USB-Schnittstelle: Schadsoftware könnte beim Datenaustausch oder beim Aufladen übertragen werden.

Die Hälfte der Smartphone- und Tablet-Benutzer verwendet keine Passwörter, Sicherheitssoftware oder Back-up-Systeme.

Sicher am Smartphone

Das Sicherheitsbewusstsein vieler Nutzer mobiler Kommunikationsgeräte ist gering. IT-Experten des BMI geben Tipps, worauf man im Umgang mit mobilen Geräten achten sollte.

Laut dem Internet-Sicherheitsbericht 2013 der Computer Emergency Response Teams *CERT.at* und *GovCERT.at* verwendet die Hälfte der Smartphone- und Tablet-Benutzer keine Passwörter, Sicherheitssoftware oder Back-up-Systeme. Mehr als die Hälfte der Nutzer wissen nicht, dass es für mobile Geräte Sicherheitssysteme und -produkte gibt. Etwa die Hälfte der Menschen nutzen ihre mobilen Geräte auch in der Arbeit.

Aufgrund ihres Funktionsumfangs und der Möglichkeit, beinahe uneingeschränkt auf Unternehmensdaten zuzugreifen, bergen diese „Minicomputer" Risiken. Viele Unternehmen verwenden veraltete Software und tauschen diese nicht aus – trotz Kenntnis über deren Schwachstellen. Mit dem Einsatz der richtigen Schutzsoftware, Information und Schulung der Mitarbeiterinnen und Mitarbeiter könnte man sich vor Angriffen auf Unternehmen schützen.

IT-Sicherheitsexperten des Bundesministeriums geben Tipps, worauf man bei der Nutzung von mobilen Geräten wie Smartphones und Tablets achten soll:

Tastensperre und PIN-Code. Mobile Geräte sollten mit einem Passwort oder Pin-Code gesperrt werden. Die Gerätesperre soll automatisch nach einer bestimmten Zeit aktiv werden. Das schützt vor unberechtigten Zugriffen. Es sollen starke Passwörter oder Zahlen-Buchstaben-Kombinationen verwendet werden. Zahlen-Buchstaben-Pins sind gegenüber Wischmustern zu bevorzugen, da Wischmuster zwar leichter zu merken sind, aber einfacher ausgespäht werden können. Es wird empfohlen, das Display regelmäßig zu reinigen, da bei der längeren Verwendung desselben Wischmusters Fingerspuren am Display hinterlassen werden.

Vermieden werden sollten einfache Zahlenkombinationen oder naheliegende Werte wie Geburtsdaten, da diese Kombinationen häufig benutzt werden und die Gefahr für einen unerlaubten Zugriff erhöhen. Ein starkes Passwort sollte zwischen zehn und zwölf Zeichen haben und aus einer Kombination aus Buchstaben, Zahlen und Zeichen bestehen.

Drahtlosverbindungen. Immer öfter werden WLANs (Funknetzwerke) in öffentlichen Bereichen zur freien Nutzung angeboten. Hier ist Vorsicht geboten. Unverschlüsselte Daten können bei der Übertragung mitgelesen werden – auch Zugangsdaten wie Benutzername und Kennwort. Zudem kann es über WLAN oder Bluetooth unbemerkt zur Installation von Schadsoftware kommen. Deshalb sollten Funktionen wie Bluetooth oder WLAN nur für den Zeitraum der Nutzung aktiviert werden. Dies gilt ebenso für GPS damit keine Positionsdaten mitprotokolliert werden können.

Umsichtige Internetnutzung. Die Kommunikation mit mobilen Geräten erfordert die gleiche Sorgfalt wie mit stationären Geräten. Schadsoftware für mobile Geräte verbreitet sich zunehmend. Internet-Browser bieten breite Angriffsflächen für Schadcodes.

Die Nutzung des Internets mit mobilen Geräten sollte auf ein unbedingt notwendiges Maß reduziert werden und sich auf vertrauenswürdige Web-Angebote beschränken.

Schadsoftware kann in eingebetteten Werbebannern auf Webseiten enthalten sein. Die Aktivierung des eingebetteten Inhalts z. B. durch das Anklicken von Werbebannern kann genügen, um Schadsoftware auf dem eigenen mobilen Endgerät zu installieren.

Datenbereinigung. Wer im Internet surft, hinterlässt Spuren. Nicht unbedingt notwendige Daten sollten von mobilen Geräten gelöscht werden. Vor allem die Download-Ordner, temporäre Internet-Dateien, Multimediadaten (Bilder, Videos u. a.), Dateianhänge von E-Mails, Internet-Historien und Cookies.

USB-Schnittstelle. Der Datenaustausch zwischen mobilen und stationären Geräten über eine USB-Schnittstelle kann ein Risiko darstellen. Schadsoftware könnte beim Datenaustausch sowie beim Aufladevorgang über die USB-Schnittstelle übertragen werden. Mobile Geräte sollten nur mit Original-

Fotos: Alexander Tuma, Egon Weissheimer

Mobile Geräte sollten mit einem Passwort oder PIN-Code gesperrt werden.

Nutzung privater Smartphones in der Arbeit: Risiken bestehen in der Möglichkeit, beinahe uneingeschränkt auf Unternehmensdaten zugreifen zu können.

zubehör (Ladegeräten) und möglichst über eine Stromsteckdose geladen werden und nicht über den USB-Anschluss von Notebooks oder PCs.

Onlinekonten. Die Nutzung mobiler Geräte ist meist mit der Notwendigkeit verbunden, Benutzerkonten für Dienste wie *iTunes, Google+, live.com* u. a. bei verschiedenen Anbietern einzurichten. Diese Konten stellen nicht nur Angebote wie „Apps" zur Verfügung, sie bieten oft zusätzliche Leistungen wie Ortungs-, Cloud- und Fernwartungsfunktionen an. Wenn man diese Zusatzfunktionen erlaubt, gibt man Informationen preis, die der jeweilige Diensteanbieter speichert.

Diese Daten sind auch Ziel von Ausspähungen. Wer ein Firmengerät benutzt, sollte aus Sicherheitsgründen kein derartiges Benutzerkonto einrichten. Besteht dennoch Bedarf, ein Benutzerkonto für ein beruflich verwendetes mobiles Gerät einzurichten, wird empfohlen, als Benutzername keine Namen zu verwenden, die Rückschlüsse auf die Identität der Person oder Organisation zulassen. In diesen Fällen sollte danach getrachtet werden, dass dem Benutzerkonto – sofern erforderlich – keine personalisierte Kreditkarte zugewiesen wird, sondern „Pre-paid"-Varianten benutzt werden.

Synchronisation von E-Mails. Berufliche Mails werden vor der Zustellung von firmeneigenen Virenscannern überprüft, wenn sie mit dem beruflichen Smartphone synchronisiert werden. Die Synchronisation von privaten E-Mails auf „Unternehmens"-Smartphones ist problematisch, da vor allem Gratis-E-Mail-Anbieter kaum einen Virenschutz bieten und Anhänge und Links ein Risiko für die Sicherheit der oftmals sensiblen beruflichen Daten am Gerät darstellen.

Es sollten selbst bei beruflichen E-Mails Anhänge nur bei absoluter Notwendigkeit und grundsätzlicher Vertrauenswürdigkeit des Absenders abgerufen werden.

Installation von Apps. Trotz Sicherheitsmaßnahmen der diversen App-Store-Anbieter gelangen immer wieder „bösartige" Apps in den Store. Schadsoftware kann sich dabei auch über Werbebanner, die bei Benützung der App eingeblendet werden, installieren. Das ermöglicht Kriminellen den Zugriff auf Zugangskennungen und Daten auf dem Gerät.

Apps fordern zum Funktionieren bestimmte Rechte vom Betriebssystem ein, die unter Umständen den Zugriff auf das Adressbuch, den Telefonspeicher u. a. ermöglichen. Diese Informationen können ausgelesen und an den App-Hersteller oder Dritte weitergegeben werden.

Ein Beispiel dazu ist das Programm zum Austausch von Nachrichten „WhatsApp". Es gehört zu jenen Apps, die sich bei der Installation je nach Betriebssystem durchaus fragwürdige Berechtigungen vom Anwender genehmigen lassen. Dadurch werden die Kontaktdaten im Telefon und die gesamte Kommunikation an die „WhatsApp"-Server übermittelt.

Man muss sich dieses Umstands bei der Nutzung von Apps bewusst sein. Überwiegend Gratis-Apps „leben" von der weiteren Verwertung dieser personenbezogenen Informationen.

Das Auslesen von personenbezogenen Informationen aus dem mobilen Gerät und Übertragen an externe Server kann unter Umständen auch durch bereits am Gerät vorinstallierte Apps erfolgen. Da diese meist nicht gelöscht werden können, ist es empfehlenswert, diese Apps zu deaktivieren (z. B. Wetter-Apps, Karten-Apps) oder umsichtig zu nutzen.

Cloud-Services wie *iCloud, Google Drive, Skydrive, Dropbox* u. a. sollten mit einem beruflich genutzten Gerät nur bei Vorgabe durch den Arbeitgeber genutzt werden. Der Speicherort und die Zugriffsrechte auf Daten (Kontaktdaten, Kalenderdaten …) sind bei einem Cloudspeicher zumeist nicht klar definiert. Dadurch werden berufliche Daten der eigenen Verfügungsgewalt und Kontrolle entzogen. Man kann zur Datensicherheit beitragen, indem man die Sicherheitsempfehlungen einhält und Smartphones umsichtig benutzt.

Weitere Informationen: www.onlinesicherheit.gv.at

Fotos: Alexander Tuma