB_152.pdf

Umfassende Studie basierend auf einer CATI-Befragung von 5'000 Unternehmen in Deutschland.

Cyberangriffe gegen Unternehmen in Deutschland: Ergebnisse einer Folgebefragung 2020

Arne Dreißigacker, Bennet von Skarczinski, Gina Rosa Wollinger (2021)

https://kfn.de/wp-content/uploads/Forschungsberichte/FB_162.pdf

Online-Folgebefragung mit Ergebnissen von 687 Unternehmen, die bereits an der CATI-Befragung 2018/2019 teilgenommen haben.

Befragung zur Sicherheit in Unternehmen bezüglich digitaler und physischer Angriffe: Auswertungsbericht zuhanden des Verbands Swissmem

Anna Isenhardt, Louise Frey, Ueli Hostettler (2022)

https://doi.org/10.48350/172496

Online-Umfrage der Universität Bern als Auftragsarbeit für die Swissmem Initiative «Industrie 2025» mit Ergebnissen von 271 Unternehmen der Schweizer Tech-Industrie.

Cybersicherheit − Umfrage zur Bedrohungslage mit Empfehlungen für die Praxis. Swissmem

Initiative Industrie 2025, Swissmem (2023)

https://www.industrie2025.ch/fileadmin/industrie2025/Dokumente/Publikationen/Publikation_Studie_Cybersicherheit_in_der_MEM-Industrie_01.pdf

Zusammenfassung der Umfrageergebnisse der Universität Bern durch die Swissmem Initiative «Industrie 2025».

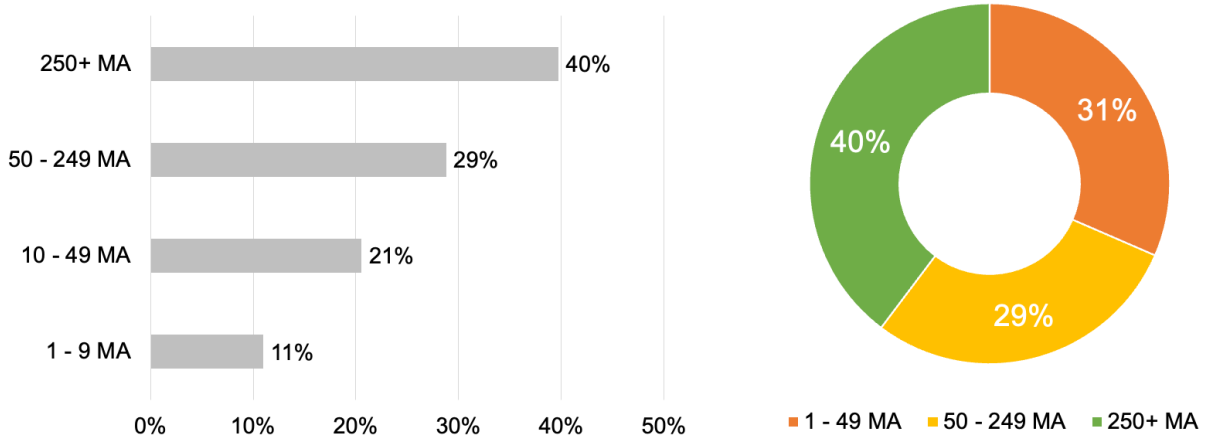
Die Masterarbeit von Reto Nüesch Erismann ist in der ZHAW digitalcollection abrufbar.

Umfrageteilnehmende

Wie die Abbildungen auf dieser Seite zeigen, ist die Studie bezüglich Unternehmensgrösse und Funktionsbereich der Teilnehmenden breit abgestützt. Die Stichprobe für die Online-Umfrage umfasst Unternehmen unterschiedlicher Grössen, wobei insbesondere grosse und mittlere Unternehmen sowie Teilnehmende aus Geschäftsleitungen oder Vorständen überrepräsentiert sind.

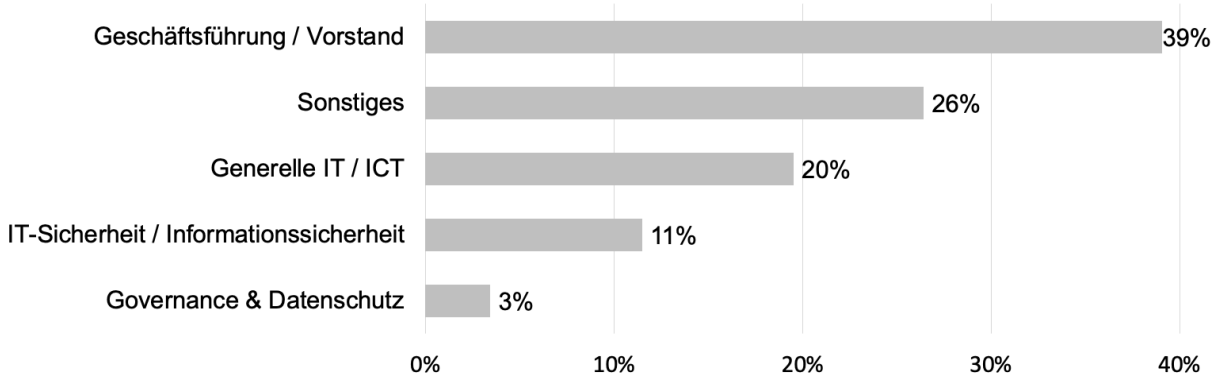
Teilnehmende nach Mitarbeitendenzahl (MA)

N=73



Teilnehmende nach Funktionsbereich

N=73



Die 5 wichtigsten Erkenntnisse

Die Auswertung der Online-Umfrage und des Fachgespräches in der Schweizer Speditions- und Logistikindustrie, sowie der direkte Vergleich mit den vorhandenen Daten aus Deutschland und der Schweiz, führte zu nachfolgenden 5 Erkenntnissen:

WAHRNEHMUNG DER RISIKEN

- Cyberrisiken werden oft von den verantwortlichen Personen als zu tief eingeschätzt, insbesondere von KMU-Geschäftsleitungen, die das Thema Cybersecurity an externe Dienstleister outsourcen.
- Es wird empfohlen, Cyberrisiken in das Risikomanagement zu integrieren und das Risiko von Cyberangriffen als hoch einzustufen.

BEDROHUNG DURCH CYBERANGRIFFE

- Die Schweizer Speditions- und Logistikindustrie unterscheidet sich in Bezug auf Cyberangriffe nur geringfügig von der Schweizer Tech-Industrie und der Situation in Deutschland.
- Der Vergleich zur deutschen Speditions- und Logistikindustrie sowie zur deutschen Tech-Industrie zeigt, dass «CEO-Fraud» in der Schweiz häufiger auftritt als in Deutschland. Es wird vermutet, dass die erhöhte Häufigkeit von «CEO-Fraud-Angriffen» mit der flacheren Hierarchie in Schweizer KMU zu tun hat.
- Die Bedrohungslage könnte sich aufgrund der fortschreitenden Entwicklung im Gebiet der künstlichen Intelligenz, insbesondere in Form schwer erkennbarer «Phishing-Angriffe», verschlechtern.

KOMMUNIKATION DER CYBERANGRIFFE

- Die Schweizer Speditions- und Logistikindustrie zögert, Cyberangriffe proaktiv an Kunden und der Öffentlichkeit zu kommunizieren.
- Die Unternehmen sind sich oft nicht bewusst, dass sie Vorfälle beim Nationalen Zentrum für Cybersicherheit (NCSC) melden sollten.
- Ein vorbereiteter Prozess für die Meldung ans NCSC und die Entwicklung eines Kommunikationskonzepts für verschiedene Angriffe werden empfohlen.

ANWENDUNG VON IT-SICHERHEITSMASSNAHMEN

- Das technische und organisatorische Abwehrdispositiv der Schweizer Speditions- und Logistikindustrie ist auf einem guten Stand.
- Unternehmen der Schweizer Tech-Industrie haben technische IT-Sicherheitsmassnahmen konsequenter umgesetzt als die Speditions- und Logistikindustrie. Diese hat einen leicht höheren Umsetzungsgrad bei organisatorischen IT-Sicherheitsmassnahmen.

STELLENWERT DER MITARBEITENDEN

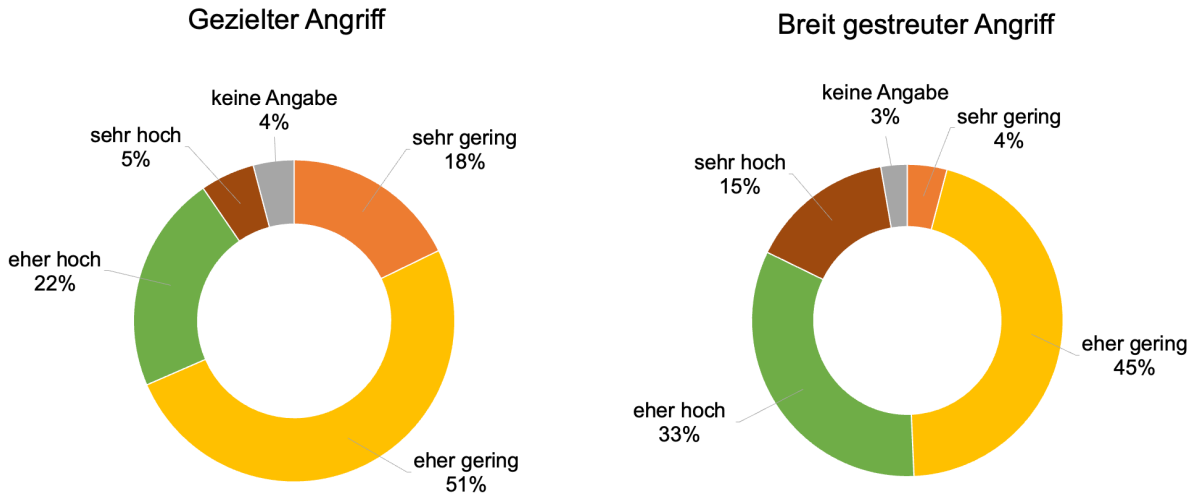
- Die Bedeutung der Mitarbeitenden für die Cyberabwehr ist den Unternehmen erst teilweise bewusst. Das Bewusstsein erhöhte sich jeweils nach einem Angriff und es wurde z.B. in Cyber Awareness Trainings investiert.
- E-Learning ist eine effektive Methode zur Sensibilisierung der Mitarbeitenden. Zusätzlich sollten diese Sequenzen durch individuelle Präsenzschulungen ergänzt werden.

Risikoeinschätzung der Unternehmen

Durchschnittlich gaben 35% der befragten Unternehmen an, ICT-Services ausgelagert zu haben. Trotzdem oder gerade deshalb schätzten 51% der befragten Unternehmen das Risiko, in den nächsten 12 Monaten Opfer eines gezielten Cyberangriffes zu werden, als «eher gering» ein. Auch ein breit gestreuter Cyberangriff wird von 45% der Unternehmen als «eher gering» eingestuft.

Risikoeinschätzung der Unternehmen Oper eines Angriffes zu werden

N=73



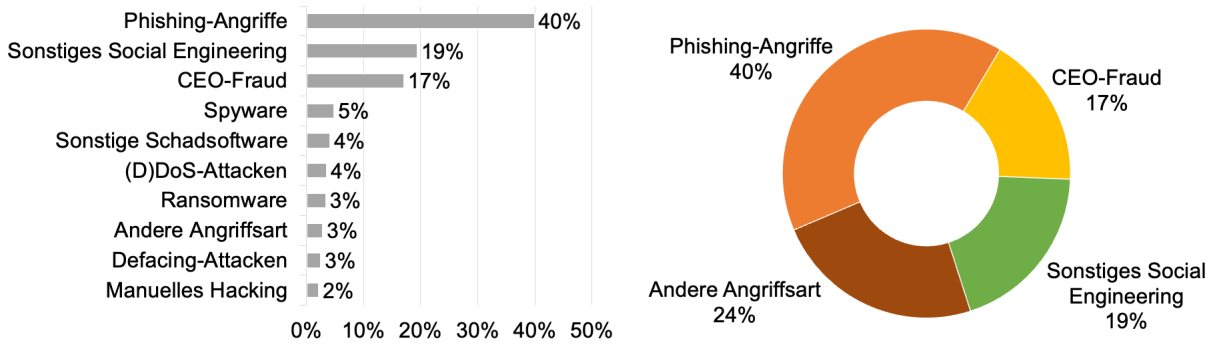
Die Unternehmen nehmen zu 53% an, dass sie aufgrund ihrer Reputation oder ihrem Kundenkreis angegriffen würden. 14% der Unternehmen nehmen an, dass sie aufgrund ihrer besonderen Produkte, Herstellungsverfahren oder Dienstleistungen angegriffen würden.

Cyberangriffe im Zeitraum von 24 Monaten vor der Befragung

Von den teilnehmenden Unternehmen gaben 64% an, seit der Firmengründung einmal oder mehrmals von einem Cyberangriff betroffen gewesen zu sein. Nachfolgend wird die Situation in den 24 Monaten vor der Befragung dargestellt.

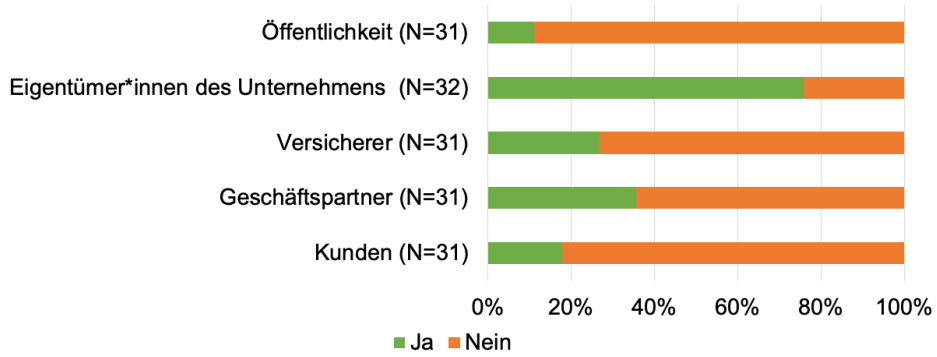
Cyberangriffe im Zeitraum von 24 Monaten vor der Befragung

N=72



45% der Unternehmen waren von mindestens einem Angriff betroffen. Am häufigsten waren mit 40% die «Phishing-Angriffe», gefolgt von «sonstigem Social Engineering» mit 19% und «CEO-Fraud» mit 17%.

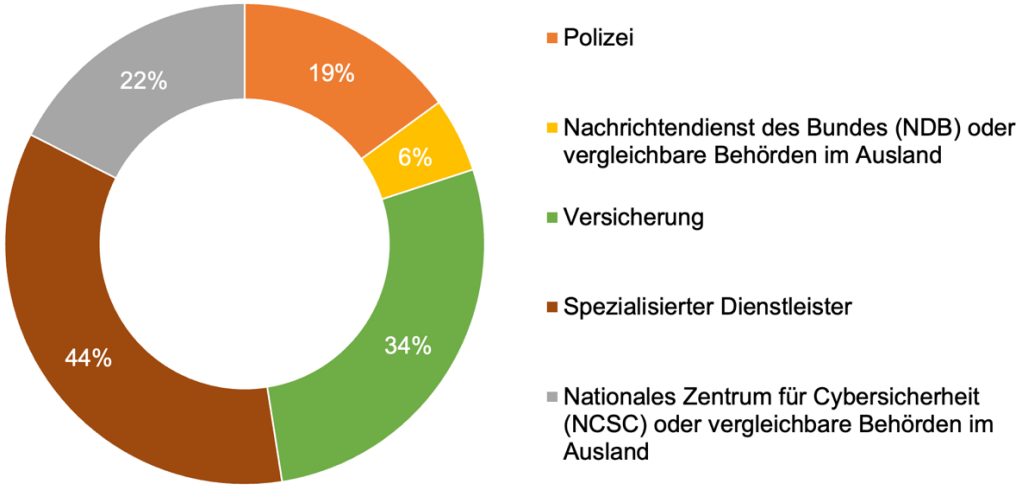
Information nach einem Cyberangriff



Zwei Drittel der betroffenen Unternehmen informierten nach einem Cyberangriff die Eigentümerschaft des Unternehmens. An zweiter Stelle folgten die Geschäftspartner. Die Kunden und die Öffentlichkeit wurden am wenigsten oft informiert.

Kontaktaufnahme nach einem Cyberangriff

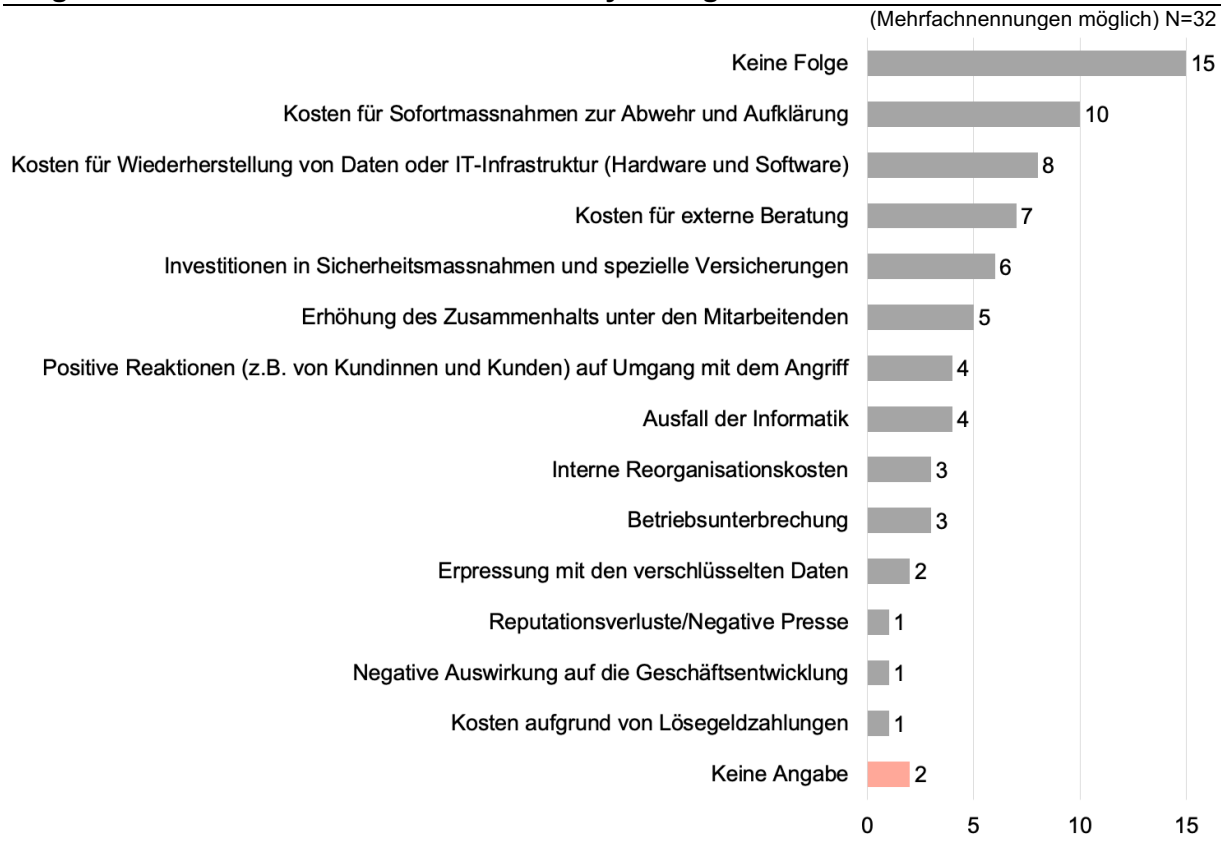
N=32



44% der Unternehmen wandten sich nach dem schwerwiegendsten Angriff an einen spezialisierten Dienstleister. 22% informierten das Nationale Zentrum für Cybersicherheit (NCSC), während 9% die Polizei kontaktierten.

Folgen für das Unternehmen nach einem Cyberangriff

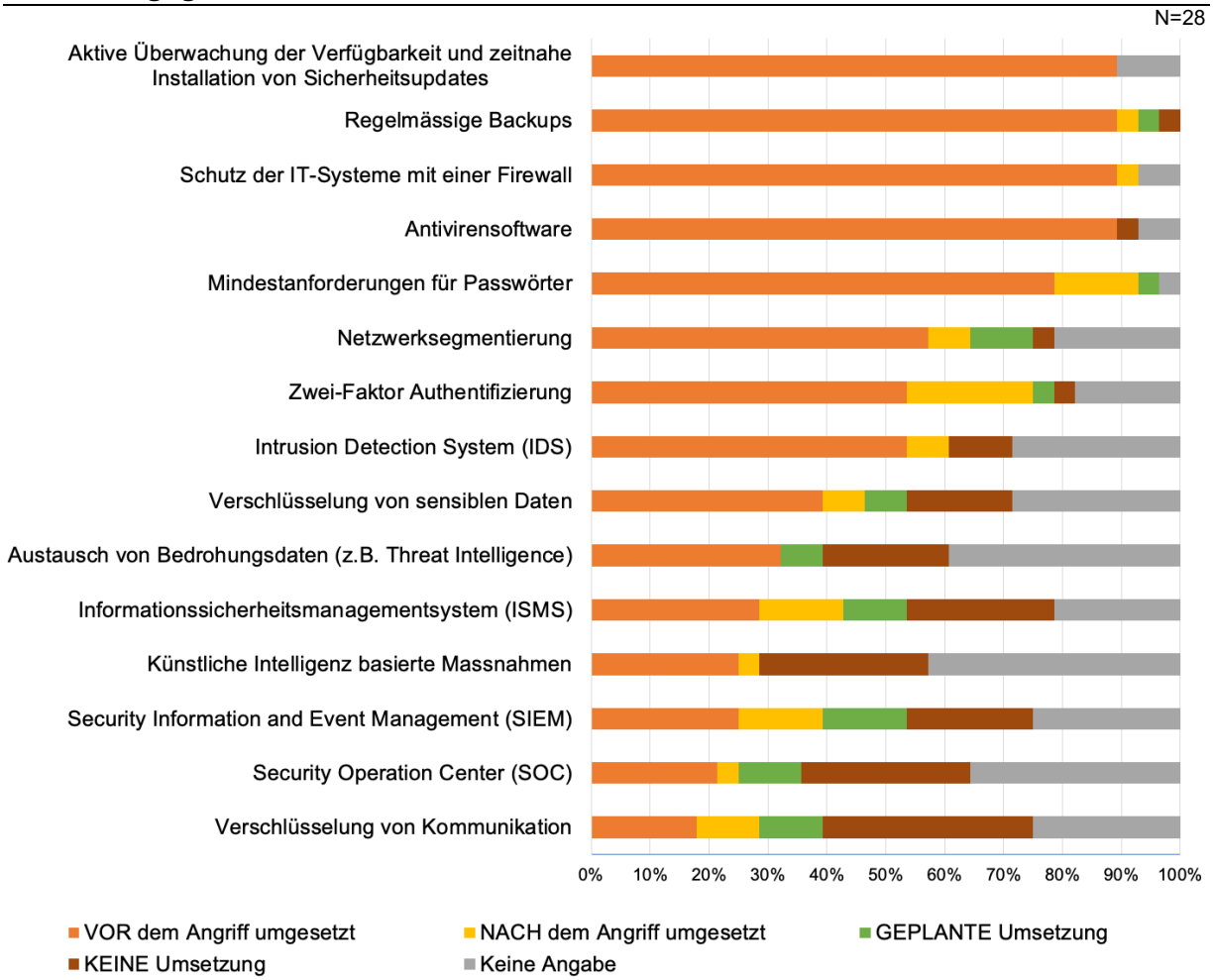
(Mehrfachnennungen möglich) N=32



Für die Hälfte der Unternehmen hatte der Angriff «keine Folgen». Am häufigsten wurden Kostenfolgen für die Wiederherstellung von Daten und IT-Infrastruktur genannt.

Technische Sicherheitsmassnahmen

Umsetzungsgrad der technischen IT-Sicherheitsmassnahmen

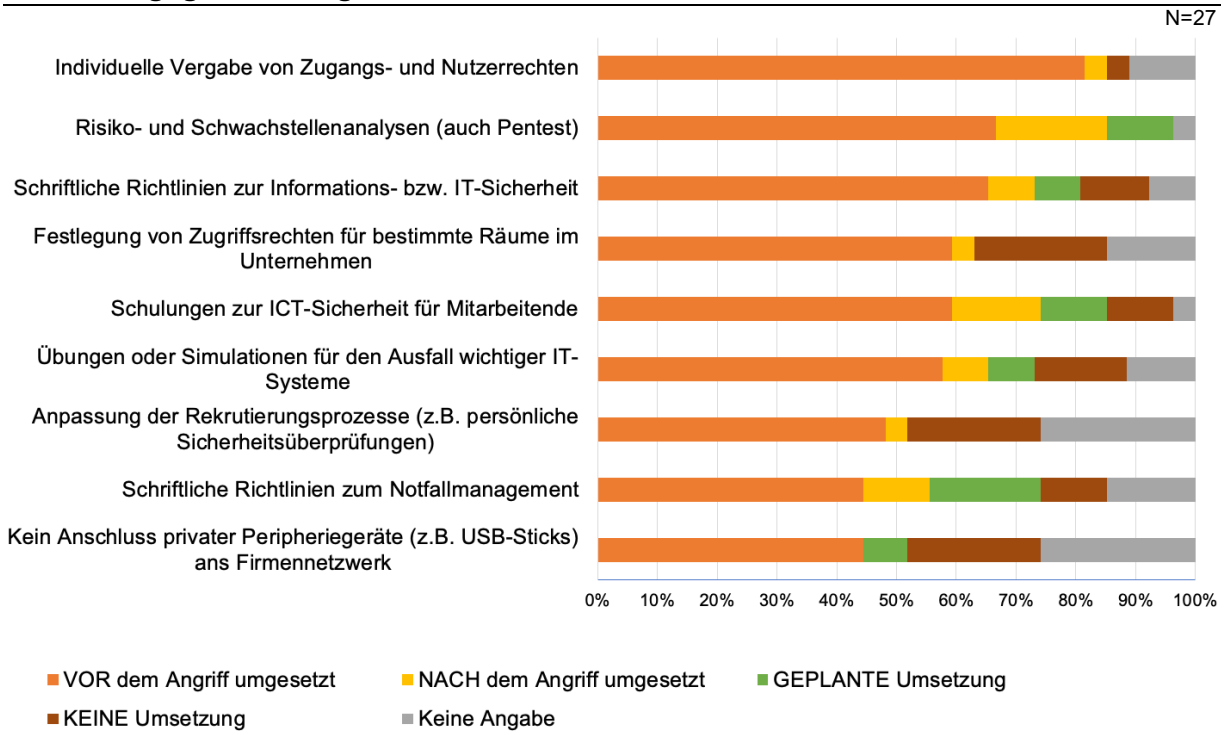


Bereits vor dem Angriff waren in der Speditions- und Logistikindustrie durchschnittlich 53% der 15 technischen IT-Sicherheitsmassnahmen umgesetzt. Nach einem erfolgten Angriff erhöhte sich dieser Umsetzungsgrad auf 60% (inkl. der nach einem Angriff umgesetzten Massnahmen). Dies ist 11% tiefer als ein vergleichbarer Umsetzungsgrad in der Schweizer Tech-Industrie.

Die Umfrage zeigte, dass in der Schweizer Tech-Industrie 9% seltener «Intrusion Detection Systems (IDS)» betrieben, 8% seltener «Netzwerksegmentierungen» vorgenommen und 7% weniger «Informationssicherheitsmanagementsysteme (ISMS)» implementiert wurden als in der Speditions- und Logistikindustrie. Dafür wurden 25% häufiger «Security Information and Event Management (SIEM)» eingesetzt und 12% häufiger auf die «Verschlüsselung von sensiblen Daten» gesetzt.

Organisatorische IT-Sicherheitsmassnahmen

Umsetzungsgrad der organisatorischen IT-Sicherheitsmassnahmen



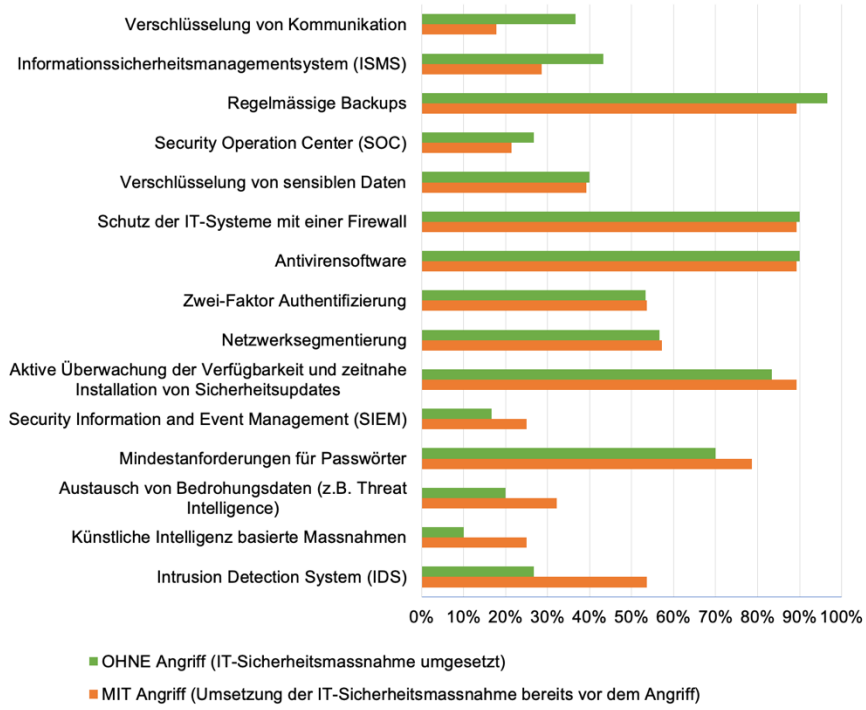
Bereits vor dem Angriff waren in der Speditions- und Logistikindustrie durchschnittlich 59% der organisatorischen IT-Sicherheitsmassnahmen umgesetzt. Nach einem erfolgten Angriff erhöhte sich dieser Umsetzungsgrad auf 66% (inkl. der nach einem Angriff umgesetzten Massnahmen). Dies ist 5% höher als in der Schweizer Tech-Industrie.

Die Umfrage zeigte, dass in der Schweizer Tech-Industrie 29% seltener «Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme» durchgeführt werden, 25% weniger oft «Anpassung der Rekrutierungsprozesse (z.B. persönliche Sicherheitsüberprüfung)» vorgenommen werden und 14% seltener «Risiko- und Schwachstellenanalysen (auch Pentest)» ausgeführt werden als in der Speditions- und Logistikindustrie.

Vergleich von angegriffenen und nicht angegriffenen Unternehmen

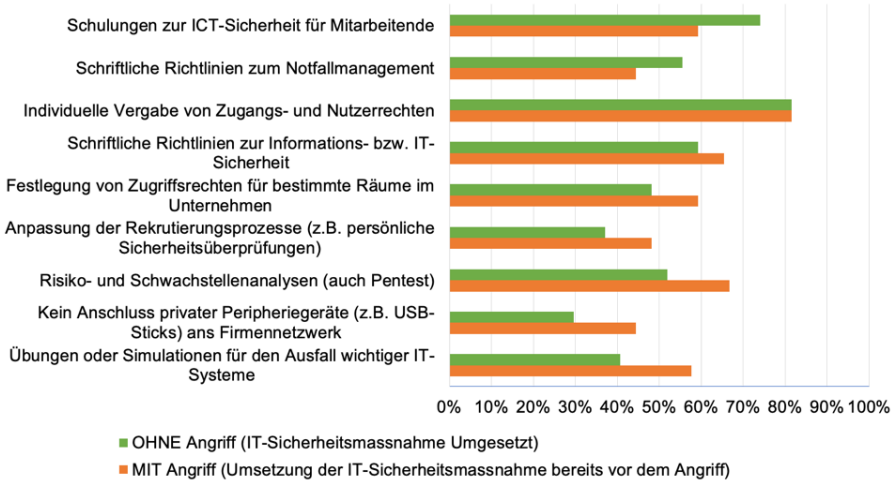
Vergleich des Umsetzungsgrades der technischen IT- Sicherheitsmassnahmen zwischen angegriffenen und nicht angegriffenen Unternehmen

mit Angriff N = 28; ohne Angriff N = 30



Vergleich des Umsetzungsgrades der organisatorischen IT- Sicherheitsmassnahmen zwischen angegriffenen und nicht angegriffenen Unternehmen

mit Angriff N = 28; ohne Angriff N = 30



Der Vergleich der umgesetzten IT-Sicherheitsmassnahmen in angegriffenen und nicht angegriffenen Unternehmen zeigt, dass die nicht angegriffenen Unternehmen u.a. mehr in die «Schulung der Mitarbeitenden», in «schriftliche Richtlinien zum Notfallmanagement» und in ein «Informationssicherheitsmanagementsystem» investiert haben. Dies lässt den Schluss zu, dass eine Sensibilisierung für Cyberrisiken ein wirksames Mittel ist, um Angriffe zu vermeiden.

Fazit

Da die Gelegenheitsstichprobe keine repräsentative Aussage erlaubt, ist weiterführende Forschung notwendig. Insbesondere die Korrelation zwischen technischen und organisatorischen IT-Sicherheitsmassnahmen und der Häufigkeit von erfolgreichen Angriffen sollte weiter untersucht werden.

Zusammenfassend lassen sich jedoch folgende Empfehlungen für die Schweizer Logistikindustrie ableiten:

Bewusstsein für Cyberrisiken in den Geschäftsleitungen schaffen

Geschäftsleitungen gestalten die Rahmenbedingungen und sprechen die Budgets, damit sich eine Cyber- und Informationssicherheitskultur etablieren kann. Dazu sollten alle Mitglieder dieses Führungsgremiums über aktuelles Wissen zum Thema Cybersicherheit verfügen, um die sich stetig ändernde Bedrohungslage beurteilen zu können. Letztere sollte regelmässig an Geschäftsleitungssitzungen traktandiert werden. Dazu sollten auch jüngere Mitarbeitende im Unternehmen und externe Dienstleistungsunternehmen beigezogen werden.

> **«Das Management von KMU wiegt sich oft in falscher Sicherheit.»**
>
> Philip Hauri, Geschäftsleiter Industrie 2025, Swissmem

Integriertes Risikomanagement in den Geschäftsleitungen etablieren

Geschäftsleitungen beurteilen regelmässig die Unternehmensrisiken, indem sie ein Risikomanagementsystem bewirtschaften. Dabei sollten die Cyberrisiken unbedingt eingeschlossen und in kürzeren Zyklen überprüft werden als eher statische Risiken. Diese Aufgabe sollte nicht an den CIO oder ein externes Dienstleistungsunternehmen delegiert werden.

> **«Das Thema Cybersicherheit ist bei KMU auf strategischer Ebene zu wenig verankert.»**
>
> Jan Eberle, Head of Industry Engagement Transport and Logistics, GS1 Switzerland

Nutzung externer Ressourcen

Oft verfügen kleinere und mittlere Unternehmen nicht über die notwendigen Ressourcen, um eine eigene IT-Sicherheitsabteilung zu betreiben. Es ist indes nicht sinnvoll, das Thema Cybersicherheit intern an jemanden im Nebenamt zu delegieren. Vielmehr sollten KMU professionelle Dienstleistungsunternehmen mit der Aufgabe betrauen bzw. fest einbinden, um die Cybersicherheit zu gewährleisten. Spezialisierte Dienstleister sind auch in der Lage, die Systeme rund um die Uhr zu überwachen, was für die Cybersicherheit entscheidend ist.

> **«KMU haben oft das Gefühl, alles selbst machen zu müssen. Doch genau bei diesen Thema gibt es unterdessen sehr gute Dienstleister auf dem Markt, die z.B. «Cyber Awareness Trainings» anbieten...»**
>
> Philip Hauri, Geschäftsleiter Industrie 2025, Swissmem

Risikobasierte und individualisierte «Cyber Awareness Trainings»

Das richtige Verhalten der Mitarbeitenden ist elementar in der Cyberabwehr. Und die Cybersicherheit immer nur so gut, wie das schwächste Einfallstor. Um alle Mitarbeitenden nachhaltig ausbilden zu können, sollten die Vorgesetzten gemeinsam mit den IT-Verantwortlichen das Arbeitsumfeld nach möglichen Cyberrisiken analysieren und daraus individuelle und gegebenenfalls mehrsprachige «Cyber Awareness Trainings» erstellen (z.B. Mitarbeitende der Buchhaltung in der Abwehr von «CEO-Fraud-Angriffen» ausbilden). Dabei sollte ein Augenmerk auf die Vermittlung der Inhalte gelegt werden, denn die Mitarbeitenden sind aufnahmefähiger, wenn das Training abwechslungsreich ist, Spass macht und sich die Teilnehmenden einbringen können.

> **«8'100 Mitarbeitende werden jetzt dann mit einem E-Learning geschult. Dies erfolgt nach jahrelanger massiver Überzeugungsarbeit, dass dies ein Thema für alle Mitarbeitenden ist.»**
>
> Bettina Thurnher, CISO, Gebrüder Weiss GmbH

Cyberangriffe ins «Business Contingency Planning» integrieren

Es sollte ein nach Schweregrad von Cyberangriffen abgestuftes Notfallkonzept erarbeitet werden (Krisenorganisation, aktueller Kundenstamm, externe Partner, Checklisten, Telefonlisten, Kommunikationskonzept, Ersatzgeräte, etc.). Die vorgesehenen externen Dienstleister sollten bei der Erstellung des Konzeptes bereits involviert werden. So kann sichergestellt werden, dass die Zusammenarbeit im Ernstfall funktioniert. Wichtig ist ferner, dass im Kommunikationskonzept eine Meldung an das NCSC vorgesehen ist. Es wird empfohlen, dass die Notfallszenarien nicht nur auf technischer, sondern auch auf organisatorischer Ebene regelmässig überprüft, angepasst und trainiert werden, um im Krisenfall angemessen und rasch reagieren zu können.

> **«Ein Kommunikationskonzept und entsprechende Checklisten sollten vorbereitet werden.»**
>
> Angelo Zaccari, CIO Rhenus Alpina

Danksagungen

Diese Publikation hat von der Zusammenarbeit und Unterstützung einiger Institutionen und Personen stark profitiert. Jenen, die massgeblich zum Gelingen dieser Arbeit beigetragen haben, danken wir an dieser Stelle herzlich:

Arne Dreißigacker vom Kriminologischen Forschungsinstitut Niedersachsen und Anna Isenhardt vom Institut für Strafrecht und Kriminologie der Universität Bern für die grosszügige Bereitstellung der Daten ihrer Umfragen.

Thomas Schwarzenbach von Spedlogswiss und Jan Eberle von GS1 Switzerland, die unsere Online-Umfrage über ihre Mitgliederregister verteilten.

Der Expertin Bettina Turnher und den Experten Jan Eberle, Philip Hauri, Michael Trommer und Angelo Zaccari, die sich zu einem Fachgespräch zur Verfügung gestellt und die Erkenntnisse der Umfrage diskutiert haben.

School of Management and Law

St.-Georgen-Platz 2
Postfach
8401 Winterthur
Schweiz

www.zhaw.ch/sml

AACSB ACCREDITED

swissuniversities

FT FINANCIAL TIMES European Business Schools Ranking 2021