first frame networkers
IT, die Sie weiterbringt

Schutz der Unternehmensdaten auf privaten Mobilgeräten

Der Einsatz von mobilen Geräten ist längst Standard geworden in den Unternehmen. Überall sieht man Menschen, die im Zug, im Bus, im Restaurant, im Wartezimmer beim Arzt auf Smartphones und Tablets arbeiten. Das mobile Arbeiten bringt eine massive Produktivitätssteigerung und Flexibilität. Für das Management der IT ist es allerdings eine grosse Herausforderung in Bezug auf die Sicherheit.

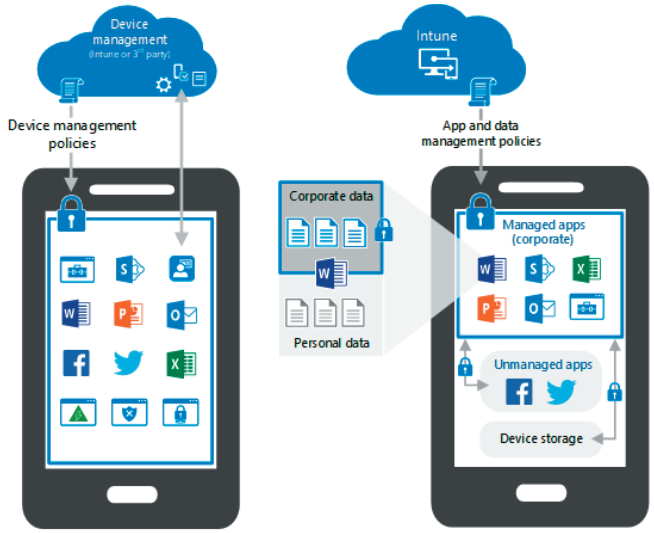
Sichere Mobility-Strategie mit MAM

Smartphones und Tablets werden heutzutage noch oft schlecht geschützt, obwohl sie in vielen Fällen für geschäftliche Kommunikation genutzt werden. Sensible Unternehmensdaten sind somit nicht geschützt, wenn sie auf mobilen Geräten aufgerufen werden. Diese haben mit ihren Möglichkeiten einen grossen Mehrwert für die Nutzer, sind aber ebenfalls anfällig für Bedrohungen. Von vielen Unternehmen wurden daher Mobile Device Management (MDM)-Lösungen eingeführt. Sie erhoffen sich mit dieser Massnahme eine Erhöhung der Sicherheit bei den Mobilgeräten. MDM allein reicht allerdings nicht aus, es braucht zu einer sicheren Mobility-Strategie mehr als nur die Verwaltung von Geräten. Deshalb kommt Mobile Application Management (MAM) zur Bereitstellung und Verwaltung mobiler Anwendungen ins Spiel.

Unternehmensdaten im Container schützen

Eine MAM-Lösung ist auf den Schutz der Unternehmensdaten fokussiert und kann als Container betrachtet werden. Eine Mobile Device Management (MDM)-Lösung hingegen verwaltet das gesamte Endgerät. Der MAM-Container ist ein abgeschotteter Sektor innerhalb des mobilen Device, für welchen man eine zusätzliche Authentifizierung benötigt. Das erhöht die Sicherheit und sollte dieses Gerät einem Diebstahl zum Opfer fallen, bleibt der Inhalt des Containers geschützt. Unternehmensdaten werden verschlüsselt innerhalb des Containers gespeichert und können mit der entsprechenden Container-Software aus der Ferne gelöscht werden. Die geschäftlichen Applikationen laufen getrennt von privaten Anwendungen. Die IT-Abteilung hat nur Zugriff auf die Daten und Applikationen des Unternehmens und nicht auf die privaten Aktivitäten des Mitarbeitenden.

first frame networkers
IT, die Sie weiterbringt



Vergleich der MDM- und MAM-Funktionen

Problemlose Verwendung von Privatgeräten

Oft gehören Smartphones und Tablets dem Mitarbeitenden und sie werden auch im Unternehmen genutzt. Mit Microsoft Intune können private und firmeneigene Geräte geschützt werden, mit minimalem Aufwand. Daten und Apps des Unternehmens können ohne Registrierung der Geräte verwaltet und geschützt werden. Apps aus dem Microsoft-Umfeld (Outlook, Teams, OneDrive), sowie weitere Partner Apps, lassen sich so verwalten.
Mittels App-Schutzrichtlinien besteht die Möglichkeit, den Benutzern App-Einstellungen zuzuweisen, welche beispielsweise die Extrahierung von Daten verhindern oder einen zusätzlichen Sicherheitsfaktor verlangen, um auf die jeweilige App zugreifen zu können. Zudem lässt sich die Speicherung von Daten an einem privaten Speicherort verhindern.
Bei einer Bring Your Own Device (BYOD)-Strategie ist dieses Vorgehen ideal. Die geschäftlichen Daten sind geschützt und kontrollierbar. Die Privatsphäre der Benutzer wird dabei nicht verletzt. Voraussetzungen dafür sind der Einsatz von Microsoft Exchange Online oder Exchange Server mit Hybrid Modern Authentication. Die Intune-Lizenzen (pro User) sind Microsoft 365- oder Enterprise Mobility-Plänen enthalten.

Die first frame networkers ag setzt intern ebenfalls auf die MAM-Lösung mit Microsoft Intune, da keine zusätzlichen Lizenzkosten anfallen (Intune in Microsoft 365 E3 & E5 inkludiert) und bereits eine Microsoft-Strategie besteht. Die Lösung bietet den Mitarbeitern einen guten Kompromiss zwischen Usability und Security, wobei die Privatsphäre der Mitarbeiter bewahrt und die Akzeptanz einer solchen Lösung erhöht wird.

Lizenz-Voraussetzungen

- Microsoft Exchange Online oder Exchange Server mit Hybrid Modern Authentication.
- Intune-Lizenz (pro User).
  Intune ist in folgenden Lizenzen inkludiert:
  - Microsoft Intune
  - Microsoft 365 E3 & E5
  - Enterprise Mobility & Security E3 & E5
  - Microsoft 365 Business Premium
  - Microsoft 365 F1 & F3
  - Microsoft 365 Government G3 & G5
  - Intune for Education
  - Microsoft 365 A3 & A5 (Schulen)

FAZIT: Private Smartphones und Tablets werden oft schlecht geschützt, obwohl sie auch für geschäftliche Kommunikation genutzt werden. Mobile Application Management (MAM) ist auf den Schutz der Unternehmensdaten fokussiert. Die Microsoft-Lösung mit Intune schützt private und firmeneigene Geräte mit minimalem Aufwand. Die nötigen Lizenzen sind in vielen Microsoft 365-Plänen enthalten.

Interessiert?

Die first frame networkers stehen Ihnen für weitere Auskünfte gerne zur Verfügung.
Sie erreichen uns über verkauf@firstframe.net oder +41 41 768 08 00.

first frame networkers ag
haldenstrasse 1
ch – 6340 baar

www.firstframe.net
+41 41 768 08 00