Virtual Solution

Daten schützen mit Container-App

[11.06.2020] Unsichere Kommunikationstools stellen in der öffentlichen Verwaltung ein Risiko dar. Um Microsoft 365 und Exchange Online besser vor Hacker-Angriffen zu schützen und zudem DSGVO-konform zu nutzen, ist eine Container-App eine sinnvolle Ergänzung.

Während der Corona-Krise mussten auch Behörden ihre Mitarbeiter ins Homeoffice schicken. Dort greifen viele auf Microsoft-Dienste wie Teams oder 365 zurück, um produktiv weiterzuarbeiten. Mit einer Container-App können Microsoft-Konten vor dem Missbrauch sensibler Bürger- und Behördendaten (wir berichteten) geschützt werden. Gleichzeitig ist damit die Einhaltung der strengen DSGVO-Vorgaben garantiert.
Auch unabhängig von Corona ist mobiles Arbeiten bei Behörden und öffentlichen Institutionen immer stärker auf dem Vormarsch. Werden Notebooks, Tablets und Smartphones – ob nun dienstlich gestellt oder privat – für die Kommunikation genutzt, haben Sicherheit und Datenschutz oberste Priorität. Allerdings lauern gerade bei der Nutzung von E-Mail-Clients und Messenger-Diensten erhebliche Sicherheits- und Compliance-Risiken – etwa indem Daten unkontrolliert abfließen. Auf diese Gefahren müssen die IT-Verantwortlichen in Ämtern und Behörden mit entsprechenden Schutzvorkehrungen reagieren.

Kontrolle über eigene Daten

Eine mobile Office-App wie SecurePIM lässt sich einfach mit Exchange Online verbinden, um E-Mails, Kalender oder Kontakte verschlüsselt zu synchronisieren. Über eine Einstellung im Exchange-Admin-Bereich können die IT-Verantwortlichen dabei sicherstellen, dass vom Mobilgerät aus nur die Container-App Zugriff auf Exchange Online hat. Damit hat die Behörden-IT die volle Kontrolle über die eigenen Daten, ohne dabei in die Privatsphäre ihrer Mitarbeiter eingreifen zu müssen beziehungsweise zu können. Das spielt gerade bei BYOD (Bring Your Own Device)-Modellen, also dienstlich genutzten Privatgeräten, eine wichtige Rolle. Auch Exchange Server der eigenen Infrastruktur können problemlos angebunden werden, zudem ist der sichere Zugriff auf OneDrive for Business möglich. Behörden können darüber hinaus den in die SecurePIM-App integrierten Messenger nutzen, um mit Kollegen verschlüsselt zu chatten, Dateien und Standorte zu teilen sowie zu telefonieren.

Privates und Dienstliches getrennt

Eine Container-Lösung wie SecurePIM bündelt alle wichtigen Office-Tools in einer App, die durch hochsichere Verschlüsselungsmechanismen die behördlichen Daten von den restlichen Apps auf dem Mobilgerät trennt. So kann beispielsweise der beliebte Messenger-Dienst WhatsApp bei BYOD-Konzepten nicht auf personenbezogene Daten wie Kontakte innerhalb des Containers zugreifen. Die IT-Administratoren könnten zudem dank Remote Wipe gezielt einzelne Ordner oder festgelegte Bereiche aus der Ferne löschen, was im Falle eines Handy-Verlusts die IT-Compliance sicherstellt. Besonders wichtig ist in der derzeitigen Krisensituation, dass der einfache Roll-out und die intuitiven Nutzeroberflächen einen schnellen Start unterstützen, den Trainingsaufwand minimieren sowie die aktive und sichere Nutzung deutlich erhöhen.
Basierend auf der Container-Technologie können Ämter und Behörden die Tools bereitstellen, mit denen

ihre Mitarbeiter unterwegs oder im Homeoffice komfortabel, sicher und datenschutzkonform arbeiten können. Das steigert Effizienz, Flexibilität und Sicherheit gleichermaßen.

()

Stichwörter: IT-Sicherheit, Homeoffice, Mobile Device Management, Virtual Solution AG