Empfohlene Sicherheitsmaßnahmen aus Sicht eines Betreibers

Wien, 26.2.2015

Smartphones.

- Ihr Smartphone ist ein vollwertiger Computer.

- Ihr Smartphone enthält interessante Daten
    - Ihren Wohnort (z.b. in der Navigations-App)
    - Wann Sie in Urlaub fahren (in der Kalender-App)
    - Es kennt ihren Aufenthaltsort (per GPS)

- Es ist auch interessant sie zu beobachten wenn Sie mit ihrem Smartphone zum Beispiel
    - Online Banking durchführen
    - Online Einkaufen

- Ihr Smartphone enthält Fotos und Nachrichten die Sie vielleicht nicht mit der Allgemeinheit teilen möchten.

- Ihr Smartphone ist üblicherweise permanent mit dem Internet verbunden.
- Ihr Smartphone kann verloren gehen.

Angriffe aus der Distanz I

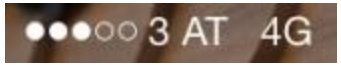
Ihr Smartphone kommuniziert per **2G/3G/4G**, WLAN (& Bluetooth)
Ihr Smartphone kann über all diese Wege angegriffen werden.

2G/3G/4G

- üblicherweise schirmt ihr Provider ihr Smartphone vor Verkehr der aus dem Internet unaufgefordert gesendet wird ab. Das gilt auch im Ausland.

- ist (unterschiedlich stark) gesichert & verschlüsselt

- identifiziert anhand der SIM Karte im Handy



Angriffe aus der Distanz II

Ihr Smartphone kommuniziert per 2G/3G/4G, **WLAN** (& Bluetooth)
Ihr Smartphone kann über all diese Wege angegriffen werden.

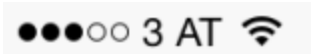
WLAN

Sie entscheiden ob und in welches WLAN ihr Handy sich einbucht
→ das passiert je nach Einstellung auch automatisch

WLANs sind nicht zwingend sicher und verschlüsselt

Sie wissen oft nicht wer das WLAN betreibt

Smartphones bevorzugen im allgemeinen WLAN für die Kommunikation



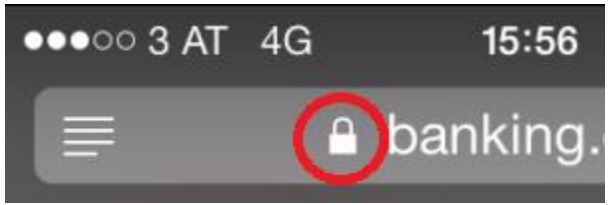
Angriffe aus der Distanz erschweren I

Smartphone & Apps

- Halten Sie ihre Software am Smartphone auf aktuellem Stand
- Installieren sie keine Betriebsystemupdates die nicht vom Hersteller (*oder ihrem Provider*) kommen.
- Seien Sie sich bewusst wenn sie auf ein altes Betriebssystem setzen das etwaige Lücken offen bleiben
- Installieren sie auch bei Apps regelmäßig Updates
- Bedenken Sie die Warnungen ihres Endgeräts bei neuen Apps (zb. Android) und verwenden Sie nur die App Stores der Hersteller.

Angriffe aus der Distanz erschweren II

- Verwenden Sie verschlüsselte WLANs („WPA2“) denen sie vertrauen.
- Verwenden Sie keine offenen WLANs bei sensiblen Anwendungen
- Im Zweifel deaktivieren Sie WLAN und verwenden sie ihre mobile Datenverbindung
- Achten sie im Browser darauf bei sensiblen Seiten ob die Kommunikation noch zusätzlich verschlüsselt wird



- Ein gesundes Maß an Skepsis ist auch beim Smartphone angesagt

Angriffe aus der Nähe

Ein gestohlenes/gefundenes Smartphone verrät potentiell sehr viel über den Besitzer.

Smartphones stellen ein bevorzugtes Ziel für Diebe dar, den sie sind

- klein
- für Taschendiebe leicht zu stehlen
- Benutzer haben keine Scheu ihr teures Endgerät öffentlich zu zeigen

- Abgesehen vom Wert des Smartphones kann man auch aus den Daten am Smartphone Kapital schlagen
    - Photos
    - Urlaubszeiten + Wohnort
    - Emails
    - …

Angriffe aus der Nähe erschweren

Sie werden ihr Handy verlieren oder es wird ihnen gestohlen.

Aktuelle Smartphones können gegen Benutzung anderer gesichert werden
→ Sperrcode einrichten / Fingerabdruck verwenden
(das ist nicht der SIM PIN Code)

Aktivieren Sie Mechanismen zum Orten des Handys
(z.b. *Find my iPhone*). Das erlaubt ihnen je nach
Lösung auch Nachrichten an ihr Handset zu senden &
verhindert eine Inbetriebnahme des Handys nach zurücksetzen.

(Erstellen Sie regelmäßige Backups ihres Handys – zuhause oder in der Cloud!)

Benutzen Sie die Sicherheitsfunktionen ihres Handys.
Installieren Sie Sicherheitsupdates.
Machen Sie regelmäßige Backups.

Setzen Sie ihren Hausverstand ein.

Danke.

Es geht auch anders.