Mobile Security

Sicher unterwegs

Mobiles Arbeiten ist in. Doch was passiert bei einem Geräteverlust? Tipps für das Security- und Risikomanagement geschäftlicher Daten. **Von Jonas Hofer**

Die Nutzung von Smartphones und Tablets im geschäftlichen Umfeld hat sich in allen Branchen längst durchgesetzt. Dennoch verfügen die wenigsten Firmen über entsprechende Sicherheitskonzepte und fokussieren weiterhin auf den Schutz von PC-Endgeräten. Das Einbinden von Mobilgeräten in Unternehmen erfordert einen Paradigmenwechsel. Das Konzept des Netzwerkperimeters verschwindet zunehmend: Unternehmensdaten sind in der Cloud verfügbar und liegen somit ausserhalb des hauseigenen Netzwerks. Mobile Devices sind per Mobilfunknetz und fremde Hotspots ans Netz angebunden anstatt per Firmen-Wi-Fi. Ein alleiniges Ausdehnen etablierter Sicherheitskontrollen auf die Mobilgeräteflotte bleibt also ohne Effekt. Denn nicht nur bei Apps, sondern auch auf Geräte-, Netzwerk- und Web- respektive Inhaltsebene tun sich neue Bedrohungen auf. Bösartige Apps können Informationen abziehen, Geräte beschädigen und unberechtigten Systemen oder Personen Fernzugriff auf Unternehmensdaten oder das Nutzerverhalten gewähren. Hinzu kommen Bedrohungen wie Malware, die sich über Exploits oder achtlos erteilte Nutzerberechtigungen auf Geräten einschleusen. Auch missbräuchliche Apps, mit denen Anbieter bösartige oder unbefugte Absichten verfolgen, können Schaden verursachen. Selbst namhafte Software-Unternehmen veröffentlichen immer wieder Apps, die Schwachstellen enthalten, die nicht selten erst bekannt werden, nachdem sie bereits Schäden angerichtet haben. Auch von professionellen Entwicklern geschaffene Apps können ungewollten Datenabfluss begünstigen, wenn etwa mit Code aus Code-Bibliotheken Funktionen umgesetzt werden. Viele Sicherheitsverantwortliche gehen dennoch davon aus, dass sie ihre Lösung für das Mobile Device Management (MDM) vor schädlicher Software schützt. Allerdings können Nutzer per «Sideload» auch vom Unternehmen nicht genehmigte Apps auf ihren Smartphones installieren und auf diese Weise das MDM unterlaufen.

Geräte absichern

Sicherheitsbedrohungen, die Betriebssysteme und Firmware von mobilen Geräten beeinträchtigen, können sowohl zu katastrophalem Datenverlust als auch zu ungewollter Überwachung führen. Denn Angreifer können sich auf diese Weise höhere Berechtigungsstufen verschaffen, als üblicherweise an Apps vergeben werden. Das Antippen eines Links in einer manipulierten Phishing-SMS genügt, und der Angreifer kann Kamera und Mikrofon des Smartphones aktivieren und Gespräche abhören oder Bewegungen des Opfers nachverfolgen. Das eigentliche Problem bei Gerätebedrohungen besteht darin, dass alle übrigen Geräteschutz- und Managementmassnahmen voraussetzen, dass das Gerät selbst nicht kompromittiert ist. Ist ein Mobilgerät aber erst einmal infi-

Bild: Shutterstock/Wutzkohphoto

ziert, kann die Sicherheit der Unternehmensdaten mit MDM- und MAM-Lösungen (Mobile Application Management), nicht länger garantiert werden. Noch akuter wird das Problem, wenn Unternehmen mobile Geräte als Teil einer mehrstufigen Authentifizierungslösung nutzen und zu sehr auf das Soft-Token-Zertifikat des Mobilgeräts als zweiten Standard-Authentifizierungsfaktor vertrauen. Die infizierten Geräte gestatten es dem Angreifer, das Benutzerpasswort während der Eingabe zu stehlen, sich den Code des zweiten Authentifizierungsfaktors anzueignen und sich mithilfe eines SMS-Tokens beispielsweise in das Bankkonto des Opfers einzuloggen. Um Unternehmensdaten zu kompromittieren, wird durch das Vorhandensein von Token auf Mobiltelefonen ein Angriff auf diese unumgänglich, um den zweiten Faktor für Remote-Zugriffe abzudecken.

Lücken im Netzwerk schliessen

Je nachdem, wie Websites oder Anwendungen an das Internet angebunden sind, variieren auch die Wege für Angreifer. Diese nutzen vorhandene Schwachstellen in Verbindungen über WLAN-, Mobilfunk- oder andere Netzwerke aus. Diese Angriffe können entweder direkt oder mithilfe von Malware automatisiert erfolgen. Beispiele hierfür sind Man-in-the-Middle-Angriffe, die Vortäuschung eines Zertifikats, TLS-/SSL-Stripping oder das Herabstufen von TLS-/SSL-Cipher-Suites. Früher waren Netzwerkangriffe zwar möglich, aber selten. Was sich innerhalb der Firewall befand, galt generell als sicher. Heute ist aber jedes Gerät einer mobilen Flotte täglich länger mit anderen Netzwerken verbunden als mit dem Unternehmensnetzwerk. Während sich früher die Häufigkeit von Netzwerkangriffen im überschaubaren Rahmen hielt, solange sich unternehmenseigene Geräte hauptsächlich innerhalb des Gebäudes befanden, hat sich die Situation heute total verändert und bedarf einer neuen Standortbestimmung.

Web- und Content-Bedrohungen

Schädliche Inhalte werden in erster Linie mittels Phishing-E-Mails oder -Textnachrichten verbreitet. Diese enthalten Links, die User zu vermeintlich offiziellen Anmeldeseiten weiterleiten können, um entsprechend ihre Zugangsdaten abzufangen. Es gab in den letzten Monaten zudem mehrere Beispiele für die Verteilung von Schad-Software, in denen nach dem Klick auf einen Link in einer solchen Phishing-SMS keine weitere Interaktion des Benutzers erforderlich war. Mittels einer Browser-Schwachstelle wurde ein Angriffspunkt des Kernels ausgenutzt, um das Gerät zu kompromittieren.

Die Gefahr, dass Nutzer von Mobilgeräten ihre Anmeldedaten auf Phishing-Seiten eingeben, ist um ein Mehrfaches höher als bei Desktop-Usern. Aber auch Content-Bedrohungen sollten im Zusammenhang mit der Mobilgerätenutzung unbedingt ernst genommen werden. Um diese zu verhindern, müssen die einzelnen Phasen der Bedrohung frühzeitig abgewehrt werden – wie zum Beispiel Textnachrichten, die Spyware implementiert haben oder ein Drive-by-Download, der einen Trojaner auf dem Gerät des Users installiert. Die Abwehr von Web- und Content-Bedrohungen erfordert ergänzend zu einer Mobile-Threat-Defense-Lösung einen mobilgerätespezifischen Phishing-Schutz für E-Mail und Anti-Spam. Ebenso muss der Web-Content-Filter für mobile Zwecke ausgelegt sein. Mithilfe von Sicherheits-Tools für soziale Netzwerke können Anwender zudem vor Phishing-Angriffen über soziale Netzwerke geschützt werden.

«Heute ist jedes mobile Gerät täglich länger mit fremden Netzwerken verbunden als mit dem firmeneigenen»

Jonas Hofer

Fazit

Eine umfassende Strategie zum Schutz vor mobilen Bedrohungen beinhaltet eine Management-Lösung für das Mobile-Application- und Device-Management. Das System sollte unternehmenseigene Geräte genauso verwalten wie Intrusion-Defense- und -Prevention-Systeme, die Einbindung von Daten über mobilgerätespezifische Bedrohungen, die Überprüfung mobiler App-Downloads mithilfe von URL-Filtern und Internetsicherheitskontrollen sowie Netzwerkkontrollen. Hierzu zählen etwa Blacklisting mobiler Command-and-Control-Server in Firewalls.

Solche Ansätze ermöglicht beispielsweise die Kombination von MDM-Anwendungen mit Endpoint-Security-Lösungen. Einen guten Überblick über den aktuellen Stand der Anbieter liefert der im August 2017 erschienene «Market Guide for Mobile Threat Defense Solutions» von Gartner. Das Marktforschungsunternehmen schätzt, dass allein der Anteil von mobiler Malware von heute 7,5 Prozent bis 2019 auf einen Drittel zunimmt und bis 2020 der Anteil von Unternehmen, die mobile Threat-Defense-Lösungen an ihre MDM-Anwendungen anbinden, von 10 auf 30 Prozent ansteigt. ■

Jonas Hofer
ist Mobile Security Engineer bei Nomasis:
www.nomasis.ch