Das Smartphone ist der Trust-Anker für sicheres Arbeiten von unterwegs

Wenn Mitarbeitende ausserhalb des Firmenbüros arbeiten, haben Unternehmen ohne geeignete Massnahmen nur ungenügenden Einfluss auf die Sicherheit ihrer Daten. Es braucht deshalb neue Ansätze bei der Cybersicherheit.

DER AUTOR

Patrick Trevisan
Mobile Security Consultant und Head of Product Management, Nomasis

Den Beitrag finden Sie auch online
www.netzwoche.ch

Wenn Mitarbeitende 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 damit nicht oder nur teilweise hinter der Firewall des Unternehmens geschützt. Es sind deshalb neuartige Konzepte wie die der Zero-Trust-Sicherheitsarchitektur gefragt. 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.

BILD: PRODUCTION PERIG - STOCK.ADOBE.COM

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? Bei der Geräteverwaltung mittels eines MDM-Systems (Mobile Device Management) werden private und geschäftliche Daten und Apps voneinander getrennt und so dem Datenschutz und Datenverlust vorgebeugt. Ausserdem erfolgt die Kommunikation mit möglichen hausinternen Systemen im eigenen Netzwerk oder mit geschäftlichen Cloud-Diensten verschlüsselt. Das Smartphone stellt aber durch die eindeutige Zuweisung an einen einzigen Mitarbeiter auch seine Identität sicher. Es kann damit als «Trust-Anker» für verschiedene Use Cases dienen.

• **Das Smartphone als Identität für sichere Authentifizierung:** 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 wird bei Authentifizierungsanfragen eine Kombination von verschiedenen Kriterien wie etwa Geräteidentität, Gesichtserkennung, Fingerabdruck oder Push-Benachrichtigung geprüft. Der Zugriff auf die Daten hängt somit von einer Multi-Faktor-Authentifizierung ab. Mitarbeitende können auf eine Authentifizierung mittels Single Sign-On 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.

• **Das Smartphone als Zutrittskarte:** Durch die Einführung eines Zutrittssystems mit NFC-Sensor kann der Trust-Anker auch gleich als Zutrittskarte für geschäftliche Smartoffices 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, selbst wenn nur Teile der Unternehmens-IT in der Cloud vorgehalten werden, ist es technisch nicht sinnvoll, veraltete Methoden wie etwa VPN (virtuelle private Netze) zu verwenden. Denn es ist aus technischer Sicht nicht sinnvoll, den Netzwerkverkehr über VPN in die Firmeninfrastruktur hinein und von dort wieder zurück ins Homeoffice oder das Co-Working-Büro zu leiten. Mit dem Smartphone als «Trust-Anker» können Unternehmen auf benutzerfreundliche Weise ihre Daten und die ihrer Mitarbeitenden voneinander trennen und die Informations- und Datensicherheit sowie die nötige Privatsphäre gewährleisten.