DATENSICHERHEITSPROBLEME BEI GESCHÄFTLICHER NUTZUNG DES PRIVATEN SMARTPHONES

«Bring Your Own Device»

Haben Sie sich privat ein Smartphone oder ein Tablet zugelegt? Z.B. ein schickes Apple iPhone oder eines mit dem Google-Betriebssystem Android? Brauchen Sie dieses private Gerät z.B. für geschäftliche E-Mails? Synchronisieren Sie geschäftliche Termine und Kontakte mit Ihrem Smartphone? Ja? Das ist «Bring Your Own Device».

TEXT MICHAEL H. QUADE

Ein Smartphone oder Tablet kann eigentlich alles, was der Computer am Arbeitsplatz auch kann. Es braucht dafür nur die entsprechenden Programme. Die Geräte können standardmässig E-Mails und Office-Dokumente verarbeiten sowie PDF-Dateien öffnen. Im Internet surfen klappt in der Regel problemlos. Auch kann man die Funktion mit sogenannten Apps beliebig erweitern. Apps sind ja nichts anderes als Programme, und wer ein Smartphone oder Tablet hat, weiss, dass eine App aus dem Store von Apple oder Google innert Sekunden installiert ist.

Apps können Spiele sein oder kleine Anwendungen, die einem dabei helfen, Notizen zu verwalten. Es gibt auch Apps, die einen für die Smartphone-Anzeige optimierten Zugriff auf Dienste wie Facebook oder Twitter ermöglichen. Ausserdem gibt es Apps für die kostenlose Kommunikation wie z.B. Skype oder WhatsApp. Immer mehr Software-Anbieter für Business Software bieten ihre Client-Programme als App an. So haben z.B. die ERP-Systemanbieter ABACUS und Sage bereits Client-Apps für ihre Software-Lösungen entwickelt.

Die Datensicherheit ist das Problem

Das Problem bei Apps ist nun aber, dass diese Berechtigungen verlangen, um bestimmte Funktionen auf dem Smartphone oder Tablet zu nutzen. Betreffend Datensicherheit gibt es heikle und weniger heikle Berechtigungen. Sehr heikel sind die Berechtigungen, die z.B. den Datenzugriff auf die Kontakte im Telefon oder auf die Anruferliste erlauben. Nicht minder heikel sind solche, die den Zugriff auf die lokal auf dem Smartphone oder Tablet gespeicherten Daten, die eingerichteten E-Mail-Konten oder den aktuellen Standort ermöglichen.

Ausgesprochen heikel wird es dann, wenn Mitarbeitende ihre privaten Geräte unbedarft auch für geschäftliche Aktivitäten nutzen, eben «Bring Your Own Device», wenn gegebenenfalls z.B. der ganze Kundenstamm unter «Kontakte» abgespeichert ist. Oder wenn die Mitarbeitenden Kunden mit ihrem privaten Smartphone anrufen, auch wenn die dabei eingesteckte SIM-Karte vom Arbeitgeber ist. Apps mit entsprechenden Berechtigungen können dann auch diese Daten mitlesen.

Und da das Gerät dem Mitarbeitenden gehört, kann dieser ja installieren und mit dem Gerät machen, was er will. Denn die eingesteckte SIM-Karte und das Konto, mit dem man auf den App-Store zugreifen kann, sind voneinander losgelöst. Das heisst: Eine SIM-Karte des Arbeitgebers verhindert nicht, dass man auf dem Gerät installieren kann, was man will.

Daten bleiben auch oft auf dem Smartphone des Mitarbeitenden gespeichert, wenn dieser das Unternehmen verlässt. Wer denkt beim Austritt eines Mitarbeitenden daran, dessen privates Smartphone zu kontrollieren?

Wie soll man mit BYOD umgehen?
Bei sehr hohem Sicherheitsbedarf gibt es die Variante, «Bring Your Own Device» komplett zu verbieten und den Mitarbeitenden Smartphones oder Tablets bereitzustellen. Diese können dahingehend konfiguriert werden, dass die Daten sicher sind. Nur der IT-Support darf das Gerät konfigurieren und neue Anwendungen installieren. Anwendungen können auch über einen unternehmensinternen App-Store bereitgestellt werden. Das heisst: Alles, was auf dem Smartphone installiert und genutzt wird, ist durch das Unternehmen kontrollierbar. Für ein kleines Unternehmen mit wenigen Mitarbeitenden ist diese Variante jedoch zu teuer und zu aufwendig.

Eine weitere Variante bei hohem Sicherheitsbedarf ist, dass das Unternehmen eine spezialisierte App auf dem privaten Gerät installieren lässt. Eine App, welche private und geschäftliche Daten trennt. Solche Anwendungen setzen jedoch in der Regel auch noch Softwaresysteme wie z.B. Microsoft Exchange beim Unternehmen voraus. Diese sind nicht notwendigerweise in jedem Unternehmen im Einsatz.

Organisatorische Massnahmen
Für weniger hohen Sicherheitsbedarf gibt es ein paar Massnahmen organisatorischer und technischer Art, die auch für kleine Unternehmen durchaus im Bereich des Möglichen liegen. Die erste organisatorische Massnahme sollte die Erstellung eines Inventars sein (was natürlich auch bei hohem Sicherheitsbedarf Sinn hat). Wer im Unternehmen wendet BYOD an? Welche geschäftlichen Daten nutzen die Mitarbeitenden auf ihren Geräten? Welchen Sicherheitsbedarf haben diese Daten? Mit der Erstellung eines Inventars kann ein Unternehmen gleich prüfen, ob ein Bedarf an BYOD besteht. Denn mit BYOD können sich dem Unternehmen auch neue Möglichkeiten erschliessen, die zur Verbesserung der Geschäftsprozesse führen.

Die zweite organisatorische Massnahme ist eine Richtlinie oder Weisung. Mitarbeitende können durch eine Weisung für das Thema BYOD und die oben erwähnten möglichen Zugriffe auf Daten durch Apps sensibilisiert werden. In der Weisung können die Mitarbeitenden auch in die Pflicht genommen werden, einfache technische Massnahmen auszuführen, welche die Sicherheit erhöhen.
Die Weisung sollte auch die rechtliche Situation regeln. Hierzu sollte sich das Unternehmen Antworten auf die folgenden Fragen erarbeiten:
– Wem gehört das Gerät?
– Wem gehören welche Daten?
– Auf welche Daten darf mit dem privaten Gerät zugegriffen werden und auf welche nicht?
– Wer kommt für allfällige Lizenzkosten auf?
– Wie wird vorgegangen bei Verlust des Gerätes oder wenn das Gerät im geschäftlichen Einsatz ausfällt?
Die Antworten auf diese Fragen sind umso wichtiger, je stärker ein Unternehmen auf BYOD setzt.

Einfache technische Massnahmen
Die erste und einfachste technische Massnahme ist es, den Passcode zu aktivieren. Eine Zahl, die man jedes Mal eingeben muss, wenn man das Telefon «aufweckt». Die zweite Massnahme ist die Verschlüsselung aller Daten auf dem Smartphone oder Tablet. Das aktuelle Betriebssystem Android kann das standardmässig. In den Einstellungen ist einfach die entsprechende Option zu aktivieren (allerdings dauert es danach einen Moment, bis alle Daten verschlüsselt sind und das Gerät wieder benutzt werden kann). Beim iPhone oder iPad sind mit der Version 5 des Apple-Betriebssystem IOS einige Daten verschlüsselt, wenn man das Telefon mit dem Passcode schützt. Man kann bei IOS auch die komplette Löschung aller Daten aktivieren, falls der Passcode mehrere Male falsch eingegeben wurde.

Die zweite einfache technische Massnahme besteht darin, eine App zu installieren, welche das System und die Daten vor Gefahren schützt. Das kennen Sie sicher von Ihrem Arbeitsplatzrechner: Installieren Sie ein Virenschutzprogramm! Dabei unterscheiden sich die Funktionen der Virenschutzprogramme für Smartphone und Tablet leicht von der PC-Version: Diese Virenschutzprogramme kontrollieren in der Regel schon bei der Installation einer neue App, ob diese als sicher eingestuft ist oder nicht (was mit den oben erwähnten Berechtigungen zu tun hat).

Die meisten Schutz-Apps bieten Funktionen zur Fernlöschung von Daten, wenn das Gerät z.B. gestohlen wurde. Dazu muss man sich beim Anbieter des Virenschutzprogramms nur mit seinem Gerät registrieren. Das funktioniert im Übrigen auch, wenn eine andere SIM-Karte eingelegt wurde.

DER AUTOR

Michael H. Quade ist Dozent für Wirtschaftsinformatik an der Fachhochschule Nordwestschweiz FHNW. Im Rahmen der Business-Software-Studie 2012 beschäftigt er sich mit dem Thema BYOD und Mobile Device Management.
michael.quade@fhnw.ch