Container-Lösung auf iOS-Geräten

ALLGEMEIN

Die Container-Lösung für iOS ermöglicht die Trennung von geschäftlichen und privaten Daten auf nur einem Gerät. Damit werden BYOD- (**B**ring **Y**our **O**wn **D**evice) und COPE-Programme (**C**ompany **O**wned **P**rivatly **E**nabled) für Unternehmen mit Apple-Geräten möglich. Firmendaten und Netzwerken bleiben gesichert, während gleichzeitig die Privatsphäre der Nutzer geschützt wird, weil die Administratoren keine tiefen Einblicke sowie Kontrolle private Daten der Geräte erhalten.

FUNKTIONSWEISE

Die Trennung der Bereiche basiert auf einer Trennung der Apple-IDs. Neben der privaten Apple-ID wird auch eine durch die Firma oder Bildungsreinrichtung verwaltete Apple-ID auf dem Gerät installiert. Dadurch werden Daten und Apps getrennt und haben keinen Zugriff auf den jeweils anderen Bereich.

Allgemein unterscheidet Apple zwischen zwei Arten von Apps:

- Apps, die vom MDM installiert werden (Managed Apps)
- Apps, die vom User aus dem Store geladen werden (Unmanaged Apps)

MANAGED APPS

Managed Apps sind Unternehmens-Apps, die über das MDM installiert werden und mit der geschäftlichen Apple-ID verknüpft sind.

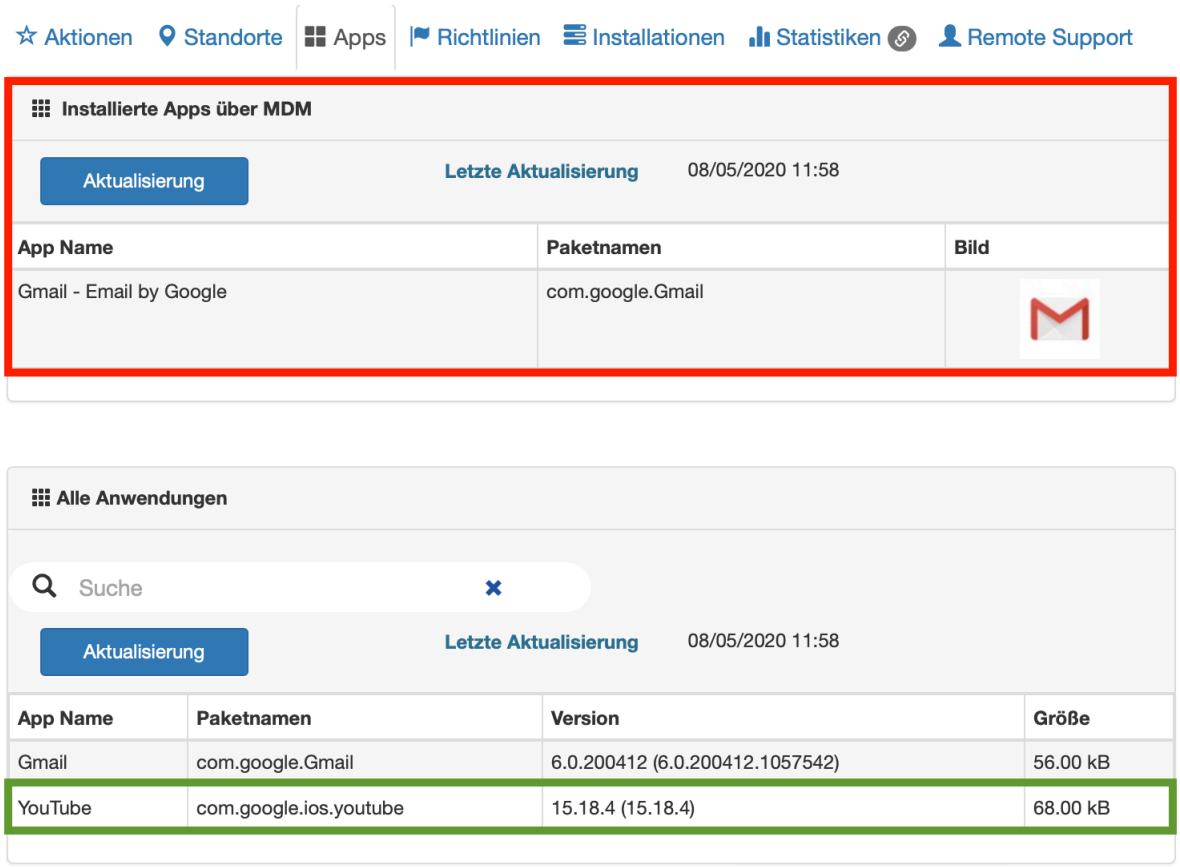
Das Ziel von Managed Apps ist es, Unternehmensdaten zu schützen, auf die der User Zugriff hat. Managed Apps werden durch die IT-Abteilung im Unternehmen installiert und verwaltet. Dadurch können Richtlinien festgelegt werden, welche die Interaktion mit Unternehmensdaten einschränken können z.B.:

- Zugriff auf bestimmte Websites
- Übertragung von Daten zwischen Anwendungen
- Speichern von Dateien
- Kopier- und Einfügevorgänge
- PIN-Zugriffsanforderungen
- Erstellung von Screenshots

UNMANAGED APPS

Unmanaged Apps sind private Apps, die wie gewohnt aus dem App Store geladen werden können und mit der privaten Apple-ID verknüpft sind.

Unamanged Apps können nicht durch Richtlinien eingeschränkt werden, gelöscht oder installiert werden. Damit wird sichergestellt, dass die Nutzer in keiner Weise eingeschränkt werden und immer die volle Kontrolle über ihre privaten Daten behalten.



Beispiel: Gmail ist auf dem Gerät als Managed App (rot) installiert, während YouTube als Unmanaged App (grün) installiert ist.

VORTEILE

Der entscheidende Vorteil der Container-Lösung ist die Datentrennung. Durch den Einsatz von Managed und Unmanaged Apps kann verhindert werden, dass bspw. geschäftliche Kontakte mit WhatsApp synchronisiert werden. Unternehmen können ihre Daten schützen, ohne den Benutzer einzuschränken. Dadurch können Firmen BYOD- und COPE-Programme datenschutzkonform anbieten, was für die Mitarbeiter Vorteile hinsichtlich der Flexibilität und Benutzerfreundlichkeit bringt und den Arbeitgeber gleichzeitig attraktiver macht.

UNTERSCHIED ZU ANDROID

Auch Android bietet eine Container-Lösung mit ähnlicher Funktionsweise an. Die wesentlichen Unterschiede liegen im App-Management. Während bei Android eine App doppelt im geschäftlichen UND im privaten Bereich installiert werden kann, muss bei iOS entschieden werden, ob eine App geschäftlich (gemanaged) ODER privat (ungemanaged) installiert werden soll. Möchte man bspw. Gmail geschäftlich und privat auf einem iOS-Gerät benutzen und die Daten trennen, muss für einen der Bereiche auf eine unabhängige Mail-App zurückgegriffen werden. Für den Geschäfts-Bereich eignet sich in diesem Fall z.B. **MobiVisor Secure Mail** optimal, wodurch zusätzliche Sicherheitseinstellungen und -richtlinien ganz einfach festgelegt werden können.