Mit dem Smartphone sicher unterwegs arbeiten

Ohne entsprechende Massnahmen haben Unternehmen ungenügenden Einfluss auf die Sicherheit, wenn Mitarbeitende ausserhalb des Firmenbüros arbeiten. Es braucht neue Ansätze bei der Cybersicherheit.

VON PATRICK TREVISAN

Bei Unternehmen ist für die Cybersicherheit entweder die interne IT-Abteilung oder ein externer Dienstleister für die Verwaltung der Endgeräte wie PCs, Laptops, Smartphones oder Tablets zuständig. Zwar besteht auch hier bei vielen Unternehmen noch Entwicklungspotenzial. Wenn man es aber richtig machen will, müssen nicht nur die Rechner, sondern auch Smartphones oder Tablets von der IT verwaltet werden – mit einem MDM (Mobile Device Management)- respektive UEM-System (Unified Endpoint Management). 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 keine Garantie für IT-Sicherheit bieten, lassen sich doch bereits einige grundsätzliche Einstellungen diesbezüglich vornehmen: Zum Beispiel müssen private und geschäftliche Apps und Daten getrennt und verschlüsselt werden und geschäftliche Apps müssen im Falle einer Kompromittierung des Geräts oder der Datenverbindung sofort entfernt werden. 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 verletzen an die Geräte ausgerollt.

Veränderte Voraussetzungen bei der IT-Sicherheit

Wenn Mitarbeitende ausserhalb des Firmennetzes – im Homeoffice, in öffentlichen WLANs oder im Co-Working-Space arbeiten –, verlieren Sicherheitsverantwortliche die Kontrolle über die Sicherheit der Geräte, der Datenverbindung und damit die Wahrung der Daten- und Informationssicherheit. Hinzu kommt, dass immer mehr Unternehmen eine Cloud-Strategie verfolgen. Das «Datencenter» ist im Internet und

FOTO: UNSPLASH.COM


SLO-MO
VIDEO
PHOTO
PORTRAIT
PANO

IT-SICHERHEIT

Web-Shell-Angriffe als neue Top-Bedrohung

Die Zahl von Angriffen über Web-Shells ist in den ersten drei Monaten 2023 überdurchschnittlich stark angestiegen. Laut Analysen von Cisco Talos war diese Angriffsform für ein Viertel aller Vorfälle verantwortlich.

Laut dem Threat-Intelligence-Unternehmen Cisco Talos waren öffentlich zugängliche Web-Applikationen ein Hauptziel der Bedrohungsakteure im ersten Quartal 2023. Nahezu die Hälfte aller Angriffe (45%) nutzen solche Anwendungen als initialen Vektor, um sich Zugang zu Systemen zu verschaffen. Gegenüber dem Vorquartal entspricht dies einem Anstieg von 15%. Bei vielen dieser Angriffe kamen Web-Shells zum Einsatz, die über das Internet zugängliche Server kompromittierten. Generell gesprochen handelt es sich bei einer Web-Shell um ein schädliches Skript, das sich als legitime Datei ausgibt und so eine Hintertür zum Webserver öffnet. Web-Shells werden in der Regel nach einer bereits erfolgreichen Infiltration für weitere Attacken «hinterlassen». Laut den Talos-Forschern profitierten Angreifer von der Tatsache, dass viele Nutzerkonten von Web-Applikationen nur mit schwachen Passwörtern oder Single-Factor-Authentifizierung geschützt waren.
Die Bedrohung durch Ransomware bleibt aber hoch. Auch wenn Cisco Talos im ersten Quartal 2023 einen generellen Rückgang erfolgreicher Erpressungsfälle beobachten konnte, bleiben Ransomware-Aktivitäten insgesamt hoch. Sogenannten «Pre-Ransomware»-Aktivitäten machten zirka ein Fünftel aller Attacken aus, sodass in den nächsten Monaten wieder mit einem Anstieg der erfolgreichen Angriffe gerechnet werden kann. Viele der vorbereitenden Angriffsmassnahmen konnte Cisco Talos bekannten Ransomware-Gruppen wie Vice Society zuordnen. Nach Einschätzung der Forscher hat das schnelle Eingreifen der Security-Teams der Opferunternehmen dazu beigetragen, Angriffe einzudämmen, bevor die Verschlüsselung stattfinden konnte. Im ersten Quartal 2023 war vor allem das Gesundheitswesen Ziel der Kriminellen, dicht gefolgt vom Einzelhandel, der Immobilienbranche und dem Gastgewerbe.
Doch es gibt auch erfreulichere Nachrichten: Aktuelle Erfolge der Strafverfolgungsbehörden zur Zerschlagung grosser Ransomware-Banden (z.B. Hive) zeigen Wirkung. Allerdings schafft dies Raum für neue Familien oder die Bildung neuer Partnerschaften. So trat mit Daixin Ransomware in Q1/2023 eine neue Ransomware-as-a-Service (RaaS)-Familie in Erscheinung.

Quelle: www.cisco.com

Cybersicherheit: die Top-Bedrohungen im ersten Quartal 2023.

damit nicht oder nur teilweise hinter der Firewall des Unternehmens geschützt.

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. Die wichtigsten Aspekte eines modernen Workplace-Managements sind der Schutz der Privatsphäre der Mitarbeitenden und die Sicherheit der Unternehmensdaten. Die IT-Security soll dabei nicht die Produktivität und das Benutzererlebnis beeinträchtigen, sondern sich in die bereitgestellten Services und Business-Prozesse einbinden. 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, das 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

Mittlerweile gilt das Smartphone für die meisten mobil arbeitenden Menschen auch als Arbeitsgerät. Weshalb es dann nicht gleich auch für die IT-Sicherheit einsetzen? Und das geht folgendermassen: Die Geräte werden via ein MDM/UEM-System verwaltet. Dabei werden die privaten und geschäftlichen Daten und Apps voneinander getrennt und damit dem Datenschutz und Datenverlust vorgebeugt. Wichtig ist 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 vom Gerät abziehen. Das Smartphone stellt aber durch die eindeutige Zuweisung an einen einzigen Mitarbeitenden auch seine Identität sicher. Das Smartphone kann als Trust-Anker für verschiedene Use Cases dienen und so die Geschäftsabläufe mit einwandfreien und gleichzeitig benutzerfreundlichen Sicherheitsfunktionen anreichern.

«Man muss davon ausgehen, das alles im Netzwerk eine potenzielle Bedrohung darstellt.»

Wenn Mitarbeitende von ausserhalb auf IT-Systeme zugreifen, verlieren Unternehmen die Kontrolle über die Einhaltung der Sicherheitsanforderungen.

- **Das Smartphone als Identität für sichere Authentifizierung:** Unternehmen verlassen sich weiterhin auf die altmodische Authentifizierung mittels Passworteingabe. Passwörter werden mittlerweile aber als eine der unsichersten Komponenten angesehen. Darüber hinaus sind kontinuierliche Passworteingaben und regelmässige Passwortänderungen ineffizient und vor allem benutzerunfreundlich. Mit dem persönlich zugewiesenen Smartphone 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 verschiedener Kriterien wie zum Beispiel Geräteidentität, Gesichtserkennung, Fingerabdruck, Push-Benachrichtigung usw. geprüft. Der Zugriff auf die Daten hängt somit von einer Multi-Faktor-Authentifizierung (MFA) ab. Der Mitarbeitende kann auf eine Authentifizierung mittels Single Sign On (SSO) zählen. Die Services werden dadurch nicht nur sicherer, sondern auch benutzerfreundlicher.
- **Das Smartphone als Perimeter für 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.
- **Das Smartphone als Zutrittskarte:** Das Smartphone kann auch als Schlüssel für das Büro dienen. Schlüssel oder Zutrittskarten gehen oft verloren oder werden zu Hause vergessen. Durch die Einführung eines Zutrittssystems mit NFC-Sensor kann der Trust-Anker auch gleich als Zutrittskarte für geschäftliche Smart Offices oder entsprechend ausgerüstete Co-Working-Arbeitsplätze verwendet werden.

Gleiche IT-Sicherheit wie in der Firma

Wenn Mitarbeitende von ausserhalb auf IT-Systeme zugreifen, verlieren Unternehmen die Kontrolle über die Einhaltung der Sicherheitsanforderungen. Wenn Unternehmen eine «Cloud First»-Strategie fahren, aber selbst wenn 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. Denn es macht aus technischer Sicht keinen Sinn, den Netzwerkverkehr über VPN in die Firmeninfrastruktur hinein und von dort wieder zurück ins Homeoffice oder das Co-Working-Büro zu leiten. Ein vom Unternehmen verwalteter Zugangspunkt ins Internet, sei dies nun ein Smartphone oder ein extra Router im Homeoffice erlauben es, die Sicherheitsanforderungen des Unternehmens auch ausserhalb aufrechtzuerhalten. Die Kommunikation kann so direkt via Internet in die Cloud gesteuert und abgesichert werden. Mit dem Smartphone als Trust-Anker oder auch einem von der IT gemanagten Heim-Wifi-Service benötigen die Mitarbeitenden keine technischen Vorkenntnisse. Die Unternehmen können so auf benutzerfreundliche Weise ihre Daten und die ihrer Mitarbeitenden voneinander trennen und die Informations- und Datensicherheit sowie die nötige Privatsphäre gewährleisten.

Autor

Patrick Trevisan ist Mobile Security Consultant und Head of Product Management bei Nomasis. Dieses Schweizer Unternehmen bietet Managed Services in den Bereichen Cyber Security, 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.

> *www.nomasis.ch*