WIESO SOLLTE ICH MEIN SMARTPHONE SCHÜTZEN?

Quelle: Handysektor

Das Thema Sicherheit in Hinblick auf die Nutzung eines Smartphones hat viele Facetten. Da gibt es zum einen die verschiedenen **Sicherheitseinstellungen**, die am Gerät selbst vorgenommen werden können. Zum anderen kann das Smartphone auch mittels **Programmen**, Apps, geschützt werden, die aus dem jeweiligen App-Store geladen werden können.

Das Thema Sicherheit in Hinblick auf die Nutzung eines Smartphones hat viele Facetten. Da gibt es zum einen die verschiedenen **Sicherheitseinstellungen**, die am Gerät selbst vorgenommen werden können. Zum anderen kann das Smartphone auch mittels **Programmen**, Apps, geschützt werden, die aus dem jeweiligen App-Store geladen werden können.

In den Einstellungen von Android-Geräten kann man den PIN unter „Einstellungen → Sicherheit" einrichten. Die Bildschirmsperre kann unter „Einstellungen → Bildschirmsperre" aktiviert werden.

Besteht die Möglichkeit eine **Zahlenkombination** zu wählen, sollte man unbedingt auf gängige Zahlenkombinationen wie z. B. „1234“, „1111“ oder dergleichen verzichtet werden. Zu einfach wäre es Unbefugten, die Kombination zu knacken. Bei einer *Mustersperre* kann man sich ein eigenes Muster aus verschiedenen vorgegebenen Punkten zusammensetzen, z. B. ein Rechteck, Quadrat oder einen Buchstaben. Aber Vorsicht! Auf dem Touch-Display entstehen im Lauf der Zeit sichtbare **Spuren durch Fingerabdrücke**. Deshalb sollte das Display regelmäßig gesäubert werden, wenn eine Mustersperre verwendet wird. Generell ist von dieser Art der Sperrung eher abzuraten. Wird das Smartphone mit einem Passwort geschützt, sollte dieses Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Je länger es ist, desto sicherer ist es oft.

Neuere Smartphones bieten auch die Option des sog. **„FaceUnlock“** – des Entsperren mittels Gesichtserkennung. Diese Option bietet jedoch wenig Sicherheit, da sie einfach mittels eines Bildes des Besitzers ausgetrickst werden kann.

Wird das Smartphone gestohlen, sollte man die **SIM-Karte** (SIM = engl. subscriber identity module) des Geräts bei dem Netzbetreiber unter Angabe der Telefonnummer sperren lassen. Die SIM-Karte dient zur Identifikation des Nutzers, über die auch die Telefonkosten abgerechnet werden. Ist diese Karte gesperrt, kann kein Fremder mehr damit telefonieren und hohe Kosten verursachen. Im Anschluss daran sollte Anzeige bei der Polizei erstattet werden. Hier ist auch die **„Seriennummer“**(IMEI-Nummer) des Smartphones anzugeben. Die Nummer findet sich unter dem Akku (so nicht verklebt), auf der Originalverpackung oder der Rechnung zum Handykauf. Schreiben Sie diese auf jeden Fall auf, so dass Sie im Falle eines Handyverlusts schnell griffbereit ist. Die Betriebssysteme Android, iOS und Windows Phone bieten außerdem verschiedene Dienste zum Wiederfinden oder Sperren des Smartphones bei Verlust, z. B. den „Android Geräte-Manager“ von Google oder die „iCloud“ von Apple. Informieren Sie sich dazu beim Handykauf im Shop Ihres Anbieters oder auf den Websites vom Handy-Hersteller oder Anbieter der Betriebssysteme.

Smartphones sind Computer und deshalb auch anfällig für Viren und Malware. Es ist daher ratsam, einen Virenscanner in Form einer App zu installieren.

Oft werden persönliche Daten (Kontakte, aktueller Standort,...) ganz unbemerkt und ungewollt gesammelt und übermittelt. Neben dem Betriebssystem selbst sind dafür auch Anwendungen verantwortlich. Daher ist es ratsam, **Anwendungen, die gerade nicht gebraucht werden und aktiv sind, abzuschalten**. Auch Bluetooth ist eine Schnittstelle nach „draußen". Über

Bluetoothkönnen z.B. Dateien von Handy zu Handy über einige Meter Entfernung getauscht werden, ohne die Geräte über ein Kabel zu verbinden. Auch spezielle Bluetooth-Kopfhörer können kabellos Musik oder Telefonate übertragen. Ist **Bluetooth** eingeschaltet, steigt die Gefahr, dass andere ungewollt persönliche Daten vom Gerät abrufen. Deshalb sollte man Bluetooth nur einschalten, wenn es tatsächlich benötigt wird. Das gilt auch für die WLAN-Funktion. Hier sollte auch die automatische Einwahl in öffentliche WLAN-Netze deaktiviert sein.