SICHERHEIT VON MOBILEN GERÄTEN UND DATENTRÄGERN

Rainer Helfrich – E-Mail: helfrich@kepi.de – Oktober 2016

Einleitung

Ein Smartphone ist inzwischen ein Alleskönner, das hunderte von Funktionen in einem kleinen Gerät vereinigt. Nicht nur ist eine Vielzahl von privaten Informationen darin gespeichert, es enthält auch häufig Zugriff auf Zahlungsdienste (z.B. iTunes oder App Stores, kontaktloses Bezahlen mit NFC[1]). Umso schwerer wiegt der Schaden, wenn dieses in die falschen Hände gerät. Hier sollen Schutzmaßnahmen behandelt werden, um im Falle des Verlustes des Smartphones Schlimmeres zu verhindern.

Auch auf anderen mobilen Datenträgern wie USB-Sticks und mobilen Festplatten können sensible Daten liegen. Daher wird im Folgenden an den passenden Stellen auf entsprechende Techniken hingewiesen, um auch solche Geräte zu schützen.

Bildschirmsperre

Der erste Schritt sollte die Einrichtung einer Bildschirmsperre sein. Sobald das Smartphone auf Standby geschaltet wird (manuell oder nach einem bestimmten Zeitraum), muss der Nutzer sich identifizieren, um das Gerät wieder benutzen zu können. Je nach Gerät gibt es verschiedene Möglichkeiten, den Bildschirm zu entsperren:

- Zahlenkombination – der Nutzer muss eine vierstellige Zahl eingeben; hier sollte keine primitive Kombination wie „1234“ verwendet werden. Zudem hinterlässt man bei jeder Eingabe Fingerabdrücke auf dem Display, die einen Hinweis auf die Zahlen der Kombination geben. Der Bildschirm sollte daher regelmäßig gereinigt werden.
- Entsperrmuster – der Nutzer muss eine Reihe von Feldern in einer bestimmten Abfolge berühren. Hier besteht auch das Problem der Fingerabdrücke.
- Gesichtserkennung – mit der Kamera und biometrischen Daten erkennt das Gerät den rechtmäßigen Besitzer. Dieses System kann unter Umständen mit einem Foto des Besitzers ausgetrickst werden.
- Passwort – bei einem gut gewählten (langen) Passwort ist die Sicherheit am höchsten. Problem: Der Nutzer will vielleicht nicht jedes Mal ein Passwort einzugeben, wenn er das Handy benutzen will.

Verschlüsselung

Moderne Smartphone-Betriebssysteme können ihre Daten verschlüsseln, allerdings muss der Benutzer dies auf manchen Versionen manuell aktivieren. In diesem Fall kann man auf die Daten nur mit Kenntnis des Entsperrcodes zugreifen.

Um USB-Sticks oder Festplatten zu sichern, können diese auch verschlüsselt werden. Dabei gibt es zunächst die Möglichkeit, Verschlüsselungsprogramme wie z.B. VeraCrypt[2] zu verwenden.
Eine Anleitung finden Sie hier: *https://lehrerfortbildung-bw.de/werkstatt/sicherheit/stickcrypt/vc/*

Dieser Vorgehensweise hat den Nachteil, dass das Programm VeraCrypt auf jedem Computer vorhanden sein muss, auf dem auf die Daten zugegriffen werden soll. Wenn verschiedene

1 Near Field Communication – ein drahtloses Kommunikationsprotokoll, das Datenübertragung über Strecken von wenigen Zentimetern erlaubt. Es wird z.B. zum Bezahlen von kleineren Einkäufen (bis 25 €) ohne Unterschrift oder Eingabe einer PIN verwendet.
2 *https://veracrypt.codeplex.com/*

Betriebssysteme verwendet werden, ist das unter Umständen nicht immer der Fall.

Eine Alternative sind USB-Sticks und Festplattengehäuse, die auf Hardware-Ebene verschlüsseln. Bei diesen muss vor der Verwendung eine PIN über Tasten am Gerät eingegeben werden. Der Vorteil ist, dass diese Geräte ohne weitere Software auf allen gängigen Betriebssystemen funktionieren. Ein Nachteil ist allerdings der deutlich höhere Preis.

Diebstahlsicherung

Im Fall eines Diebstahls des Smartphones sollten die folgenden Schritte möglichst schnell ausgeführt werden:

- Sperren der SIM-Karte über den Anbieter. Die SIM-Karte wird in ein Handy eingesetzt, um den Kunden des Mobilfunkanbieters zu identifizieren. Ist die SIM-Karte gesperrt, kann der Dieb nicht mehr mit dem Gerät telefonieren oder ins Internet gehen.
- Anzeige bei der Polizei erstatten. Hier hilft es, die sogenannte IMEI-Nummer zu kennen, um das Gerät später identifizieren zu können. Diese kann auf dem Gerät durch Eingabe der Nummer „#06#“ oder über die Geräteeinstellungen abgefragt werden. Alternativ findet man sie auf der Originalverpackung oder der Rechnung.
- Die Hersteller der verbreiteten Betriebssysteme Android, iOS und Windows Phone bieten verschiedene Dienste zum Wiederfinden oder Sperren des Smartphones an, z.B. den „Android Geräte-Manager“ oder die „iCloud“. Wichtig: Machen Sie sich mit den Funktionen der Dienste vertraut, bevor der Ernstfall eintritt.
- Diebstahlschutz-Apps: Der Name ist etwas irreführend, weil keine App vor Diebstahl schützen kann. Es gibt aber Apps, die es ermöglichen, im Fall eines Diebstahls das Smartphone aus der Ferne zu orten, zu sperren oder zu löschen. Einen Vergleich verschiedener Diebstahlschutz-Apps finden Sie hier: *http://www.stern.de/digital/smartphones/was-tun--wenn-das-smartphone-weg-ist--3107034.html*

Datensparsamkeit

Generell sollte man sich gut überlegen, welche Daten auf dem Smartphone liegen sollten. Bankdaten oder Passwörter zu sensiblen Systemen haben z.B. nichts auf einem Gerät zu tun, das überall herumgetragen wird. Auch sollte man vorsichtig sein, welche Zahlungsoptionen man freischaltet. Im Falle eines Diebstahls kann der Dieb z.B. über den App Store digitale Waren kaufen. Zudem kann der Dieb Zugriff auf den E-Mail-Account erhalten. Da viele Online-Dienste eine Passwort-Rücksetzung per E-Mail anbieten, kann ein Angreifer auf diesem Weg die Identität des Eigentümers eines Smartphones übernehmen.

Weitere Materialien

http://www.klicksafe.de/themen/kommunizieren/smartphones/sicherheit-wie-schuetze-ich-das-smartphone/

https://www.netzwelt.de/handy-ortung/handy-verloren.html