Security to go

TITELTHEMA

MARKTÜBERSICHT MOBILE SICHERHEIT

Der mobile Arbeitsplatz wird in den nächsten Jahren die Arbeitswelt dominieren. Damit entwickelt sich auch eine Vielzahl neuer Mobilgeräte zum integrierten Bestandteil des Unternehmensnetzes. Dies hat natürlich Konsequenzen für die IT-Sicherheit. Schutz vor Datenverlust, Definition sowie Isolation unternehmenswichtiger Informationen sind neue Elemente, die IT-Entscheider in klassische Sicherheitsregeln einbeziehen müssen.

Daniel Liebhart

Bereits heute arbeiten über eine Milliarde Menschen mobil. IDC-Analysten gehen davon aus, dass bereits im nächsten Jahr rund ein Drittel von uns mit Laptops, Tablets oder Smartphones und bald auch mit Uhren oder Datenbrillen von außen auf Firmennetze und Anwendungen zugreifen werden. Und das betrifft sämtliche Berufsgruppen – vom klassischen Außendienst über Sachbearbeiter bis hin zum Fertigungspersonal.

Die Arbeit der Zukunft ist also mobil und damit wird der zugehörige mobile Arbeitsplatz früher oder später zum wichtigsten überhaupt. Dies hat weitgehende Konsequenzen für die unterstützenden IT-Systeme. Sicher mobil arbeiten bedeutet im Klartext, dass bestehende Konzepte zum Schutz sensibler Daten deutlich erweitert werden müssen. Dies wiederum erfordert eine verbesserte Definition und Klassierung businessrelevanter Informationen und deren Verwaltung.

Muster des mobilen Arbeitens

Mobiles Arbeiten stellt aus Unternehmenssicht verschiedene Sicherheitsanforderungen, die aufgrund der Zugangsart auf das Firmennetzwerk unterschieden werden. Je nachdem, ob der Zugang lokal statisch, lokal dynamisch, remote statisch oder remote dynamisch ist: Es sollte zwingend ein entsprechendes Sicherheitsdispositiv vorliegen.

Im einfachsten Fall, dem lokal statischen Zugang durch ein Gerät, das sich im Unternehmensnetz auf dem Firmengelände befindet, sind bestehende Sicherheitsregelungen auch in Zukunft vollkommen ausreichend. Anders sieht es jedoch im Fall eines lokal dynamischen Zugangs aus. Diesen nutzen vor allem Personen, die sich zwar auf dem Firmengelände befinden, dort jedoch ständig unterwegs sind. Selbst wenn die Geräte niemals das Firmengelände verlassen, bestehen zusätzliche Risiken wie beispielsweise der Geräteverlust oder das externe Abhören des WLANs, die es abzudecken gilt.

Dies gilt für die anderen beiden Zugangsarten in besonderem Maße. Remote statischer Zugang durch Personen, die zu Hause oder von Außenbüros zugreifen und Remote dynamischer Zugang durch diejenigen, die ständig unterwegs sind, stellen eine weitere Steigerung des Risikopotenzials dar. Sie benötigen Sicherheitsmechanismen, die einerseits der Zugangsart Rechnung trägt und andererseits ein einfaches mobiles Arbeiten erlaubt.

Risiko = Verlust von Daten

Das größte Risiko des mobilen Arbeitens ist der unbewusste oder bewusste Verlust von unternehmenswichtigen Informationen. Dieser Verlust hat verschiedene Gesichter. Geraten kritische Informationen in falsche Hände, kann dies für eine Firma fatale Auswirkungen haben. Gehen sensitive Daten verloren, die wichtig für das tägliche Arbeiten sind, so kann dies für den Mitarbeitenden und für die Leistungserbringung des Unternehmens Konsequenzen haben.

Verliert jemand Daten, die leicht wiederzubeschaffen sind, so leidet im besten Fall lediglich die Arbeitsproduktivität. Jede dieser Datenverlustarten ist bestenfalls unangenehm für eine Firma. Leider ist es für viele Unternehmen sehr schwierig, überhaupt zwischen kriti-

DER AUTOR

Daniel Liebhart ■ Dozent für Informatik an der Züricher Hochschule für Angewandte Wissenschaften (ZHAW), Experte für Enterprise-Architekturen und Solution Manager der Trivadis AG. Zudem ist er Autor und Co-Autor verschiedener Fachbücher.

STATEMENT

Frank Melber
Head of Business Development Security Solutions, TÜV Rheinland i-sec

Unternehmen brauchen Unterstützung

„Der Trend zur Mobilität von Kommunikation und Business und der Internationalisierung von Unternehmen wird weiter zunehmen. Unternehmen und zunehmend auch Behörden müssen sich im Klaren darüber sein, dass ihre Mitarbeiter immer häufiger vor und nicht hinter der Firewall der Organisation sitzen. Die traditionelle Trennung zwischen Innen = Unternehmensnetzwerk und außen = Internet wird immer mehr aufweichen. Umso wichtiger wird es sein, den Zugang zu internen Services und Web-Applikationen von außen so sicher wie möglich zu gestalten.

Unternehmen, die verstärkt oder überwiegend mit mobilen Geräten arbeiten, empfehlen wir stets vor allem drei Dinge:

1. Definieren Sie Ihren Anspruch an die Sicherheit der Unternehmensdaten auf mobilen Geräten und setzen Sie ihn auch konsequent durch.

2. Kontrollieren und umsetzen lässt sich dies am besten mit einem entsprechenden Mobile-Device-Management-, Mobile-Application-Management- oder Mobile-Content-Management-System.

3. Klären Sie Ihre Benutzer bezüglich Verwendung und Sicherheit von Apps und (Cloud-) Services auf oder schränken sie die Möglichkeiten stark ein.

In vielen Fällen ist es sinnvoll, hier Unterstützung durch auf mobile Sicherheit spezialisierte neutrale Beratungshäuser beziehungsweise Integratoren zu Rate zu ziehen. TÜV Rheinland begleitet Unternehmen von der Konzeption der Mobile Security bis zur Implementierung von MDM-Systemen sowie sicheren Mobile-Filesharing-Lösungen. Bei Bedarf leistet TÜV Rheinland auch Unterstützung mit Managed Security Services."

schen, wichtigen und anderen Daten zu unterscheiden. Zumal gemäß einer Studie der Tower Group zentral strukturierte Daten in größeren Unternehmen im Schnitt elf Mal vorhanden sind. Von den unstrukturierten Daten werden wohl kaum weniger Kopien vorhanden sein, auch wenn im Schnitt lediglich eines von 50 Dokumenten wirklich kritische Daten enthält.

Das Ponemon Institute hat genau untersucht, wie Daten verloren gehen. Weit über die Hälfte aller Unternehmen, die an der entsprechenden Studie teilnahmen, waren von einem Datenverlust betroffen. Nachlässigkeit und Geräteverlust waren die Hauptursachen. Fehler und kriminelle Energie waren lediglich in jeweils etwas mehr als fünf Prozent der Fälle im Spiel. Es gilt also, den bewussten oder unbewussten Verlust von Daten zu vermeiden. Und dies für sämtliche Zugriffsarten durch stationäre und insbesondere mobile Geräte.

Erweiterte Sicherheitsüberlegungen

Datenverluste in der mobilen Arbeitswelt vermeiden, heißt in den meisten Fällen, bestehende Sicherheitsüberlegungen im Hinblick auf den Kontext der Datennutzung, also auf den Datenzugriff zu erweitern oder allenfalls zu überprüfen. Dabei spielt es eine Rolle, ob die Daten zentral gespeichert, innerhalb oder außerhalb des Firmennetzes transportiert oder auf einem dezentralen Gerät gehalten werden. In jedem Szenario gilt es, mögliche Sicherheitsmechanismen möglichst genau abzuwägen. Dazu gibt es eine Vielzahl von Techniken und Methoden, die in Kombination zu einem guten Gesamtergebnis führen können.

Im Falle des Zugriffes auf zentral gespeicherte Daten gilt es, Sichtbarkeit, Zugriff und Sicherheit zu berücksichtigen. Die Sichtbarkeit von Unternehmensinformationen ist nur dann kontrollierbar, wenn bekannt ist, welche Daten wo überall gespeichert sind. Insbesondere muss bekannt sein, welche kritischen und sensitiven Daten sich in welchen Systemen und Infrastrukturen befinden.

Die Kontrolle des Zugriffs erfolgt über eine möglichst exakte Regelung, die exakt festlegt, wer welche Daten wie manipulieren und in welchem der Zugriffsarten die betreffende Person das überhaupt darf. Die Sicherheit der gespeicherten Daten wird durch Verschlüsselung sowie eine redundante Speicherung gewährleistet.

Werden Daten transportiert, so gilt es zunächst einmal, eine unkontrollierte Kommunikation über das Netz zu verhindern – sei es auch via WLAN, Bluetooth oder andere Funktechnologien. Darüber hinaus müssen die Sicherheitsüberlegungen in diesem Fall über die konventionelle Absicherung von Netzwerkverbindungen hinausgehen.

Dabei gilt es vor allem gängige Kommunikationskanäle wie E-Mail, Messaging, Filetransfer und andere konsequent abzusichern. Wichtige Hilfsmittel sind Content Monitoring oder auch Content Scanning – also Techniken, die ähnlich wie Firewalls oder Intrusion-Detection-Systeme funktionieren. Basierend auf einem definierten Regelwerk überwachen und protokollieren sie die Einhaltung vorgegebener Sicherheitsrichtlinien.

Dabei spielt die Zugriffsart eine wichtige Rolle. Der sicherlich am besten abzusichernde Fall stellt das Szenario des remote dynamischen Zugriffs dar. Neben firmeninternen Richtlinien sind für den eigentlichen Datentransport auch länderspezifische Datenschutzbestimmungen einzubeziehen.

Der Verlust mobiler Geräte gilt derzeit als Hauptursache für die unbeabsichtigte Weitergabe sensibler Informationen. Der Schutz kritischer oder sensitiver Daten auf mobilen Geräten muss von der einfachen Verschlüsselung des internen Speichers über Memory Sticks mit automatischen Löschungsmechanismen bis hin zu sich selbst zerstörenden Dateien reichen. Bereits heute existiert dazu eine Vielzahl marktreifer Technologien – für die neuesten Geräte sind sie bereits in Entwicklung.

Eine Frage der Haftbarkeit

Der mobile Arbeitsplatz der Zukunft stellt aber auch neue Anforderung in Bezug auf die Haftungsrisiken. Viele Fragen bezüglich der Haftbarkeit sind eng mit den Besitzverhältnissen des mobilen Gerätes verbunden. Es geht dabei um die finanzielle und gesetzliche Haftbarkeit, die stark davon abhängt, ob das Smartphone oder Tablet von der Firma bereitgestellt wird oder ein privates Gerät zum Arbeiten genutzt wird.

Dass die Kosten für ein privates Smartphone, das vor allem geschäftlich genutzt wird, durch das Unternehmen übernommen werden, ist nachvollziehbar. Es stellt sich jedoch die Frage, wer beispielsweise für anfallene Roaming-Kosten aufkommen muss, die aufgrund eines Konfigurationsfehlers durch den Angestellten entstanden sind. Doch auch ein Extremfall wäre denkbar: Ein Angestellter tätigt illegale Geschäfte mit finanziellen Konsequenzen über ein Firmenhandy – obwohl das Unternehmen sowohl die Verantwortung für das Smartphone als auch für die darauf gespeicherten Daten hat.

Die gesetzlichen Rahmenbedingen verändern die Haftungsregeln je nach Land und Kontinent, was insbesondere für international tätige Unternehmen eine große Herausforderung darstellt. So ist in der Europäischen Union und Japan diejenige Person haftbar, die entsprechende E-Mails nebst Anhängen verfasst hat.

In anderen Ländern sieht dieser Sachverhalt anders aus: In den USA beispielsweise ist die Firma für alle Unternehmensdaten verantwortlich, die durch Mitarbeiter auf dienstlichen Geräten gespeichert werden. Dies gilt auch für E-Mails – und das unabhängig davon, ob es sich um private oder um geschäftliche Korrespondenz handelt.

Fazit: Was zu tun ist

Um die Vorteile mobiler Arbeitsplätze sicher nutzen zu können, sollten Unternehmen die Integration sämtlicher Mobilgeräte technisch und organisatorisch gut vorbereiten. Dabei ist es ratsam, bestehende Sicherheitsdispositive zu überdenken und auf zu verwendende Handys, Smartphones und Tablets auszudehnen.

Die Sicherheit der Firmendaten sollte oberste Priorität genießen – vom eigentlichen Zugriff über den Tansport bis hin zu Vorkehrungen für einen möglichen Geräteverlust. Schutzbedürfnisse und Haftungsbedingungen sind für alle vier Zugangsarten auf das Unternehmensnetz zu prüfen und gegebenenfalls mit geeigneten Richtlinien, Methoden und Techniken abzusichern.

In der Praxis hat sich dazu ein schrittweises Vorgehen bewährt: Ausgehend vom lokal statischen Zugang durch stationäre Geräte, der als Nächstes den remote statischen Zugang absichert, um schließlich den lokal dynamischen und einen sicheren remote dynamischen Zugang zu gewährleisten. Darüber hinaus sollten die Mitarbeiter über Vorteile und Konsequenzen mobilen Arbeitens informiert und in enger Abstimmung mit dem Management möglichst exakte Regelungen geschaffen werden.

[rm]

Das mobile Business bringt eine Reihe von Sicherheitsrisiken mit sich, die beherrscht werden müssen.