

Merkblatt

«Nutzung von Apps auf dienstlich verwendeten Mobilgeräten in der Bundesverwaltung»

Was muss ich wissen?

Die Nutzung von IKT-Anwendungen des Bundes mit Mobilgeräten ist generell mit der «Einsatzrichtlinie Smartphone/Smarttablet Sync E021» geregelt.
[E021 - Einsatzrichtlinie Smartphone/Smarttablet Sync](#)

Dieses Merkblatt enthält Empfehlungen des Bundes zur Nutzung von Apps auf dienstlichen Mobilgeräten und auf privaten Mobilgeräten, die dienstlich genutzt werden. Es richtet sich an die Mitarbeitenden des Bundes.

04/2023



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

Apps zurückhaltend installieren

Jede zusätzliche App stellt ein potentiell Sicherheitsrisiko dar. Deshalb sollten Sie Apps, die Sie nicht mehr benötigen, löschen. Je weniger Apps, desto besser der Überblick und geringer die Sicherheitsrisiken. Überprüfen Sie die installierten Apps regelmässig.

Empfehlung

- Installieren Sie nur Apps, die Sie tatsächlich benötigen.
- Löschen Sie Apps, die Sie nicht mehr benötigen.

Apps aktuell halten

Apps, die nicht auf aktuellem Stand sind, können ein Sicherheitsrisiko darstellen. Überprüfen Sie regelmässig, ob Updates für Apps zur Verfügung stehen und installieren Sie diese umgehend.

Empfehlung

- Halten Sie Ihre Apps immer auf aktuellem Stand. Am besten richten Sie die Apps so ein, dass die Updates automatisch durchgeführt werden.

Berechtigungen erteilen

Wenn Apps zum ersten Mal in Gebrauch sind, oder manchmal auch bei Updates, werden die Berechtigungen der App abgefragt. Viele Apps greifen dabei auf persönliche Daten zu. Über die Einstellungen Ihres Mobilgerätes können Sie das verhindern.

Empfehlung

- Vergeben Sie Berechtigungen (z. B. den Zugriff auf das Adressbuch) nur, wenn Sie die Funktion zwingend benötigen. Im Zweifelsfall lehnen Sie die Berechtigung ab. Unter «Einstellungen» können Sie die Berechtigungen nachträglich immer noch vergeben.
- Prüfen Sie für jede App, welche Art von Zugriff gestattet ist.

Social Media-Apps

Social Media-Apps dürfen auf dienstlichen Mobilgeräten installiert werden (Instagram, Facebook, TikTok usw.). Social Media-Apps erhalten aber potentiell sehr weitreichende Berechtigungen und sind bekannt dafür, besonders viele Daten, wie beispielsweise Kontaktdaten, zu sammeln.

Empfehlung

- Prüfen Sie, ob Sie die Apps wirklich auf dem dienstlich genutzten Mobilgerät benötigen.
- Geben Sie den Apps so wenig Rechte wie möglich.
- Beachten Sie im Umgang mit Social Media zusätzlich den Leitfaden des EPA.

Ortungsdienste

Die Ortungsdienste greifen nicht nur in Ihre Privatsphäre ein, sondern verbrauchen zusätzlich Akkuleistung. Einige Apps funktionieren nicht ohne den Zugriff auf bestimmte Funktionen wie Ortungsdienste. Steuern Sie diesen Zugriff bei Gebrauch manuell. Unter den «Ortungsdiensten» finden Sie alle Apps, die Zugriff auf Ihren Standort verlangen und können dies manuell einstellen.

Empfehlung

- Benötigen Sie die Ortungsdienste in einer App nicht, können Sie diese komplett ausschalten. Öffnen Sie dazu die «Einstellungen», wählen Sie dort die Kategorie «Datenschutz & Sicherheit» aus.



Datenschutz und Sicherheit

- Häufig reicht die Ortungsoption «Beim Verwenden», statt «immer».



Swisstopo



Beim Verwenden >

Vertrauliche Kommunikation

Für die vertrauliche Sprachkommunikation (Telefon, Sprachnachrichten und Chat) steht den Mitarbeitenden mit verwalteten Mobilgeräten (MDM) die App «Threema Work» zur Verfügung.

Empfehlung

- Für heikle, interne Gespräche und/oder Chats verwenden Sie die Apps «Threema Work» oder «Skype for Business».
- Für vertrauliche Gespräche verwenden Sie ausschliesslich «Threema Work».
- Führen Sie keine geschäftlichen Unterhaltungen über Messengers von Drittherstellern, ausser den hier erwähnten.

Vorgabe

E027 – Einsatzrichtlinie: Verschlüsselte Sprachkommunikation auf Smartdevice

Bedeutung der Statussymbole

Beobachten Sie die Statusleiste auf dem Bildschirm. An den Symbolen können Sie jederzeit erkennen, wenn eine App Ortungsdaten sammelt oder Funkschnittstellen aktiviert. Laufen Aktivitäten, ohne dass Sie diese bewusst genutzt haben, sollten Sie der Ursache auf den Grund gehen, indem Sie überprüfen, welche Apps gerade aktiv sind.

Empfehlung

Achten Sie stets darauf, welche Statuszeichen in der Statusleiste beim iPhone angezeigt werden.



Eine App oder eine Website verwendet Ihren Standort (Ortungsdienste).



Dieses Symbol, deutet darauf hin, dass Netzwerkaktivitäten stattfinden die z. B. von Apps verwendet werden.



Anrufweiterleitung ist aktiviert.



Eine App verwendet das Mikrofon des Geräts.



Eine App verwendet entweder die Kamera oder die Kamera und das Mikrofon des Geräts.



Das Gerät nimmt entweder gerade Ton auf oder erstellt ein Bildschirmfoto.

Bei Verdacht auf Unregelmäßigkeiten, nehmen Sie Kontakt mit dem Servicedesk Ihres Leistungserbringers auf.

Benutzung des Mobilgerätes im Ausland

Auf Auslandsreisen gilt eine besondere Sorgfaltspflicht im Umgang mit Apps.

In einzelnen Ländern ist es den Grenzbehörden erlaubt, Apps zu untersuchen. Um dies zu verhindern, müssen Sie die MDM-Secure-Apps (Secure Mail, Secure Notes, Secure Tasks) vor der Einreise in das jeweilige Land deinstallieren. Sind zwingend Apps (z. B. aufgrund von Vorgaben des jeweiligen Landes) nötig, sollte dafür ein separates Mobilgerät verwendet werden.

Empfehlung

- Nehmen Sie nur die wirklich benötigten Geräte auf Auslandsreisen mit.
- Für exponierte Personen, welche unter diplomatischem Status reisen, gelten besondere Bestimmungen. Insbesondere bezüglich der Offenlegung von Informationen. Erkundigen Sie sich dazu bei Ihrem Amt oder VIP-Support über die entsprechenden Vorschriften und Möglichkeiten.
- Reisehinweise des EDA:
[EDA - Reisehinweise](#)
- Website NCSC - Reisen ins Ausland:
[NCSC - Auslandsreisen](#)

Wechsel des Mobilgerätes

Wenn ein Gerät ausgewechselt wird, bleiben viele Daten auf den Mobilgeräten gespeichert.

Empfehlung

- Sorgen Sie dafür, dass Ihre Daten bei einem Gerätewechsel gelöscht werden.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC