Zehn Wege zur Sicherung der mobilen Geräte

„Vergessene“ Endpunkte im Griff

Die Sicherheit mobiler Geräte ist ein Punkt, der in IT-Budgets oft deutlich zu kurz kommt. In den meisten Fällen haben Dinge wie Sicherung des Unternehmensnetzwerks, der Rechenzentren, E-Mails und Endgeräte wie Laptops und Desktops deutlich höhere Priorität. Zu oft übersehen Cybersicherheitspläne ein erhebliches Risiko, das von den neuen Cyberangriffsflächen des Unternehmens ausgeht: mobile Geräte und Tablets.

Mobile Geräte werden immer mehr zu primären Enterprise-Computing-Geräten für Mitarbeiter. Mehr als die Hälfte des Internetverkehrs entsteht auf mobilen Geräten.[1] Benutzer haben über ihre mobilen Geräte sehr oft Zugriff auf wichtige Unternehmensdaten und andere digitale „Kronjuwelen“ des Unternehmens. Darüber hinaus fungieren diese Geräte mittels Zwei-Faktor-Authentifizierungstoken des Benutzers gleichzeitig als Schlüssel für den Zugriff auf persönliche und andere wichtige Daten, einschließlich Bankkonten, Kreditkarten und Krankenakten.

Es wäre unvorstellbar, Laptops und Desktops ohne Antivirensoftware und andere Endgeräteschutzmechanismen in Unternehmen auf diese Weise zu nutzen, doch genau das tun die meisten Unternehmen mit mobilen Geräten. Sie ignorieren die von ihnen ausgehenden Risiken weitgehend und lassen sich selbst (und damit oft auch ihre Kunden) ungeschützt. Laut einer Umfrage von Gartner verfügen nur drei Prozent der Unternehmen über Anti-Malware-Schutz auf mobilen Android-Geräten und nur ein Prozent auf iOS-Geräten.

Bei der Entwicklung einer Cybersicherheitsstrategie, die auch Smartphones und Tablets umfasst, ist zu beachten, dass mobile Geräte anders konfiguriert und verwendet werden als traditionelle Endgeräte und daher anders gesichert werden sollten. Zum Beispiel:

- ***Mobile Geräte werden häufig von Mitarbeitern außerhalb des Unternehmensbereichs eingesetzt.***
  Dies macht traditionelle Perimeter-Sicherheitsmechanismen wie IPS, Firewalls und E-Mail-Sicherheitslösungen für den Schutz dieser Geräte irrelevant.

- ***Mobile Geräte sind oft im Besitz der Benutzer.***
  Sie werden in den meisten Fällen nicht durch die Unternehmens-IT verwaltet, die Benutzer entscheiden, welche Anwendungen auf diesen Geräten ausgeführt werden sollen. Dies steht im Gegensatz zu den von Unternehmen herausgegebenen und kontrollierten Laptops, die oft straff verwaltet werden.

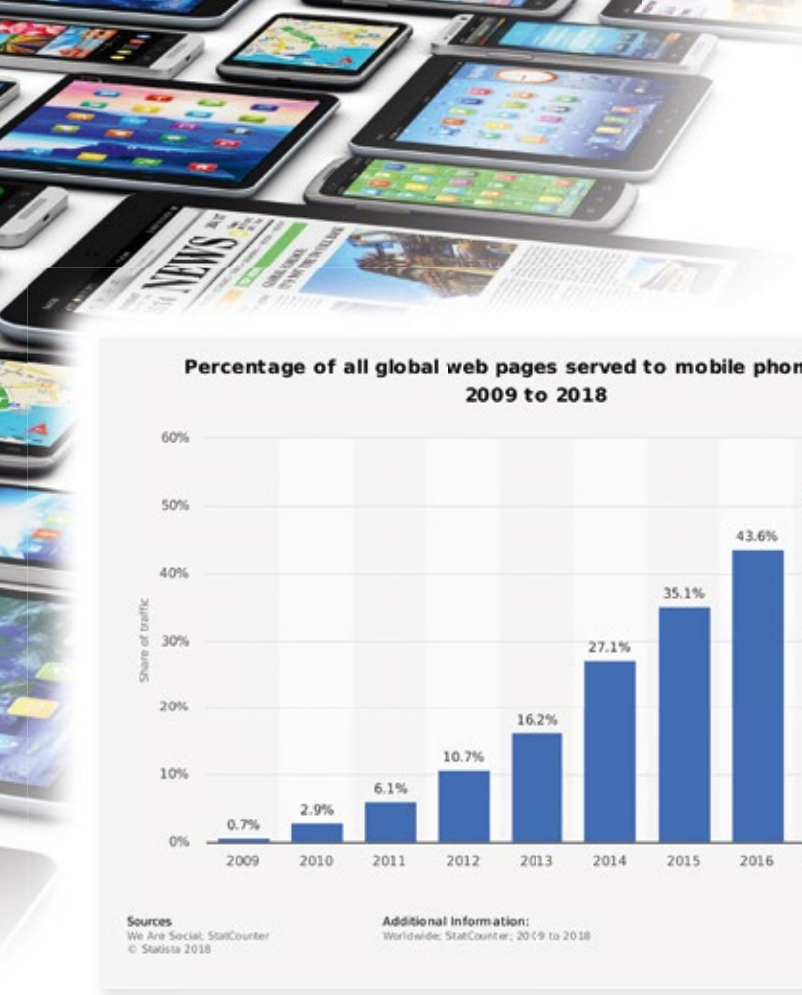
- ***Mobile Geräte sind immer angeschlossen und eingeschaltet.***
  Das macht sie zugänglicher und anfälliger für Angriffe.

- ***Mobile Geräte haben einen begrenzten Akku und eine begrenzte CPU.***
  Die Sicherheitslösungen, die ein Unternehmen zum Schutz von Laptops und anderen traditionellen Endgeräten verwendet, sind für diese Geräte nicht geeignet.

Mobile Geräte können in Sachen Sicherheit aus vielen verschiedenen Blickwinkeln betrachtet werden:

- ***Sie können komplett geknackt (Jailbreak) sein oder ihr Root-Verzeichnis kann übernommen worden sein.***
  Böswillige Akteure können so die Kontrolle über ungeschützte mobile Geräte übernehmen und alle Sicherheitsmaßnahmen der Betriebssystemhersteller umgehen.

- ***Schwachstellen im Betriebssystem können ausgenutzt werden.***
  Das Erkennen und Patchen solcher Schwachstellen auf mobilen Endgeräten



Mehr als die Hälfte des Internetverkehrs entsteht heute auf mobilen Geräten. (Quelle: Statistica 2018)

ist ebenso wichtig, wenn nicht sogar noch wichtiger als bei klassischen Endgeräten.

- ***Viele verschiedene Arten von Malware zielen speziell auf mobile Geräte.***
  Malware wird über scheinbar harmlose und legitime Anwendungen auf diese Geräte heruntergeladen. Mobile Malware soll bis 2019 ein Drittel der gesamten Malware ausmachen.[2]

- ***Selbst legitime, nicht bösartige Anwendungen können unangemessen viele persönliche Informationen sammeln:***
  Spiele, Musik-Streaming-Anwendungen, Arbeitsorganisatoren und Social-Media-Plattformen greifen oft auf sensible Ressourcen auf dem Handy eines Benutzers zu, für die sie nicht bestimmt sind, einschließlich der Kamera, des Kalenders und der Kontakte des Gerätes.

- ***Mobile Geräte verbinden sich mit mehreren öffentlichen Netzen.***
  Wenn Mitarbeiter das Unternehmensnetzwerk verlassen und sich mit verschiedenen öffentlichen Wi-Fi-Netzwerken verbinden, sind ihre mobilen Geräte anfällig für Man-in-the-Middle-Angriffe von bösartigen Wi-Fi-Zugangspunkten.

- ***Phishing wird immer häufiger zu einem Problem für mobile Geräte.***
  Ausgefeilte und intelligent gestaltete Phishing-Mitteilungen kommen über verschiedene mobile Anwendungen wie SMS und Social Messaging. Sie verleiten die Benutzer dazu, auf bösartige Links zu klicken, die in ihnen eingebettet sind. Benutzer können auf mobilen Geräten nicht immer die Gültigkeit der Zertifikate überprüfen, so dass es fast unmöglich ist festzustellen, ob die Links schädlich sind. Dies macht Phishing zu einer größeren Herausforderung für mobile Geräte als für andere traditionelle Endgeräte.

Diese Sicherheitsrisiken haben mobile Geräte inzwischen zur beliebtesten Angriffsfläche für Hacker gemacht, die auf die Daten

und Netzwerke von Unternehmenssystemen abzielen. Viele Unternehmen sind auf diese Herausforderungen nicht gut vorbereitet, da die meisten nicht in geeignete Maßnahmen zum Schutz ihrer Systeme im Mobilfunkbereich investieren. Wenn ein Unternehmen den Zugriff auf wichtige Unternehmensdaten von mobilen Geräten aus zulässt, können diese Endpunkte in seinem Cybersicherheitsplan nicht ignoriert werden.

Zehn Tipps für den Schutz mobiler Endgeräte

Sobald Ihr Unternehmen das Ausmaß seiner Anfälligkeit für die beschriebenen Sicherheitsrisiken ermittelt hat, können die folgenden Maßnahmen ergriffen werden, um mobile Bedrohungen zu minimieren und mobile Endgeräte zu schützen:

1. ***Definieren Sie das Bereitstellungsmodell für mobile Endgeräte Ihres Unternehmens.***
   Geben Sie firmeneigene Geräte an Mitarbeiter aus oder erlauben Sie Mitarbeitern, ihre eigenen Geräte mitzubringen (BYOD-Modell)?

2. ***Bewerten Sie das Bedrohungsprofil und die Stellung Ihrer mobilen Flotte.***
   Wie viele Android-/iOS-Geräte sind in Ihrer Flotte? Welche Betriebssystemversionen laufen auf den Geräten und welche Schwachstellen sind darin vorhanden?

3. ***Entwickeln Sie eine Sicherheitsstrategie für mobile Endgeräte.***
   Die Strategie basiert auf dem Bereitstellungsmodell, dem Bedrohungsprofil und der Risikobewertung.

4. ***Machen Sie mobile Endgerätesicherheit zur Priorität im Cyber-Sicherheitsbudget***.
   Viele Cybersicherheitsbeauftragte sind der Meinung, dass ihr Budget nicht ausreicht. In der EY-Untersuchung (EY ist ein weltweit führender Anbieter von Versicherungs-, Steuer-, Transaktions- und Beratungsdienstleistungen) 2017–2018 „Global Information Security Survey of Enterprise CIOs and CISOs" gaben 87 Prozent an, dass sie bis zu 50 Prozent mehr Budget benötigen, aber nur zwölf Prozent erwarten eine Steigerung von 25 Prozent oder mehr – alle anderen erwarten eine zum Teil weitaus geringere Budgetsteigerung.[3]

5. ***Investieren Sie in mobile Bedrohungsabwehrlösungen.***
   Die Eigenschaften und die Reife dieser Produkte variieren bei den verschiedenen Anbietern auf dem Markt. Suchen Sie nach Produkten, die ganzheitliche Lösungen für jeden der genannten potenziellen Angriffsvektoren bieten, einschließlich Geräte-, Betriebssystem-, Netzwerk-, Anwendungs- und Phishing-Schutz.

6. ***Blicken Sie nicht nur auf Phishing-Schutz für Unternehmens-E-Mails.***
   Reine E-Mail-Sicherheitslösungen filtern oft nur potenzielle Phishing-E-Mails und bösartige URLs heraus, bevor sie auf den E-Mail-Server des Unternehmens gelangen, schützen aber nicht vor bösartigen Links, die über verschiedene mobile Anwendungen wie SMS und Social Messaging eingehen können.

7. ***Bringen Sie strenge Sicherheits- und Compliance-Richtlinien auf den Weg.***
   Eine gute Lösung zur Abwehr mobiler Bedrohungen erkennt Schwachstellen, die im aktuellen Betriebssystem vorhanden sind, und sendet eine Warnung, wenn das Betriebssystem veraltet ist oder wenn das mobile Gerät nicht mehr den Anforderungen entspricht. Ermutigen Sie Anwender, ihr Betriebssystem auf die neueste Version zu aktualisieren und Compliance-Verstöße schnell zu beheben. Blockieren Sie beispielsweise den Zugriff auf Unternehmensdaten von jedem mobilen Gerät, das nicht auf die neueste Betriebssystemversion aktualisiert wurde oder nicht konform mit Ihren Richtlinien ist.

8. ***Bleiben Sie auf dem Laufenden über mobile Cybersicherheitsrisiken und -lösungen.***
   CISOs und Abteilungen, die für IT-Sicherheit verantwortlich sind, sollten die Richtlinien und die Einhaltung der Vorschriften regelmäßig überprüfen, um sicherzustellen, dass die Organisation den Bedrohungen durch mobile Sicherheitssysteme immer einen Schritt voraus ist.

9. ***Schulung der Mitarbeiter, um ihre mobilen Geräte vor bösartigen Akteuren zu schützen.***
   Führen Sie Schein-Phishing-Kampagnen und Schulungsprogramme für Mitarbeiter durch, um sie über Phishing auf mobilen Geräten aufzuklären.

10. ***Arbeiten Sie mit einem Experten für mobile Cybersicherheit zusammen.***
    Wählen Sie einen Anbieter, der Ihr Unternehmen dabei unterstützt, über neue Trends und neue Sicherheitsbedrohungen auf dem Laufenden zu bleiben und Ihre Sicherheitsstrategie weiterzuentwickeln. ■

VIJAYA KAZA,
Chief Development Officer bei Lookout

Quellenangaben:

(1) https://www.statista.com/statistics/241462/global-mobile-phone-website-traffic-share/
(2) https://www.gartner.com/doc/3829569/predicts--security-solutions
(3) https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf