Mobile Bedrohungen werden vernachlässigt. Bei den meisten Unternehmen hinkt das Risikomanagement der zunehmenden Verwendung von Smartphones und Tablets massiv hinterher.

VON JONAS HOFER*

Um es gleich auf den Punkt zu bringen: Wenn Unternehmen die Verwendung mobiler Geräte wie Smartphones und Tablets zulassen und fördern, müssen sie diese auch in ihrem Risikomanagement respektive ihrer Security-Strategie mitberücksichtigen. In der Praxis ist es aber leider nach wie vor so, dass Sicherheitsverantwortliche den Schwerpunkt vor allem auf konventionelle PC-Endgeräte und Laptops legen. Selbstverständlich gibt es Risiken, die sowohl PC als auch mobile Endgeräte betreffen. Die Sicherheitsstrategie für die PC-Flotte einfach auf Smartphones und Tablets auszuweiten, bleibt aber leider ohne Wirkung. Hinzu kommt, dass sich Security-Verantwortliche auch noch anderweitig in falscher Sicherheit wiegen. Sie nutzen zwar Anwendungen für das Management mobiler Geräte, gehen aber fälschlicherweise davon aus, dass ihre EMM-oder MDM-Lösungen (Enterprise Mobile Management oder Mobile Device Management) sie auch vor mobilen Bedrohungen schützen. Dem ist aber nicht so. EMM-Anwendungen sind gut darin, Geräte zu verwalten, Daten auf Geräten zu löschen, eine Aufteilung auf den Geräten zwischen persönlichen und Unternehmensdaten vorzunehmen, Zugriffe auf Unternehmensanwendungen oder Inhalte zu erlauben oder Nutzer zu authentifizieren. Klar gibt es auch bei solchen Anwendungen zur Verwaltung von Geräten und Nutzern gewisse Sicherheitsfunktionen. Einen ausreichenden Schutz aber können nur dezidierte Lösungen bieten, welche das gesamte Spektrum mobiler Risiken oder zumindest die den konkreten Anwendungsfall betreffenden Gefahren für ungewollten Datenabfluss abdecken.

Apps, Geräte und Netzwerke betroffen. Sicherheitsrisiken für mobile Plattformen sind verglichen mit traditionellen Desktops vielseitiger und stärker abhängig von herstellerspezifischen Möglichkeiten. Diese Sicherheitsrisiken betreffen nicht nur die Apps selbst, sondern umfassen auch Geräte, Netzwerk- und Web- respektive die Inhalteebene. Dabei kann es sich jeweils um Bedrohungen, Schwachstellen oder Verhaltens- und Konfigurationsrisiken handeln. So können etwa bösartige Apps Informationen auslesen, Geräte-Hardware beschädigen oder unberechtigten Fernzugriff gewähren. Apps können aber ganz einfach auch Schwachstellen enthalten. Nicht umsonst liefern namhafte Software-Hersteller regelmässig Patches, um in ihren Apps enthaltene Lecks zu schliessen. Man berücksichtige, dass dies meistens erst dann geschieht, wenn ein Vorfall die Schwachstelle an den Tag bringt. In der Zwischenzeit aber bleibt die Geräteflotte den vielfältigen Angriffen aus dem Web ausgesetzt. Erschwerend kommt hinzu, dass viele Nutzer die zur Verfügung gestellten Releases nicht installieren. So ergab beispielsweise eine vom US-Cybersecurity-Spezialisten Lookout im letzten Jahr bei Millionen verwalteter Geräte durchgeführte Auswertung, dass einen Monat nach der Veröffentlichung des Apple-Betriebssystems iOS 10.3 lediglich 57 Prozent der IOS-Nutzer ihr Betriebssystem aktualisiert hatten. Dies ist insofern besorgniserregend, da diese Version Fehler ausgemerzt hatte, welche Geräte Angriffen über mobile Netzwerke aussetzten. Auch wenn in der Praxis vielleicht nur ein kleiner Prozentsatz mit tatsächlichen netzwerkbasierten, bösartigen Bedrohungen konfrontiert war, reicht dies aus, um Daten während der Verbindung über WLAN oder Mobilfunk abzufangen. Obwohl Mechanismen wie Certificate-Pinning eine starke Verbesserung mit sich gebracht haben, nimmt die Bedeutung von Netzwerkbedrohungen zu. Dies deshhalb, weil aufgrund der zunehmenden Mobilität der Mitarbeitenden die Geräte einer Unternehmensflotte länger mit fremden Netzwerken als mit dem eigenen Unternehmensnetzwerk verbunden sind.

© anyaberkut – Fotolia.com

Breites Spektrum an Bedrohungen. Die gleiche Untersuchung ergab überdies, dass 30 Prozent der Apps auf unternehmenseigenen iOS-Geräten auf Kontaktdaten, 75 Prozent auf die Kamera, 38 Prozent aufs GPS, 8 Prozent auf Kalender und immerhin 10 Prozent auf das Mikrofon zugreifen. Mit jedem zehnten App hätten also auch Unbefugte unbemerkt Gespräche mithören können. Sicherheitsbedrohungen auf Geräteebene können deshalb zu Datenverlust oder ungewollter Überwachung führen, weil sich der Angreifer beispielsweise über eine Phishing-SMS höhere Berechtigungsstufen verschafft. Das Problem liegt nun darin, dass reine EMM- und MDM-Lösungen voraussetzen, dass ein Gerät nicht kompromittiert ist. Tatsache ist aber, dass die Sicherheit der Daten nicht gewährleistet werden kann, wenn ein Gerät erst infiziert ist. Man bedenke, dass Angreifer, etwa mit Trojanern, Benutzerpasswörter während der Eingabe abgefangen haben. Sogar Einmalpasswörter bei mehrstufigen Authentifizierungslösungen können ausgelesen werden. So effizient die Arbeitsweise mit mobilen Endgeräten auch sein mag, mit der Häufigkeit ihrer Anwendung in Unternehmen steigt eben auch die Gefahr bösartiger Angriffe oder unbeabsichtigter Datenabflüsse. Es bedarf deshalb entsprechender Schutzmassnahmen durch speziell dafür entwickelte «Endpoint Security»-Lösungen.

ÜBER NOMASIS AG

Als Pionier und Marktführer in der Umsetzung von mobilen IT-Infrastrukturen betreut Nomasis über 200 aktive Kunden aus der Finanzbranche, den öffentlichen Diensten, Industrie, Gesundheitswesen, Handel und Bildung. Seit der Firmengründung im Jahr 2004 hat sich das Unternehmen konsequent auf die Informationssicherheit für den mobilen Mitarbeiter spezialisiert und bringt geschäftsrelevante Daten sicher und einfach auf mobile Geräte wie Smartphones, Tablets und Laptops. **www.nomasis.ch**

Integriert und benutzerfreundlich. Eine solche muss vor anwendungsbasierten Bedrohungen Schutz bieten, netzwerkbasierte Bedrohungen und nicht autorisierte Nutzungen erkennen, Apps sichtbar machen, die aus nicht offiziellen App-Stores per «Sideload» heruntergeladen werden und nicht zuletzt benutzerdefinierte Richtlinien für Problembenachrichtigungen für verschiedene Bedrohungsarten ermöglichen. Solche Lösungen beinhalten jeweils eine App für die Mitarbeitergeräte, welche üblicherweise über die Mobile-Device-Management-Software ausgerollt wird. Aktiviert der Benutzer diese, so installiert sich gleichzeitig das Gerät in einer cloud-basierten Konsole für den Administrator, über welche dieser Bedrohungen und Datenlecks in Echtzeit erkennen und entsprechende Problembehebungsszenarien in Gang setzen kann. So weit wie möglich sollten diese im Hintergrund für den Nutzer unsichtbar ablaufen. Ist allerdings eine manuelle Interaktion erforderlich, muss diese möglichst einfach zu handhaben sein. Dies kann beispielsweise bei geringem Risiko eine E-Mail-Nachricht und ein einfacher Button sein, der angeklickt ohne weiteres Zutun eine unberechtigte App deinstalliert. Geschieht dies nicht, können im Hintergrund Massnahmen ergriffen werden, etwa indem das Gerät in Quarantäne genommen wird. Mit solchen Vorkehrungen, die speziell auf die Bedrohungen durch den Einsatz von Smartphones und Tabletts ausgerichtet sind, können Unternehmen ihr Risikomanagement auf ein zeitgemässes Level heben und sich vor Datenklau schützen. Dazu müssen speziell auf die Anforderungen des Unternehmens zugeschnittene Sicherheitsmodelle erarbeitet werden. Um diesen Prozess in Gang zu bringen, können beispielsweise Lösungen von verschiedenen Anbietern gegeneinander in einem «Battle» antreten, und es kann schliesslich vom Sieger ein Machbarkeitsnachweis verlangt werden, bevor man sich für eine Lösung entscheidet.

JONAS HOFER
ist Mobile Security Engineer bei Nomasis, **www.nomasis.ch**