Bring Your Own Device: Virtual Solution benennt die wunden Punkte bei Mobile Security

12.12.2019, 11:53 | IT, New Media & Software

Pressemitteilung von: *Virtual Solution*

München, 12. Dezember 2019 – Unternehmen statten Mitarbeiter mit mobilen Endgeräten aus, um produktiver zu werden. Gleichzeitig steigt dadurch die Anzahl potenzieller Angriffsvektoren – vor allem wenn private Geräte beruflich genutzt werden. Virtual Solution nennt drei altbekannte Probleme rund um Mobile Security, die weiterhin Brisanz haben.

BYOD (Bring Your Own Device) hat sich mittlerweile etabliert – viele Unternehmen unterstützen den betrieblichen Einsatz privater Smartphones oder Tablets. Die Vorteile liegen auf der Hand: Die Produktivität der Mitarbeiter steigt, sie benötigen nur ein statt zwei Geräten, die Unternehmen wiederum sparen sich Investitionen für aktuelle Smartphones und Tablets. Der Aufwand für Administration und der Support dieser Geräte ist allerdings nicht zu vernachlässigen, auch die Einrichtung der unerlässlichen Mobile-Device-Management (MDM)-Software für die Aktivierung, Verwaltung und Absicherung der Geräte ist alles andere als trivial. Zudem entstehen durch die Vielzahl unterschiedlicher Geräte und Betriebssysteme sowie die private und geschäftliche Nutzung neue Anforderungen hinsichtlich Management, Datenschutz und Sicherheit.

Vor diesem Hintergrund erläutert Virtual Solution drei Aspekte rund um einen sicheren und benutzerfreundlichen Unternehmenseinsatz von Smartphones und Tablets, die auch 2020 nicht an Brisanz verlieren werden.

1. Strikte Trennung von geschäftlichen und beruflichen Daten: Unternehmen sind für die Einhaltung des Datenschutzes verantwortlich, auch wenn geschäftliche Informationen auf privaten Geräten gespeichert oder verarbeitet werden. Die DSVGO schreibt vor, dass personenbezogene Daten auf dem mobilen Device so sicher sein müssen, wie sie es auch in der unternehmenseigenen IT-Infrastruktur wären. Auf einem BYOD-Gerät müssen deshalb der private und der geschäftliche Bereich strikt voneinander getrennt werden. Sowohl iOS 13 für das iPhone als auch Android ermöglichen inzwischen eine entsprechende Aufteilung. Um allerdings eine optimale Abgrenzung von den privaten Daten zu erreichen, kommen Unternehmen kaum um eine MDM-Lösung herum. Der Nachteil dieser Lösung: Sie ist kompliziert in Einrichtung und Verwaltung und nicht gerade günstig. Durch MDM erhalten Unternehmen zudem weitreichende Möglichkeiten des Zugriffs und der Einsichtnahme, in die Beschäftigte explizit einwilligen müssen – andernfalls drohen den Verantwortlichen hohe Strafzahlungen.

2. Eine starke Authentifizierung: Dass ein einfaches Passwort nicht der bestmögliche Schutz ist, ist eigentlich weithin bekannt. Neben Datenverlust und Diebstahl sind unsichere Logins für die IT-Verantwortlichen in Unternehmen aber nach wie vor eine große Herausforderung. Zwar gibt es längst zusätzliche biometrische Verfahren wie Fingerabdruck, Gesichtserkennung oder Iris-Scan, viele gehen aber bei ihrem privaten Gerät den einfachsten Weg und nutzen „1234“ oder den eigenen Geburtstag als Zugangskontrolle. Sind dann die beruflichen Daten nicht abgeschottet, können Cyber-Kriminelle schlimmstenfalls Firmeninterna abgreifen oder sogar tiefer ins Netzwerk eindringen. Die Verantwortung für eine starke Authentifizierung liegt in den Händen der Unternehmen, sie sollten firmenweit beispielsweise eine Kombination aus PIN und biometrischem Verfahren ausrollen.

3. Keine Installation gefährlicher Apps: Bei BYOD-Modellen ist die Umsetzung und Kontrolle eines Verbots bestimmter Apps eigentlich nicht möglich. Die Mitarbeiter werden auf ihre liebgewonnenen Programme nicht verzichten und sie heimlich weiternutzen. Die Unternehmen verlieren damit die Kontrolle über die Daten und können nicht dokumentieren, wo personenbezogene Informationen gespeichert werden, und diese auch nicht löschen. Das stellt einen Verstoß gegen die Vorgaben der DSGVO dar, es drohen hohe Strafzahlungen. Die meisten Anwender infizieren zudem ihr privates Gerät selbst mit Schadprogrammen, indem sie Apps aus dubiosen Quellen laden. Aber auch wer nur den Google Play Store oder den iTunes Store nutzt, ist vor Schadsoftware nicht hundertprozentig geschützt: Immer wieder gelingt es Kriminellen, infizierte Apps in die beiden Plattformen zu schleusen.

„Auf Geräte-Ebene lassen sich private und berufliche Dinge nie konsequent trennen. Ein sicheres Management muss daher die Ebene der Daten und Anwendungen ins Visier nehmen, nur so lassen sich berufliche und private Daten DSGVO-konform voneinander isolieren“, erklärt Sascha Wellershoff, Vorstand von Virtual Solution in München. „Anstatt das Gerät zu kontrollieren, liegt der Fokus beim Container-Ansatz auf der Sicherung der beruflichen Daten und Anwendungen auf dem mobilen Endgerät. Mit Hilfe von Containerlösungen wie etwa SecurePIM lassen sich die Daten eines Unternehmens auf dem mobilen Gerät in einer strikt abgeschotteten Umgebung betreiben und verwalten. Dadurch wird verhindert, dass Daten unkontrolliert ab- oder einfließen beziehungsweise manipuliert oder gekapert werden.“

Portrait

Über Virtual Solution

Virtual Solution ist ein international agierender Sicherheitsspezialist mit Sitz in München und Berlin. Das Unternehmen entwickelt und vertreibt die Applikation SecurePIM und das Framework SERA für iOS- und Android-Geräte. Beide Lösungen sorgen für eine sichere und benutzerfreundliche mobile Kommunikation in Behörden und Unternehmen bis zu einer Geheimhaltungsstufe „VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH“, kurz „VS – NfD“.

Virtual Solution wurde 1996 gegründet und beschäftigt rund 80 Mitarbeiter. Alle Produkte des Unternehmens tragen das Gütesiegel "IT-Security made in Germany" des TeleTrust-IT-Bundesverbandes IT-Sicherheit e.V. Weitere Informationen unter www.virtual-solution.com.

News-ID: 1070905 • Views: 679 (Stand: 29.07.2026)

Link zur Pressemitteilung:

https://www.openpr.de/news/1070905/Bring-Your-Own-Device-Virtual-Solution-benennt-die-wunden-Punkte-bei-Mobile-Security.html