Mobilgeräteschutz wird sträflich vernachlässigt

Know-how Mobile Endgeräte sind beliebte Angriffsziele. Sie befinden sich meist ausserhalb des Unternehmensperimeters – gleichzeitig investieren viele Firmen zu wenig in den Schutz von Smartphones, Tablets und Notebooks. Beispielsweise in MTD-Lösungen.

Von Severin Freund

In der heutigen digitalen Ära stehen Unternehmen vor einer zunehmend komplexen Herausforderung: dem Schutz ihrer mobilen Geräte vor Cyberangriffen. Während PCs und Laptops seit Jahrzehnten durch verschiedene Sicherheitsmassnahmen geschützt werden, bleiben Smartphones und Tablets oft vernachlässigt. Dies ist besonders besorgniserregend, da mobile Geräte immer häufiger zum Einfallstor für Cyberkriminelle werden. Ein Grund für die Besorgnis besteht darin, dass sich die Bedrohungslandschaft dramatisch verändert hat. Denn Angreifer nutzen zunehmend künstliche Intelligenz (KI) für ihre Attacken, was sie den Anbietern von Cybersecurity-Lösungen oft einen Schritt voraus sein lässt. Diese Entwicklung und die Tatsache, dass mobiles Arbeiten auch automatisch mit Cloud Computing in Zusammenhang steht, sollten Unternehmen aufhorchen lassen, ihre Sicherheitsstrategien zu überdenken und anzupassen.

Massnahmen reichen nicht aus

Viele Unternehmen schützen zwar ihre lokalen Server- und Endgeräteinfrastrukturen, verlassen sich aber, wenn überhaupt, für die mobile Geräteflotte (Smartphones, Tablets und Notebooks) auf Systeme für Mobile Device Management (MDM) als primäre Schutzmassnahme. Das ist gut und recht. MDM bietet eine solide Basis für die Verwaltung mobiler Geräte – beschränkt sich aber auf grundlegende Sicherheitsfunktionen wie die Durchsetzung von Geräte-PINs, rudimentäre Sicherheitsrichtlinien und den Schutz vor nicht-autorisierten Änderungen am Betriebssystem. Diese Massnahmen reichen jedoch nicht aus, um komplexere Bedrohungen wie Phishing, Malware oder Netzwerkangriffe abzuwehren.

Um den steigenden Bedrohungen effektiv zu begegnen, benötigen Unternehmen daher effektivere Lösungen als nur MDM – beispielsweise Mobile Threat Defense (MTD). MTD-Systeme bieten Schutz gegen eine Vielzahl von Risiken, darunter Phishing-Angriffe, Schadsoftware, unsichere Apps und Sideloading, Netzwerkangriffe wie Man-in-the-Middle-Attacken, versteckte Jailbreaks oder Root-Zugriffe. Dazu und zur Früherkennung neuer Bedrohungen nutzen die Lösungen oft Machine Learning und grosse Datenbanken. Sie können in Echtzeit Bedrohungen aufspüren, auf Anomalien reagieren und im Fall der Fälle entsprechende Schutzmassnahmen einleiten. Die Verknüpfung mit SIEM-Lösungen (Security Information and Event Management) kann Unternehmen darüber hinaus eine umfassende Überwachung und schnelle Reaktion auf verschiedenste Cyberbedrohungen ermöglichen.

Ausserhalb des Unternehmensperimeters

Unternehmen, insbesondere KMUs, müssen die Bedrohungen für mobile Geräte ernst nehmen und im Rahmen ihrer Sicherheitsstrategie über grundlegende Lösungen hinausgehen. Die Implementierung von MTD-Systemen sollte als wesentlicher Bestandteil einer umfassenden Cybersicherheits-Strategie betrachtet werden, um nicht nur lokale IT-Infrastrukturen, sondern auch mobile Geräte zu schützen. Denn diese befinden sich naturgemäss meistens ausserhalb des Unternehmensperimeters und verbinden sich mittels unbekannten WiFi- oder Datennetzverbindungen zu den Unternehmensdaten. Das ist in sicher ein Grund, weshalb immer mehr Angriffe nicht mehr direkt auf die Unternehmensinfrastruktur, sondern auf Smartphones, Tablets und Laptops abzielen.

Dabei empfiehlt es sich, auf Spezialisten zu setzen, die sich auf mobile Sicherheit konzentrieren. Diese fehlen den meisten Firmen allerdings. Denn die Jobs dafür erfordern andere Skills als für die lokalen Infrastrukturen. Unternehmen sollten aber auch nicht warten, bis ein Schaden entstanden ist. In einer Zeit, in der Arbeit zunehmend mobil und flexibel gestaltet wird, ist dies nicht nur eine Frage der Sicherheit, sondern auch der Wettbewerbsfähigkeit und des Geschäftserfolgs. ■

DER AUTOR

Severin Freund ist Mobile Security Engineer bei Nomasis. Das Unternehmen bietet Cybersecurity-Lösungen für digitale Nomaden, also Menschen, die ortsunabhängig, flexibel und mobil arbeiten. Diese Lösungen sind speziell auf die Bedürfnisse der modernen Arbeitswelt von mobilen Geräteplattformen ausgerichtet.