Mobile Sicherheit

Herausforderungen, Bedrohungen und effektive Schutzmassnahmen

Weil KMU ihre mobilen Geräte unzureichend schützen, werden diese immer häufiger zum Einfallstor für Angriffe. Umfassende Schutzkonzepte sind unerlässlich, um Risiken wie Datenverlust und Imageschäden zu minimieren. KI verschärft die Bedrohungslage weiter, wodurch die mobile Sicherheit immer komplexer und schnelllebiger wird.

› Tiziano Bacciarini

Die Digitalisierung und der Trend zum mobilen Arbeiten haben die IT-Landschaft von Unternehmen grundlegend verändert. Smartphones, Tablets und Laptops sind längst unverzichtbare Werkzeuge für Mitarbeitende im Homeoffice oder unterwegs. Doch gerade diese Flexibilität birgt erhebliche Risiken: Mobile Geräte werden zunehmend zum Einfallstor für Cyberkriminelle, und viele Unternehmen unterschätzen die Bedrohung oder setzen nur unzureichende Sicherheitsmassnahmen um.

Bevorzugtes Ziel für Angreifer

Mobile Endgeräte sind heute für viele Geschäftsprozesse essenziell. Sie werden häufig sowohl beruflich als auch privat genutzt, was die Angriffsfläche deutlich vergrössert. Cyberkriminelle haben erkannt, dass Smartphones und Tablets oft schlechter geschützt sind als klassische PCs oder Server.

Hinzu kommt, dass Nutzer im mobilen Kontext tendenziell fahrlässiger agieren – etwa durch die Nutzung unsicherer W-LAN-Netze, das Installieren von Apps aus unbekannten Quellen oder das Öffnen von Phishing-Nachrichten.

Die häufigsten Angriffsarten auf mobile Geräte umfassen Phishing-Attacken über E-Mail, SMS oder Messenger, Schadsoftware (Malware, Ransomware, Spyware), Ausnutzung von Schwachstellen im Betriebssystem oder in Apps, Man-in-the-Middle-Angriffe in unsicheren Netzwerken, Verlust oder Diebstahl von Geräten mit sensiblen Unternehmensdaten.

! **kurz & bündig**

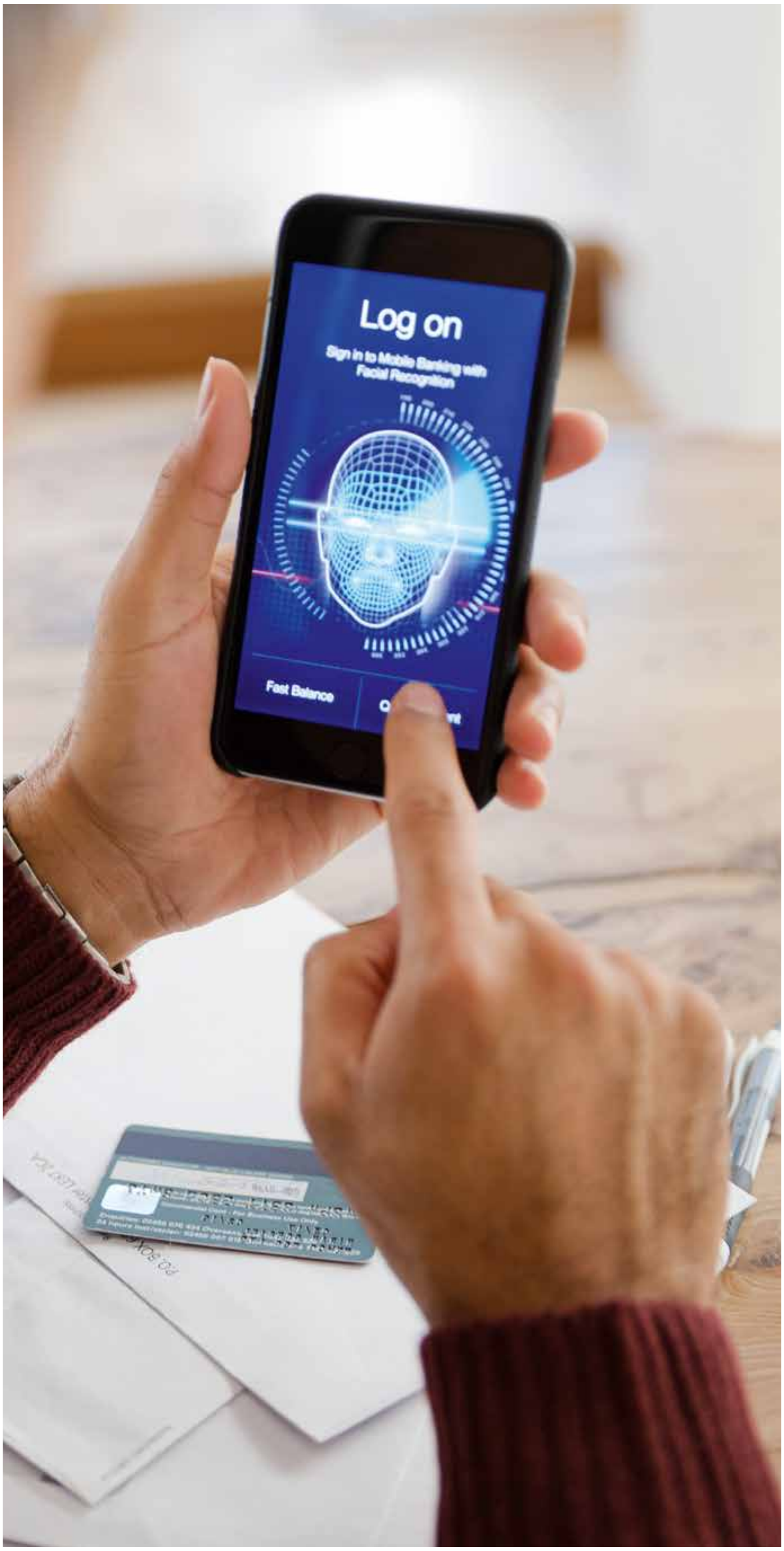
- Cyberkriminelle haben erkannt, dass Smartphones und Tablets oft schlechter geschützt sind als klassische PCs oder Server.
- Die Risiken durch unzureichend geschützte mobile Geräte sind enorm – von Datenverlust über Betriebsunterbrechungen bis hin zu massiven Imageschäden.
- Unternehmen sollten mobile Geräte als gleichwertigen Teil der IT-Infrastruktur begreifen und ihnen denselben Schutz angedeihen lassen wie Laptops, PCs und Servern.

Viele Unternehmen haben für ihre stationäre IT-Infrastruktur umfassende Schutzkonzepte etabliert – von Firewalls über Antivirenprogramme bis hin zu Backup-Strategien. Mobile Geräte hingegen werden oft nur rudimentär abgesichert. Standardmassnahmen wie Mobile Device Management (MDM) bieten zwar einen Grundschutz, sind aber gegen moderne Bedrohungen wie gezielte Phishing-Angriffe, fortgeschrittene Malware oder Netzwerkattacken nicht ausreichend.

Ein zentrales Problem ist zudem der Mangel an Know-how und klaren Prozessen im Umgang mit mobilen Sicherheitsvorfällen. Während für Laptops und PCs meist detaillierte Playbooks und geschulte Support-Teams existieren, fehlt Vergleichbares oftmals bei Smartphones und Tablets

Sicherheitsmassnahmen

Die wichtigsten Sicherheitsmassnahmen für Unternehmen lassen sich in einem



ganzheitlichen Ansatz zusammenfassen, der technische und organisatorische Aspekte vereint. Eine zentrale Rolle spielt das Mobile Device Management (MDM), das die Verwaltung, Inventarisierung und Konfiguration aller mobilen Geräte ermöglicht. Damit können Sicherheitsrichtlinien wie die Verpflichtung zu PIN-Codes oder biometrischer Authentifizierung, Vorgaben zur Betriebssystemversion, die Blockierung bestimmter Apps sowie die Verschlüsselung der Geräte durchgesetzt werden.

Auch die Möglichkeit, Geräte bei Verlust oder Diebstahl aus der Ferne zu sperren oder zu löschen, ist essenziell. Allerdings reicht dieser Basisschutz angesichts moderner Bedrohungen nicht mehr aus, da MDM-Lösungen allein keine gezielten Angriffe wie Phishing, Schadsoftware oder Netzwerkattacken erkennen und abwehren können.

Deshalb ist der Einsatz spezialisierter Mobile Threat Defense (MTD)-Lösungen notwendig. Sie ergänzen das MDM um fortgeschrittene Funktionen, indem sie das Verhalten von Apps, Netzwerkverbindungen und den Gerätezustand laufend überwachen. Bedrohungen wie Phishing-Nachrichten, Malware oder versteckte Jailbreaks werden so frühzeitig erkannt und automatisch unterbunden. Kompromittierte Geräte können isoliert und die IT-Abteilung sofort informiert werden.

Bei der Auswahl einer MTD-Lösung empfiehlt es sich, auf spezialisierte Anbieter zu setzen, die sich ausschliesslich dem Schutz mobiler Geräte widmen und ihre Lösungen kontinuierlich weiterentwickeln.

Auch das App-Management ist entscheidend: Unternehmen sollten sicherstellen, dass nur vertrauenswürdige Anwendungen aus offiziellen App-Stores installiert werden dürfen, während das Sideloading von Apps aus unbekannten Quellen unterbunden wird. Über das MDM können zudem Whitelists erstellt werden, die genau festlegen, welche Apps auf den Geräten genutzt werden dürfen.

Die Netzwerksicherheit ist ein weiterer kritischer Aspekt: Der Zugriff auf Unternehmensressourcen sollte ausschliesslich über sichere Verbindungen wie VPNs erfolgen. Unsichere WLAN-Netze sind zu vermeiden und, wo möglich, sollten auch unsichere Mobilfunkstandards wie 2G deaktiviert werden. Ergänzend empfiehlt sich der Einsatz von Secure Web Gateways, die den Datenverkehr filtern und überwachen.

Nicht technische Massnahmen

Neben technischen Massnahmen ist die Sensibilisierung der Mitarbeitenden ein Schlüsselfaktor. Regelmässige Schulungen und Awareness-Trainings helfen, das Bewusstsein für mobile Bedrohungen zu schärfen, den sicheren Umgang mit Geräten und Daten zu fördern und die Erkennung von Phishing-Versuchen zu verbessern. Klare Richtlinien und Kommunikationswege für den Fall eines Sicherheitsvorfalls müssen etabliert und den Mitarbeitenden bekannt sein. Nicht zuletzt braucht es ein effektives Notfallmanagement.

Unternehmen sollten Playbooks für den Umgang mit Sicherheitsvorfällen auf mobilen Geräten entwickeln, die klare Abläufe, Verantwortlichkeiten und Rollen definieren, damit im Ernstfall schnell und zielgerichtet reagiert werden kann. Support-Teams müssen spezifisch für mobile Geräte geschult sein, um kompromittierte Geräte genauso effizient wiederherstellen zu können wie klassische Computer.

Regelmässige Audits und Compliance-Prüfungen sorgen dafür, dass die Einhaltung aller Sicherheitsrichtlinien überwacht wird und bei Abweichungen umgehend Massnahmen ergriffen werden können. Nur ein solcher mehrschichtiger Ansatz gewährleistet, dass Unternehmen die Chancen des mobilen Arbeitens nutzen können, ohne ihre Daten und Geschäftsprozesse unnötigen Risiken auszusetzen.

Sicherheitsmassnahmen

- Mobile Device Management (MDM) als Basis, Mobile Threat Defense (MTD) für erweiterten Schutz
- Regelmässige Updates und konsequentes App-Management
- Trennung von privaten und geschäftlichen Daten
- Nutzung sicherer Netzwerke und starker Authentifizierung
- Schulung und klare Prozesse für den Ernstfall
- Kontinuierliche Überprüfung und Anpassung der Sicherheitsstrategie

Neue Bedrohungen

Mit dem Aufkommen von KI-gestützten Angriffsmethoden wird die Bedrohungslage nochmals verschärft. Phishing-Nachrichten werden täuschend echt, Malware passt sich dynamisch an und Angreifer nutzen automatisierte Tools, um Schwachstellen schneller auszunutzen. Auch die Verteidiger setzen zunehmend auf KI und Machine Learning, um Anomalien zu erkennen und schneller zu reagieren – doch das Wettrüsten ist in vollem Gange.

Unternehmen müssen aus diesem Grund ihre Schutzstrategien kontinuierlich anpassen und dürfen sich nicht auf einmal eingeführte Massnahmen verlassen. Die Integration spezialisierter MTD-Lösungen, die Überwachung durch erfahrene Spezialisten (intern oder extern) und die regelmässige Anpassung der Playbooks an neue Bedrohungen sind entscheidend.

Fazit

Die Risiken durch unzureichend geschützte mobile Geräte sind enorm – von Datenverlust über Betriebsunterbrechungen bis hin zu massiven Imageschäden. Unternehmen müssen mobile Geräte als gleichwertigen Teil der IT-Infrastruktur begreifen und ihnen denselben Schutz angedeihen lassen wie Laptops, PCs und Servern. Das bedeutet: Investitionen in Technik, Prozesse und vor allem in die Sensibilisierung der Mitarbeitenden. «

Porträt

Tiziano Bacciarini
Product and Services Manager, Nomasis

Als Pionier für Unternehmensmobilität in der Schweiz und in Liechtenstein bietet Nomasis Cyber-Security-Lösungen für digitale Nomaden, also Menschen, die ortsunabhängig, modern, flexibel und mobil arbeiten. Nomasis unterstützt ihre Kunden und deren Endbenutzer seit 20 Jahren mit IT-Services und sicheren Lösungen, die speziell auf die Bedürfnisse der modernen Arbeitswelt und mobilen Geräteplattformen ausgerichtet sind.

Kontakt

tiziano.bacciarini@nomasis.ch
www.nomasis.ch