Sicherheit im Home Office und unterwegs

Know-how Wenn Mitarbeitende unterwegs oder zuhause auf Firmendaten zugreifen, haben Unternehmen ohne entsprechende Massnahmen nur ungenügenden Einfluss auf die Sicherheit. Es braucht deshalb neue Ansätze bei der Cybersicherheit.

Von Patrick Trevisan

Bei Unternehmen, deren Mitarbeitende ausschliesslich im firmeneigenen Büro arbeiten, ist das Thema IT-Sicherheit üblicherweise klar definiert. Die interne IT-Abteilung oder ein externer Dienstleister ist für die Verwaltung der Endgeräte wie PCs oder Laptops zuständig. Trotzdem besteht in Sachen Cybersecurity bei vielen Firmen noch deutliches Entwicklungspotenzial. Wenn man es richtig machen will, müssen zum Beispiel nicht nur die Rechner von der IT verwaltet werden, auch Smartphones oder Tablets gehören dazu – mit einem Mobile-Device-Management (MDM)- respektive einem Unified-Endpoint-Mangement (UEM)-System. Das gilt sowohl für geschäftliche als auch private Geräte (Bring your own Device). Sobald ein Gerät für den geschäftlichen Einsatz genutzt wird, bedarf es eines gewissen Grundschutzes.

Obwohl MDM-Systeme kein Garant für IT-Sicherheit sind, lassen sich doch bereits einige grundsätzliche Einstellungen diesbezüglich vornehmen. Zum Beispiel müssen private und geschäftliche Apps und Daten getrennt sowie verschlüsselt werden und geschäftliche Apps im Falle einer Kompromittierung des Geräts oder der Datenverbindung sofort entfernt werden können. Darüber hinaus führt man mit einem MDM-System quasi Inventar über die Geräte. Es ist transparent, welches Gerät welchem Mitarbeitenden zugewiesen ist und ob es die aktuellen Vorgaben in Sachen Sicherheit, Betriebssystemversion und andere Kriterien erfüllt. Richtlinien, Konfigurationen und Apps werden ohne Zutun der User und ohne deren Privatsphäre zu verletzten an die Geräte ausgerollt.

Umdenken in Sachen IT-Sicherheit

Nur noch bei einer Minderheit der Unternehmen arbeiten die Mitarbeitenden heute jedoch ausschliesslich in den Räumlichkeiten der Firma. Hybride Arbeitsplatzmodelle sind die Regel. Wenn die Mitarbeitenden von verschiedenen Standorten ausserhalb des Firmennetzes – dem Home Office, in öffentlichen WLAN oder im Coworking-Space – arbeiten, verlieren die Verantwortlichen in Unternehmen allerdings die vollständige Kontrolle über die Sicherheit der Geräte, der Datenverbindungen und damit die Wahrung der Daten- und Informationssicherheit.

Hinzu kommt, dass immer mehr Unternehmen eine Cloud-Strategie verfolgen. Das Datacenter ist im Internet und damit nicht mehr oder nur noch teilweise hinter der Firewall des Unternehmens geschützt. Dass die Mitarbeitenden von überall her und von verschiedenen Geräteplattformen mit unterschiedlichen Betriebssystemen auf das Firmennetzwerk zugreifen, macht aufgrund der Dezentralisierung den Schutz der Daten nicht einfacher. Deshalb muss bei der Arbeitsplatzverwaltung und der IT-Sicherheit ein Umdenken stattfinden.

Modernes Workplace Management

Beim Modern Workplace Management liegt der Schwerpunkt auf der Bereitstellung eines flexiblen, effizienten und produktiven Arbeitsplatzes, der an die sich ändernden Geschäftsanforderungen und die sich stetig weiterentwickelnde digitale Landschaft angepasst werden kann. Doch wie sollen Unternehmen mit diesen veränderten Voraussetzungen konkret umgehen? Welche Strategien und Konzepte sollen eingesetzt werden, damit die Unternehmensdaten in der Cloud sicher und der Zugriff der Endbenutzer aus unbekannten Netzwerken und von allen möglichen Endgeräten aus sicher und ohne Kompromittierung oder Compliance-Verletzungen stattfinden kann?

Das Ziel von Modern Workplace Management ist es, ein nahtloses und integriertes Arbeitsplatzerlebnis für die Mitarbeitenden zu schaffen. Die wohl wichtigsten Aspekte sind sicherlich der Schutz der Privatsphäre der Mitarbeitenden und die Sicherheit der Unternehmensdaten. Die IT-Security soll dabei aber nicht die Produktivität und das Benutzererlebnis beeinträchtigen, sondern sich in die bereitgestellten Services und Business-Prozesse einbinden.

Eines ist klar: Altbewährte Schutzkonzepte für nomadisches Arbeiten und die Cloud anzuwenden, ist sicherlich nicht optimal. Denn es bringt oft Umgehungslösungen mit sich, und die Gefahr von Schatten-IT nimmt zu. Stattdessen sind neuartige Konzepte wie die der Zero-Trust-Sicherheitsarchitektur gefragt. Man muss davon ausgehen, dass alles im Netzwerk eine potenzielle Bedrohung darstellt. Zugriffe auf Anwendungen können erst genehmigt werden und erfolgen, wenn eine Verifizierung stattgefunden hat: Identität, Gerätestatus und Kontext müssen verifiziert und die nötigen Richtlinien kontrolliert und durchgesetzt werden.

Smartphone als Trust-Anker

In diesem Zusammenhang kommt das eingangs erwähnte Smartphone ins Spiel. Denn mittlerweile gilt das Smartphone für die meisten mobil arbeitenden Menschen auch als Arbeits-

gerät. Viele Unternehmen ermöglichen ihren Mitarbeitenden, ihr eigenes privates Gerät in die IT-Infrastruktur einzubinden oder geben ein COPE-Geschäftsgerät (Corporate Owned Privately Enabled) ab, welches meistens auch privat benutzt werden darf. Business-Prozesse für das Konsumieren und Schreiben von Daten werden zur Verfügung gestellt, um die Arbeit von überall her effizienter zu gestalten und die Mitarbeitenden besser zu informieren. Weshalb diese Geräte also nicht gleich auch für die IT-Sicherheit einsetzen?

Die Idee ist die folgende: Die Smartphones werden via ein MDM/UEM-System verwaltet. Dabei werden unter anderem und wie bereits erklärt die privaten und geschäftlichen Daten und Apps voneinander getrennt und damit dem Datenschutz und Datenverlust vorgebeugt. Besonders wichtig ist dabei auch, dass die Kommunikation mit allfälligen hausinternen Systemen im eigenen Netzwerk oder mit geschäftlichen Cloud-Diensten verschlüsselt erfolgt. Gleichzeitig hat das Unternehmen die Hoheit über die geschäftlichen Daten und Apps und kann diese, wenn nötig, jederzeit vom Gerät abziehen. Das Smartphone stellt durch die eindeutige Zuweisung an einen einzigen Mitarbeitenden aber auch seine Identität dar. Es besteht bereits eine Art «Vertrauensverhältnis» zwischen dem Gerät und dem Unternehmen. So kann das Smartphone ebenfalls als Trust-Anker für verschiedene Use Cases dienen und die Geschäftsabläufe mit einwandfreien und gleichzeitig benutzerfreundlichen Sicherheitsfunktionen anreichern.

➤ **Das Smartphone als Identität für eine sichere Authentifizierung**
Unternehmen verlassen sich weiterhin häufig auf die altmodische Authentifizierung mittels Passworteingabe. Passwörter werden mittlerweile in der IT-Security als eine der unsichersten Komponenten angesehen. Darüber hinaus sind kontinuierliche Passworteingaben und regelmässige Passwortänderungen ineffizient und vor allem benutzerunfreundlich. Mit dem persönlich zugewiesenen Smartphone des Mitarbeitenden können Biometrie, Zertifikate und Apps genutzt werden, um alle Kriterien für eine sichere Authentifizierung ohne Passwort zu erfüllen. Anstelle der Eingabe von Passwörtern werden bei Authentifizierungsanfragen eine Kombination von verschiedenen Kriterien wie zum Beispiel Geräteidentität, Gesichtserkennung, Fingerabdruck und Push-Benachrichtigun geprüft. Der Zugriff auf die Daten hängt somit von einer Multi-Faktor-Authentifizierung (MFA) ab und wird nur gewährt, wenn die Kriterien gemäss eingestellter Richtlinie erfüllt werden. Der Mitarbeitende kann dank seines Smartphones auch auf eine Authentifizierung mittels Single Sign On (SSO) zählen. Die Services werden dadurch nicht nur sicherer, sondern auch benutzerfreundlicher.

➤ **Das Smartphone als Perimeter für eine sichere Kommunikation**
Mit dem Smartphone hat man den persönlichen Zugriffspunkt für eine sichere Kommunikation ins Internet und vor allem für den Zugriff auf die Geschäftsdaten immer mit dabei. Es ist auch kontinuierlich mit dem Internet verbunden. Wieso diese Gegebenheit nicht nutzen und das Gerät als Perimeter für andere Geräte (Laptops oder Tablets) zur Verfügung stellen? Die Kommunikation wird zusätzlich verschlüsselt und der Zugriff auf die Geschäftsdaten wird auf den Perimeter via Smartphone beschränkt. Dies spart ausserdem Ressourcen und Zeit für die Beschaffung und den Unterhalt von Drittherstellter-VPN-Lösungen oder anderen Komponenten.

➤ **Das Smartphone als Zutrittskarte**
Zu guter Letzt kann das Smartphone auch als Schlüssel für das Büro dienen. Schlüssel oder Zutrittskarten gehen oft verloren oder werden zu Hause vergessen. Dies führt zu grossem Zusatzaufwand, wenn Ersatzkarten ausgestellt oder gar die Schlösser ausgewechselt werden müssen. Durch die Einführung eines Zutrittssystems mit NFC-Sensor kann der Trust-Anker auch gleich als Zutrittskarte für geschäftliche Smart Offices oder entsprechend ausgerüstete Coworking-Arbeitsplätze verwendet werden.

Smartphone oder Firmen-Router fürs Home Office

Sobald Mitarbeitende von ausserhalb auf Systeme mit Unternehmensinformationen zugreifen, verlieren Firmen, wie bereits erwähnt, die Kontrolle über die Einhaltung der Sicherheitsanforderungen. Denn private Heimnetze, öffentliche WLAN oder Netze in nicht firmeneigenen Büros können jederzeit Opfer von Cyberangriffen werden.

Wenn Unternehmen eine Cloud-First-Strategie fahren, aber selbst wenn auch nur Teile der Unternehmens-IT in der Cloud vorgehalten werden, ist es technisch nicht sinnvoll, veraltete Methoden wie beispielsweise VPN (virtuelle private Netze) zu verwenden, um sich vor entsprechenden Gefahren zu schützen. Denn es macht aus technischer Sicht keinen Sinn, den Netzwerkverkehr über VPN in die Firmeninfrastruktur hinein und von dort wieder zurück ins Home Office oder das Coworking-Büro zu leiten. Ein vom Unternehmen verwalteter Zugangspunkt ins Internet, sei dies nun ein Smartphone oder ein Extra-Router im Home Office, erlaubt es viel besser, die Sicherheitsanforderungen des Unternehmens über den Büroarbeitsplatz hinaus auch ausserhalb aufrechtzuerhalten. Die Kommunikation kann so direkt via Internet in die Cloud gesteuert und abgesichert werden.

Mit dem Smartphone als Trust-Anker oder einem von der IT gemanagten Heim-WiFi-Service benötigen die Mitarbeitenden zudem keine technischen Vorkenntnisse. Die Unternehmen können so beim Management der mobilen Arbeitsplätze auf benutzerfreundliche Weise die Informations- und Datensicherheit sowie die nötige Privatsphäre gewährleisten. ■

DER AUTOR

Patrick Trevisan ist Mobile Security Consultant und Head of Product Management bei Nomasis, einem auf Lösungen und Services für Cybersecurity und Enterprise Mobility spezialisierten Schweizer Dienstleister. Das Unternehmen bietet Managed Services in den Bereichen Cybersecurity, Modern Workplace, Infrastruktur, Cloud- und End-User-Services an. Vor seiner Zeit bei Nomasis war Trevisan unter anderem bei der Zürcher Kantonalbank und bei Swiss Re als System Engineer und Business Engineer tätig.