Gefahrenabwehr bei Smartphones und Tablets ins Risikomanagement einbeziehen

Obwohl Mitarbeitende immer häufiger mit Tablets und Smartphones unterwegs sind, beschränken sich nach wie vor viele Sicherheitsverantwortliche bei ihren Sicherheitsstrategien auf die herkömmliche PC- und Laptop-Flotte. Zur Absicherung mobiler Geräte bedarf es aber spezieller Endpoint-Security-Lösungen.

DER AUTOR

Lorenz Zollikofer
Leiter Kommunikation, Nomasis

Beim Risikomanagement der Endgeräte liegt bei vielen Unternehmen der Fokus nach wie vor auf PC und Laptops. Obwohl aus der heutigen Arbeitswelt Smartphones nicht mehr wegzudenken und auch Tablets immer stärker im Kommen sind. Und diese Geräte sind zusätzlichen Sicherheitsrisiken ausgesetzt. Die bestehende Sicherheitsstrategie der PC-Geräte auf Smartphones und Tablets ausweiten, birgt dementsprechend Gefahren, die sich auch mit den Lösungen zum Management mobiler Geräte nicht in den Griff kriegen lassen. Solche EMM- und MDM-Anwendungen (Enterprise Mobility Management und Mobile Device Management) sind zur Verwaltung der Geräte, zum Löschen von Daten, zur Trennung geschäftlicher von privaten Daten, zur Authentifizierung der Nutzer und zur Erteilung von Zugriffsberechtigungen gemacht. Sie bieten auch teilweise Sicherheits-Features, können aber niemals einen vollständigen Schutz garantieren.

Grafik: alashi/iStock.com

EMM- und MDM-Anwendungen bieten teilweise Sicherheits-Features, können aber niemals einen vollständigen Schutz garantieren.

Bedrohungen auf mehreren Ebenen

Denn die Sicherheitsrisiken sind vielseitiger und stärker herstellerabhängig als die von PCs und Laptops. Gefahren lauern nicht nur aufgrund bösartiger Apps, sondern auch auf Geräte-, Netzwerk- und Web- respektive Inhaltsebene. Es geht dabei um Bedrohungen, Schwachstellen sowie Verhaltens- und Konfigurationsrisiken. Heimtückische Apps lesen Informationen aus, schädigen Hardware oder gewähren Unberechtigten Fernzugriff. Weil auch seriöse Apps Schwachstellen enthalten können, liefern namhafte Anbieter regelmässig Patches zur Schliessung der Lecks. Allerdings meistens erst, wenn konkrete Vorfälle die Schwachstelle aufdecken. Voraussetzung aber ist, dass die Nutzer die Updates auch installieren. Auch Absicherungsmechanismen wie Certificate-Pinning mindern die Risiken. Allerdings sind Mitarbeiter immer häufiger mobil unterwegs. Entsprechend länger sind die Geräte Risiken in unternehmensfremden Netzwerken ausgesetzt.

Stichwort Endpoint-Security

Sicherheitsbedrohungen auf Geräteebene können zu Datenverlust oder ungewollter Überwachung via Mikrofon oder Kamera führen, indem sich etwa der Angreifer mit einer Phishing-SMS höhere Berechtigungsstufen verschafft. Reine EMM- und MDM-Lösungen setzen nun voraus, dass die verwalteten Geräte nicht kompromittiert sind. Ist ein Endgerät aber infiziert, können Cyberkriminelle mit Trojanern Benutzerpasswörter während der Eingabe abfangen und sogar Einmalpasswörter bei mehrstufigen Authentifizierungslösungen auslesen. Für Smartphones und Tablets sind deshalb speziell dafür entwickelte «Endpoint Security»-Lösungen unerlässlich. Solche Lösungen beinhalten eine App, die über die MDM-Software ausgerollt wird. Mit der Installation durch den Nutzer wird sein Gerät automatisch in einer Administratorkonsole sichtbar, sodass Bedrohungen und Datenlecks in Echtzeit erkannt und Vorkehrungen dagegen getroffen werden können. Wenn immer möglich sollen diese für den Anwender unbemerkt ablaufen. Allfällig nötiges Handeln des Nutzers kann mittels E-Mail und einem darin enthaltenen Button initiiert werden. Ein Klick genügt dann, um unzulässige Apps zu deinstallieren. Tut er dies nicht, kann der Administrator das Gerät in Quarantäne nehmen. Endpoint-Security-Lösungen vervollständigen das Risikomanagement, bedürfen aber auch dediziert auf die Situation der Unternehmen zugeschnittener Sicherheitsmodelle.