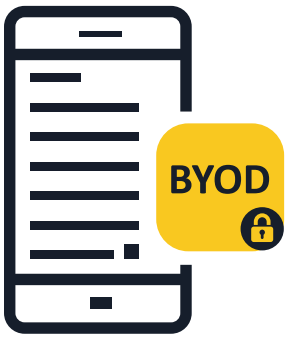
MOBILE MALWARE

TIPPS UND HINWEISE FÜR UNTERNEHMEN

1 Informieren Sie Ihre Mitarbeiter über die Risiken

- Mobiles Arbeiten lässt die Grenzen zwischen geschäftlicher und privater Nutzung verschwimmen. Unternehmen können durch einen Angriff, der zunächst gegen das mobile Gerät eines Einzelnen gerichtet war, erheblich getroffen werden. Ein mobiles Gerät ist ein Computer und sollte dementsprechend abgeschirmt werden.

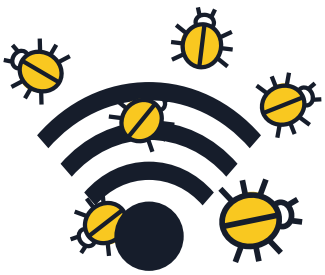


2 Legen Sie unternehmensinterne Richtlinien für Bring Your Own Device (BYOD) fest

- Mitarbeiter und Mitarbeiterinnen, die ihre eigenen mobilen Geräte (BYOD) benutzen, um auf Unternehmensdaten und -systeme zuzugreifen (auch wenn es sich nur um E-Mail, Kalender oder Kontaktdaten handelt) sollten Unternehmensrichtlinien folgen. Wählen Sie die Technologien, die zum Managen und zur Sicherung mobiler Geräte gewählt werden, sorgfältig aus und bringen Sie Ihre Mitarbeiter dazu, umsichtig zu handeln.

3 Nehmen Sie Richtlinien für mobile Geräte in Ihre Sicherheitsarchitektur auf

- Wenn ein Gerät die Sicherheitsrichtlinien nicht erfüllt, sollte eine Verbindung mit dem Unternehmensnetzwerk und Zugang zu Unternehmensdaten nicht gestattet werden. Unternehmen sollten Ihr eigenes Mobile Device Management (MDM) oder Enterprise Mobility Management (EMM) einsetzen.
- Ergänzend dazu ist es entscheidend, eine Mobile Threat Defence-Lösung zu installieren. Das sorgt für erhöhte Sichtbarkeit und kontextuelle Sensibilisierung für Gefahren auf App-, Netzwerk- und Betriebssystemniveau.

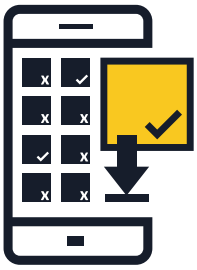


4 Seien Sie vorsichtig bei der Nutzung öffentlicher WLAN-Netzwerke für den Zugriff auf Unternehmensdaten

- Öffentliche WLAN-Netzwerke sind im Allgemeinen nicht sicher. Wenn ein Mitarbeiter/eine Mitarbeiterin am Flughafen oder in einem Café über eine kostenlose WLAN-Verbindung auf Unternehmensdaten zugreift, können die Daten böswilligen Benutzern ausgesetzt sein. Unternehmen wird geraten, Richtlinien zur Nutzung öffentlicher WLAN-Netzwerke zu entwickeln.

5 Betriebssysteme und Apps auf dem aktuellen Stand halten

- Empfehlen Sie Ihren Mitarbeitern, Software-Updates für das Betriebssystem Ihrer mobilen Geräte herunterzuladen, sobald Sie dazu aufgefordert werden. Informieren Sie sich, insbesondere für Android, über die Updaterichtlinien des Mobilfunkanbieters und Gerätehersteller. Die neuesten Updates gewährleisten nicht nur mehr Sicherheit sondern auch eine bessere Leistung des Geräts.



6 Installieren Sie Apps nur aus vertrauenswürdigen Quellen

- Unternehmen sollten für mobile Geräte, die Verbindungen zum Firmennetzwerk herstellen, nur die Installation von Apps aus offiziellen Quellen erlauben. Eine Alternative ist ein firmeneigener App Store, über den Endnutzer auf vom Unternehmen genehmigte Apps zugreifen und sie herunterladen und installieren können. Ihr Sicherheitsanbieter kann Sie bei der Einrichtung des Stores beraten, oder Sie lassen ihn betriebsintern entwickeln.

7 Verhindern Sie Jailbreaking/Rooting

- „Jailbreaking“ oder „Rooting“ ist der Prozess, bei dem die vom Anbieter des Betriebssystems auferlegten Sicherheitsbeschränkungen aufgehoben werden, um vollständigen Zugriff auf das Betriebssystem und Funktionen zu erhalten. Ein Jailbreak auf Ihrem Gerät kann dessen Sicherheit erheblich beeinträchtigen und zu Sicherheitslücken führen, die sonst nicht existieren. Geräte mit Root-Zugriff sollten in der Unternehmensumgebung nicht zugelassen werden.

8 Erwägen Sie Cloud-Storage-Alternativen (Webbasierte Speicherung)

- Mobile Nutzer wollen häufig nicht nur über ihren Firmen-PC auf wichtige Dokumente zugreifen sondern auch über ihre privaten Telefone oder Tablets außerhalb des Büros. Unternehmen sollten die Verwendung eines sicheren Cloud-basierten Speichersystems und Daten-Synchronisierungsdienstes erwägen, um auf sichere Weise auf diese Bedürfnisse einzugehen.

9 Lassen Sie Ihre Mitarbeiter eine Mobile Security App (Sicherheitssoftware) installieren

- Alle Betriebssysteme sind anfällig für Infektionen. Falls verfügbar, stellen Sie die Benutzung einer Mobile-Security-Lösung sicher, die Schadprogramme, Spyware und schädliche Apps entdeckt und blockiert und darüber hinaus Datenschutz- und Diebstahlschutzfunktionen bietet.