Mobile Device Management vs. Mobile Security App

MOBIVISOR

Über uns

Die IOTIQ GmbH stellt seit 2017 innovative Softwarelösungen für verschiedene Anwendungsbereiche bereit. Unser Anliegen ist es, Unternehmen aller Branchen und Größen darin zu unterstützen, den Weg in Richtung Digitalisierung mit den richtigen Werkzeugen an der Hand und dem richtigen Partner an der Seite zu beschreiten.
In einer Welt, die mobil ist und stetig mobiler wird, steht die Sicherheit nach wie vor an oberster Stelle.
Um diese zu sichern, haben wir MobiVisor entwickelt - das Mobile Device Management System, das genau zu Ihnen passt.

IOTIQ

Smartly Done.

1. Mit welchen Gefahren werden mobile Geräte bedroht?

Die Sicherheit mobiler Geräte ist eine Hauptsorge vieler Unternehmen. Als sogenannte Endpoints von internen Netzwerken, stellen sie, neben Desktop Computern oder Laptops, ein beliebtes Ziel dar, um Zugriff auf Netzwerke zu erlangen und wertvolle Daten zu erbeuten.

Dabei bedienen sich Angreifer verschiedener Methoden: Viren, Malware und Ransomware. Mobile Geräte können aufgrund des Aufbaus des Betriebssystems nicht von “klassischen” Viren befallen werden. Da auf Smartphones und Tablets die Komponenten des Betriebssystems in einzelnen Paketen liegen, können sich Viren nicht selbstständig replizieren, wie es auf Computern der Fall wäre. Dadurch besteht ein gewisser Schutz - denn der Aufwand ein Smartphone mit einem Virus zu infizieren rechtfertigt nicht den kaum vorhandenen Gewinn.

Mal- oder Ransomware hingegen kann auch auf mobile Geräte gelangen. Ein Beispiel ist das “Smishing” (SMS-Phishing). Dabei wird eine SMS von einem scheinbar seriösen Anbieter versendet, zum Beispiel DHL oder Amazon. Oftmals steht in der Nachricht, dass ein Paket abgelegt wurde und der Empfänger bitte den Link in der SMS anklicken soll, um zu erfahren wo sich der Ablageort befindet. Wird der Link angeklickt, so installiert sich entweder direkt eine Schadsoftware auf dem Gerät, oder die Nutzer*in wird dazu aufgefordert, Daten wie die Adresse, Bankverbindung oder Telefonnummer anzugeben. Diese Daten werden von den Hackern oftmals weiterverkauft. In anderen Fällen liest die installierte Schadsoftware mit und kann z.B. Zahlungsdaten oder Passwörter auf diese Weise erlangen. Ransomware hingegen wird das Gerät unbrauchbar machen, indem Dateien etc. verschlüsselt werden, sodass kein Zugriff mehr besteht. Dieser Zustand hält solange an, bis ein Lösegeld gezahlt wird.

In allen Fällen entstehen monetäre Schäden sowohl durch erbeutete Daten oder das Lösegeld. Im schlimmsten Fall können Unternehmen bei Verlust von Daten von ihrenr Mitarbeitenden auf Schadensersatz verklagt werden.
Jährlich werden etwa 201 Millionen Angriffe auf mobile Geräte weltweit registriert - die Bedrohung ist also nicht zu unterschätzen.

2. Was kann man tun, um mobile Geräte zu sichern?

Die Liste möglicher Bedrohungen und den entsprechenden Sicherheitsmaßnahmen ist lang.
Es sollte stets darauf geachtet werden, dass die Maßnahmen alle Ebenen abdecken.
Nicht umsonst spricht man vom “Onion-Approach” (Zwiebel- Ansatz) der mobilen Sicherheit.
Gerade Unternehmen sollten sich nicht auf das Wissen Ihrer Mitarbeitenden in Bezug auf die sichere Nutzung mobiler Geräte verlassen - auch wenn diese umfassend geschult wurden.

Im folgenden haben wir häufige Bedrohungen und deren Abwehr zusammengefasst:

SMS Phishing

Eingehende SMS grundsätzlich von unbekannten und 0800-er Nummern verbieten.
Alternativ kann ein sicherer Messenger verwendet werden. Diese Einstellungen lassen sich z.B. über ein Mobile Device Management System (MDM) vornehmen.

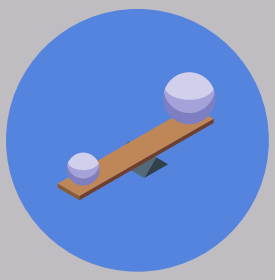
Installation von Schädlichen Apps

Über ein MDM kann die Anzahl der Apps die im Playstore zum Download bereit stehen reduziert werden. Es kann vorgegeben werden, dass nur durch das Unternehmen genehmigte Apps installiert werden können.

Nutzung unsicherer Internet-verbindungen

Offene und nicht durch ein Passwort geschützte Internetverbindungen sollten grundsätzlich gemieden werden. Aber um ganz sicher zu gehen, kann über ein MDM festgelegt werden, dass offene WLAN Verbindungen nicht genutzt werden dürfen.

Vermischung von Arbeit und Privatem



In manchen Fällen dürfen Mitarbeitende ihre eigenen Geräte auch für die Arbeit verwenden. Dieses Prinzip heißt “Bring your Own Device”. Hier darf es nicht zu einer Vermischung von privaten Daten mit Unternehmensdaten kommen.

Weitergabe sensibler Daten mit unsicheren Kommunikationsmitteln

Dies kann Anhänge betreffen, oder auch Daten, die nur den internen Gebrauch betreffen. Passwörter oder ähnliche Angaben sollten generell niemals über E-Mails oder Chats versendet werden.
Auch auf Chatprogramme, die für den privaten Gebrauch bestimmt sind, wie z.B. WhatsApp, sollte im Arbeitskontext verzichtet werden.
Nutzen Sie stattdessen lieber Alternativen, die extra für die sichere Kommunikation im Unternehmen konzipiert sind, wie z.B. MobiVisor Messenger.

3. Was taugen mobile Sicherheitsapps?

Viele Smartphone und Tablet-Nutzer*innen kennen es: mit dem Computer Antivirus-Programm wird auch ein begleitendes Antiviren Programm bzw. eine Antiviren-App für das mobile Gerät angeboten. Doch wie nützlich sind diese Apps und tragen sie wirklich dazu bei, die Geräte vollumfänglich abzusichern?

Die Meinungen darüber sind tatsächlich gespalten. Während die einen, hauptsächlich die Smartphone Anbietenden selbst, bekräftigen, dass die Geräte auch ohne Extra Apps bestens geschützt sind, so gibt es auf der anderen Seite immer wieder Stimmen von IT-Expert*innen und Anbietern von Sicherheitssoftwares, die das Gegenteil behaupten.

Grundsätzlich muss man sich allerdings vor Augen führen, was diese Apps überhaupt leisten können und in welchem Kontext sie eingesetzt werden sollen.
Abzuraten ist beispielsweise vom Einsatz einer App für die mobile Sicherheit als alleinige Lösung für die Absicherung der Geräte. Zwar fragt jede App Zugriffsberechtigungen ab, in den meisten Fällen können diese Apps aber bestenfalls Warnungen anzeigen. Ein Eingriff in das System um den Zugriff für Schadsoftware zu verhindern, ist nicht gegeben.

Generell ist die aktive Vorbeugung gegen Bedrohungen die sinnvollste Sicherheitsstrategie, denn so gelangen schadhafte Software und Apps erst gar nicht auf das Gerät. Die Vorbeugung kann dementsprechend größeren Schaden verhindern. Um aber wirksam vorzubeugen, muss das Sicherheitssystem so angelegt sein, dass Gefahrenquellen geblockt werden können. Eine Sicherheits-App kann dies in der Regel nicht.

Ein Beispiel: Die Sicherheits-App hat Zugriff auf die Netzwerke des Gerätes. Sobald das Gerät eine unsichere Internetverbindung nutzen möchte, wird eine Warnung erzeugt. Doch: der User kann diese Warnung ignorieren und die unsichere Verbindung trotzdem nutzen. Im Arbeitskontext darf dies nicht möglich sein.

Als Fazit steht fest, dass mobile Sicherheits-Apps zwar das Gefühl der Sicherheit erhöhen können - aber letztlich unvorsichtiges Verhalten nur teilweise präventiv verhindern. Bekommen Nutzer*innen zum Beispiel eine Warnung, dass ein Download Link o.ä. aus einer unsicheren Quelle stammen oder Internetverbindungen nicht abgesichert sind, so kann dies bestimmt bis zu einem gewissen Grad das Bewusstsein für die Bedrohungen schärfen und Nutzer*innen auch davon abhalten sich unvorsichtig zu verhalten. Im privaten Umfeld kann dies also durchaus sinnvoll sein.

4. MDM - die bessere Alternative?

Ein Mobile Device Management (MDM) dient grundsätzlich der Umsetzung von Sicherheitsrichtlinien von Unternehmen in die mobile Geräteflotte. Zum einen wird dadurch verhindert, dass sensible Unternehmensdaten an Drittparteien gelangen, zum anderen verhindert ein MDM den unsachgemäßen Gebrauch von Unternehmensgeräten und somit eine verkürzte Nutzungsdauer.

Aufgrund der großen Funktionalität der meisten MDMs, können Einstellungen sehr detailliert vorgenommen werden. Es kann noch dezidierter als über die Systemeinstellungen am Gerät selbst, eingestellt werden, was, wie und von wem genutzt werden darf.
Das ist ein großer Vorteil, da dadurch auch Klarheit bei den Verantwortlichkeiten und Befugnissen der Mitarbeitenden geschaffen wird.

Natürlich ist ein MDM auf den ersten Blick nicht nur umfänglicher, sondern auch weitaus komplizierter als die einfache Installation einer mobilen Sicherheits-App.
Doch sollte man stets beachten wie sich Kosten und Nutzen aufwiegen. Eine kostenlose Sicherheits-App wird nicht den tiefgreifenden Schutz bieten, den Sie sich für Ihre mobilen Geräte erhoffen. Zwar wird die Installation und Einrichtung des MDMs einige Zeit in Anspruch nehmen, aber dafür wendet es die größten Bedrohungen für die mobile Sicherheit zuverlässig ab.

Sie möchten mehr zum Thema mobile Sicherheit erfahren?

Besuchen Sie den Blog unseres Mobile Device Management Systems MobiVisor! Einfach hier klicken.

Gern beraten wir Sie persönlich! Schreiben Sie uns eine E-Mail an info@iotiq.de oder kontaktieren Sie uns telefonisch unter der 0176/ 34110095