FAQ Datentrennung auf Handys

Antworten auf die häufigsten Fragen

Von Jörg Wirtgen

Daten in US-Clouds

? Darf ich meine Daten auf Servern von US-amerikanischen Anbietern speichern?

! Rein private Daten dürfen Sie überall speichern. Sobald geschäftliche Daten auf dem Smartphone gespeichert sind, greift allerdings auch für Privatanwender das Bundesdatenschutzgesetz, das die Speicherung von personenbezogenen Daten außerhalb der EU nur bei Diensten erlaubt, die sich nach dem „EU-US Privacy Shield“ selbst beim US-Handelsministerium zertifiziert haben. Das sind mittlerweile recht viele, darunter Amazon, Dropbox, Google, Microsoft.

Allerdings gelten die Zertifikate nicht immer für sämtliche Geschäftsbereiche und Datenarten. Bevor Sie also Daten zu einem US-Unternehmen übertragen, sollten Sie folglich dessen Privacy-Shield-Zertifikat studieren (privacyshield.gov/list).

Ein weiteres Problem: Egal ob berufliche oder private Daten, egal ob erlaubt oder nicht: US-Behörden bekommen auch bei den zertifizierten Unternehmen Zugriff auf die gespeicherten Daten. Wenn Sie das verhindern wollen, müssen Sie auf EU-Server ausweichen oder die Daten verschlüsseln (siehe c’t 21/16, S. 116).

Wieso überhaupt Datentrennung

? Was ist das Problem mit der Datentrennung auf Smartphones?

! Die Smartphones mit Android, iOS und Windows 10 Mobile haben bezüglich Datenschutz zwei Schwachstellen: Erstens benötigen sie einen Account bei Google, Apple oder Microsoft, auf dem man leicht aus Versehen personenbezogene Daten speichert – vor allem Kontakte und Termine landen schnell dort, aber auch Mails oder Mail-Anhänge. Das mag ein Verstoß gegen das Bundesdatenschutzgesetz sein und gibt unter Umständen US-Behörden Zugriff auf die Daten.

Die zweite Schwachstelle sind die Apps: Sie bekommen leicht Zugriff auf Adressbuch und Terminkalender. So gelangen diese Daten zu weiteren Firmen, worüber man keine Kontrolle mehr hat. Das ist auf jeden Fall unangenehm und im Fall von personenbezogenen geschäftlichen Daten ein Verstoß gegen den deutschen Datenschutz.

Rechte der Apps einschränken

? Ich kann windigen Apps einfach den Zugriff aufs Adressbuch sperren. Das geht unter Android, iOS und Windows 10 Mobile mittlerweile ganz gut. Löst das nicht das Problem?

! Die Mobilbetriebssysteme können den Zugriff nur komplett sperren oder gewähren. Will man etwa WhatsApp für private Kontakte nutzen, sieht die App auch sämtliche Geschäftsadressen.

Darüber hinaus ist es für ein Unternehmen unverantwortlich, den Mitarbeitern die Arbeit aufzudrücken, ständig jede App auf Sicherheitsprobleme abzuklopfen und die Rechte entsprechend zu vergeben.

Lösungen für Einzelanwender

? Wie kann ich als Privatanwender das berufliche und private Adressbuch trennen?

! Dazu bieten sich Exchange-Container an: Das sind Apps zum Zugriff auf Exchange-Konten (Mail, Adressen, Termine, Notizen, Aufgaben), die nichts ins Mobilsystem weitergeben, sondern nur innerhalb der App Zugriff auf die Daten bieten. Eine beliebte App ist TouchDown, für Android kommt auch Nine von 9Folders in Frage. Mail-Attachments landen allerdings doch wieder schnell im offenen Bereich oder gar einer US-Cloud (siehe c’t 21/16, S. 122).

Getrennte Apps

? Exchange-Container helfen nur für Mails oder Termine, nicht aber für Apps. Wie gewähre ich etwa einem Messenger Zugang zu den Firmenkontakten?

! Auf vielen Android-Smartphones kann man mehrere Nutzerkonten anlegen. Die beruflichen Daten bindet man dann unter einem eigenen Konto ein und installiert dort nur vertrauenswürdige Apps, denen man bedenkenlos vollen Zugriff auf alle Adressen und Termine geben kann. Misstraut man allerdings Google und möchte daher in diesem Nutzerkonto keinen Google-Account eintragen, kommt man nicht mehr per Play Store an die Apps, sondern nur umständlich über alternative Stores.

Neuere Samsung-Smartphones beherrschen MyKnox. Das ist eine spezielle Art eines Nutzerkontos, in dem man ohne Google-Account alle Apps des Hauptkontos nutzen kann – mit separatem Datensatz, also eigener getrennter Konfiguration (siehe c’t 21/16, S. 122). Vergleichbare Lösungen für andere Handys sowie iOS und Windows 10 Mobile kennen wir nicht.

Lösungen für Firmen

? Wie behält eine Firma Kontrolle über ihre Daten und hilft den Mitarbeitern bei der Konfiguration?

! Für Firmen bieten sich Container-Lösungen an – Stichwort MDM (Mobile Device Management) und EMM (Enterprise Mobility Management). Hierbei werden zum einen Daten und Apps komplett von der privaten Nutzung getrennt, zum anderen bekommt die Firma von außen Zugriff auf diesen Container. Lösungen existieren unter anderem für Android, iOS und Windows 10 Mobile. Cloud-Lösungen kosten ab drei Euro pro Monat und Gerät (siehe c’t 21/16, S. 132). *(jow@ct.de)*