Materna Virtual Solution

Mobiles Arbeiten als Sicherheitsrisiko

[26.09.2022] Mobiles Arbeiten kann eigentlich sichere IT-Infrastrukturen verwundbar machen, warnt der Kommunikationsanbieter Materna Virtual Solution und zeigt die häufigsten Einfallstore für Cyber-Attacken auf. Umsichtiges Verhalten und technische Lösungen können Abhilfe schaffen.

Hacker lieben mobiles Arbeiten, so die These des Kommunikationsanbieters Materna Virtual Solution. Durch die mobile Kommunikation außerhalb des Firmennetzes entstünden neue Angriffsflächen in eigentlich sicheren IT-Infrastrukturen, die von Cyber-Kriminellen ausgenutzt würden. Unternehmen und Organisationen sowie die Mitarbeitenden müssten die größten Risiken kennen, um den Datenschutz, die Sicherheit der mobilen Endgeräte und die Integrität des Datentransfers zu gewährleisten. Daher zeigt Materna Virtual Solution, auf welchen Wegen Gefahren für die Daten drohen.
Nach wie vor lauere eine große Gefahr in den App Stores der großen Anbieter. Anwendungen, die nach der Installation Tür und Tor für Malware öffnen oder vertrauliche Daten auslesen, zählen weiterhin zu den Hauptgründen für Datenlecks. Doch auch Alltags-Apps bekannter Hersteller, etwa Messenger, könnten zum Problem werden, wenn deren Datenschutzeinstellungen falsch gewählt seien. Dann könnten sensible Daten unter Umständen weitergegeben werden.
Auch Sicherheitslücken in Betriebssystemen gelte es umgehend zu patchen. Bleiben Schwachstellen in Anwendungen und Betriebssystemen bestehen – etwa, weil sie dem Hersteller zunächst nicht bekannt sind – besteht die Gefahr von Datendiebstahl und der unerwünschten Installation von Malware.

Awareness-Training und technische Maßnahmen

Neben technologischen Lücken seien oftmals die Mitarbeitenden Ziel von Angreifern und sollen beispielsweise mit gefälschten E-Mails oder Web-Seiten dazu verleitet werden, vertrauliche Daten wie etwa Passwörter preiszugeben. Auch aufgrund der immer fortschrittlicheren Phishing-Methoden sollten Mitarbeitende regelmäßige Schulungen zu dieser Art von Angriffen erhalten, so Materna Virtual Solution.
Sinnvoll sei es auch, für die Gefahren ungeschützter Netzwerke zu sensibilisieren. Arbeiten im Café oder im Hotel ist längst alltäglich – zu oft würden dabei aber noch offene WLANs oder Hotspots genutzt. Das sei zwar zunächst komfortabel, doch durch die unverschlüsselte Kommunikation könnten sensible Informationen abgefangen werden.
Damit ultramobiles Arbeiten funktioniert, benötigen Mitarbeitende jederzeit und von überall Zugriff auf Daten. Um diese abzusichern, sei eine Ende-zu-Ende-Verschlüsselung angeraten, sagt Christian Pohlenz, Security Expert bei Materna Virtual Solution. Container-Lösungen könnten zudem einen abgeschirmten und vor Zugriff geschützten Bereich auf mobilen Geräten schaffen, der höchste Sicherheit gewährleistet, so Pohlenz.

(sib)

Stichwörter: IT-Sicherheit, Cyber-Sicherheit, Materna Virtual Solution, mobiles Arbeiten