Problematik

Die Sicherheitsanforderungen an mobile Geräte haben sich verändert. Mit ihrer zunehmenden Verbreitung muss auch verstärkt auf die Sicherheit der Daten, die auf solchen Geräten gespeichert sind, geachtet werden. Hinzu kommt, dass darauf inzwischen nicht nur private Daten, sondern auch immer mehr geschäftliche Informationen abgelegt werden. Damit sind Smartphones und Tablets denselben Risiken ausgesetzt wie stationäre und tragbare PCs.

Gerade weil man mit Smartphones und Tablets kinderleicht im Internet surfen kann, bieten sie Angriffspunkte für Schadsoftware oder Phishing. Die Angriffsmöglichkeiten unterscheiden sich bei Smartphones und Tablet-PC und auch je nach verwendetem Betriebssystem. Die Arbeitsweisen der Täter verändern sich ebenso rasant wie die technische Entwicklung dieser Geräte.

Smartphone Tablet-PC

Smartphone und Tablet-PC

Tipps

- Lassen Sie Ihr Smartphone oder Tablet nie unbeaufsichtigt liegen. Geben Sie es auch kurzzeitig nur in Ihrem Beisein an Dritte weiter.
- Nutzen Sie den Gerätesperrcode, die automatische Displaysperre und aktivieren Sie stets die SIM/USIM-PIN. Passwörter sollten getrennt vom Gerät aufbewahrt werden. Achten Sie bei der PIN-Eingabe darauf, dass niemand Ihr Passwort ausspähen kann.
- Löschen Sie alle sensiblen Daten, wenn Sie das Gerät verkaufen. Stellen Sie das Gerät dafür auf Werkeinstellungen zurück.
- Laden Sie keine Dateien aus unsicheren Quellen herunter. Nutzen Sie nur App-Stores seriöser Anbieter.
- Aktivieren Sie drahtlose Schnittstellen nur bei Bedarf. Eine direkte Koppelung mit anderen Geräten zum Austausch von Daten, etwa über Bluetooth oder NFC, darf nur mit vertrauenswürdigen Partnern geschehen.
- Nutzen Sie fremde WLANs, z.B. öffentliche Hotspots an Flughäfen oder in Cafés, nur mit einem VPN (Virtuelles privates Netzwerk), dieses macht Ihre Internetverbindung abhör- und manipulationssicher.
- Nutzen Sie bei Verlust oder Diebstahl mögliche Ortungs-, Fernsperr- oder Löschdienste.
- Drittanbietersperren, die Sie beim Provider einrichten, können Missbrauch durch Abofallen (z.B. teure SMS/MMS-Dienste) über die Telefonrechnung verhindern.
- Nutzen Sie, wenn verfügbar, Antivirenprogramme und Überwachungs-Apps, die Ihnen die Berechtigungen von anderen Apps (z.B. Zugriff auf das Telefonbuch) anzeigen.
- Verwenden Sie Online-Banking-Apps nicht auf dem gleichen Gerät, auf dem Sie auch die mobilen TAN empfangen.
- Hinterfragen Sie Provider-Updates, die Sie per SMS, MMS oder als Link erhalten – es kann sich um Schadsoftware handeln.

Linkempfehlungen

www.polizei-beratung.de/gefahren-im-internet
www.bsi-fuer-buerger.de
www.mjv.rlp.de/smartphones
www.klicksafe.de

OSCAR CHARLIE

(00V)150.2013.03

Wir wollen, dass Sie sicher leben.
Ihre Polizei

www.polizei-beratung.de

THEMA **Smartphone und Tablet-PC**

Klicks-Momente

Wir wollen, dass Sie sicher leben.
Ihre Polizei

Kompetent. Kostenlos. Neutral.