Datenschutz bei Windows, Android und iOS: Mit diesen Tipps sperren Sie Schnüffler aus Ihrem Handy aus

Aktualisiert am 22. Februar 2017

Lena Meyer-Landrut wird erpresst, weil intime Fotos von ihr in die falschen Hände gelangt sind. Mit einem felsenfesten Datenschutz wären ihre Bilder wohl sicher gewesen. Mit unseren Tipps sperren Sie Schnüffler aus Ihrem Handy aus - egal ob bei Windows, iPhone oder Android.

Das eispiel von ESC-Gewinnerin Lena zeigt: Pikante Bilder oder intime Videos bleiben nicht immer so privat, wie man es gerne hätte. Daher sollten Sie Ihre Daten auf Computer oder Smartphone unbedingt vor Fremden schützen. Auch wenn Sie kein Prominenter sind, können die Folgen für Sie dramatisch sein, wenn Betrüger an Ihre Daten kommen.

Windows vor Daten-Schnüfflern abschirmen

Im Fall von Meyer-Landrut war es ein gestohlenes Notebook, das sie in die unglückliche Situation gebracht hat. Auf diesem waren ihre Nacktfotos offenbar nicht vor fremden Blicken geschützt. Ihnen wäre es sicherlich genauso ergangen, denn: Selbst wenn Sie Windows so konfiguriert haben, dass Sie beim Start ein Passwort eingeben müssen, sind Ihre Daten nicht geschützt.

Angreifer können das Passwort relativ einfach umgehen und Bilder, Musik oder Videos von Ihnen anschauen - selbst die pikanten, die nicht jeder sehen sollte. In diesem Fall hilft nur eine Verschlüsselung der Daten, damit niemand Ihre Dokumente durchstöbern kann.

Ohne das richtige Passwort zum Entschlüsseln beißen sich Schnüffler die Zähne an einem solchen Schutz aus.

Eine kostenlose Software für diesen Zweck ist das weit verbreitete VeraCrypt, das gleich drei verschiedene Verschlüsselungs-Algorithmen beherrscht. Was sehr kompliziert klingt, ist mit der richtigen Anleitung für jeden machbar.

Auf YouTube finden Sie Tutorials, mit denen Sie entweder das komplette Windows-System verschlüsseln oder - was gerade für ältere und langsamere Computer praktikabel ist - einzelne Ordner und Verzeichnisse schützen.

Smartphone: Datenschutz für iOS und Android

Das Smartphone ist in der Regel der ständige Begleiter, mit dem viele ihr gesamtes Leben organisieren und mittels eingebauter Kamera auch dokumentieren. Hier kann auch mal das ein oder andere intime Foto in der Bildergalerie landen. Daher ist der Datenschutz auf iPhone & Co. sehr wichtig.

Wer ein iPhone hat, kann sich zumindest ein wenig zurücklehnen. Denn Apple verschlüsselt die Daten auf dem Smartphone von Haus aus. Aber nur unter einer Bedingung: Wenn Sie Ihr iPhone mit einem Zugangscode geschützt haben. Sollten Sie das nicht haben, sollten Sie das dringend ändern.

Gehen Sie dazu in die Einstellungen-App, navigieren Sie zu "Touch ID & Code" und geben Sie Ihr Passwort unter "Code ändern" ein. Hinweis: Ihre Bilder, die Sie in der iCloud speichern, sind dort nicht verschlüsselt. Sie sollten daher das iCloud-Backup deaktivieren, wenn Sie sensible Bilder auf Ihrem Gerät haben.

Auch bei Android gibt es die Möglichkeit, Daten zu chiffrieren. Das geht in den "Einstellungen" unter dem Punkt "Sicherheit". Dort finden Sie die Option "Telefon verschlüsseln". Leider ist die Funktion nicht unter allen Android-Versionen verfügbar und im schlimmsten Fall wird Ihr Smartphone dadurch langsamer.

Probieren Sie es einfach aus, Sie können die Verschlüsselung schnell rückgängig machen, falls es Probleme macht.

Sensible Daten nicht per Mail verschicken

Dass man Informationen, die niemanden etwas angehen, nicht gerade per E-Mail verschicken sollte, weiß so ziemlich jeder. Denn wenn Sie nicht gerade "E-Mail made in Germany" nutzen, liest im schlimmsten Fall nicht nur die NSA mit.

Landet Ihre E-Mail versehentlich - beispielsweise durch einen Tippfehler - gar nicht bei dem gewünschten Empfänger, sondern bei einem Fremden, kann das durchaus ein Problem sein.

Doch wie kommen sensible Daten am sichersten von A nach B? Klar kann man sie auf einen USB-Stick ziehen und dem Adressaten persönlich vorbeibringen. Aber so ein Stick hat auch einen Nachteil: Man kann ihn schnell verlieren, verlegen oder er kommt in fremde Hände, weil ihn vielleicht auch noch jemand anderes nutzt, beispielsweise der WG-Mitbewohner oder der Arbeitskollege.

Die Lösung: Es gibt USB-Sticks mit einem Verschlüsselungssystem. Der Stick erlaubt erst dann Zugriff auf die Daten, wenn man ein Passwort eingegeben hat. Der Haken: Diese Sticks sind etwas teurer als herkömmliche Varianten.

Wer aber öfter mit sensiblen Daten hantiert, sollte sich durchaus über solch eine Anschaffung Gedanken machen. Wie man am Fall von Lena Meyer-Landrut sieht, kann ein Daten-Klau nämlich im schlimmsten Fall nicht nur teuer, sondern auch peinlich oder zumindest sehr ärgerlich sein.

Das Dilemma mit dem Passwort

Wenn es um Passwörter geht, mag der ein oder andere die Augen verdrehen, wenn Sicherheitsexperten den Tipp geben: Für jeden Web-Dienst, für jede Internet-Seite ein eigenes, kompliziertes Passwort. Die Anforderungen sind zudem hoch: Groß- und Kleinschreibung sollte darin ebenso vorkommen wie eine Zahl und ein Sonderzeichen.

Wer soll sich aber so viele Zugangsdaten merken? Das geht tatsächlich: Mit einem Trick und einem cleveren System! Sie überlegen sich nicht ein Passwort, sondern starten mit einer sogenannten Passphrase. Beispiel: "Meine Oma wohnt in Berlin und hat 9 Katzen!". So einen Satz können Sie sich locker merken.

Nun nehmen Sie von jedem Wort des Satzes jeweils den ersten Buchstaben, also: "MOwiBuh9K!". Schon haben Sie eine gute Basis für Ihr neues Passwort-System. Was kompliziert aussieht ist dennoch einprägsam.

Wenn Sie hier nun noch ein Kürzel für den jeweiligen Online-Dienst dran hängen - also beispielsweise die ersten oder die letzten beiden Buchstaben - wird das Passwort schwer zu knacken, individuell aber dennoch leicht zu merken. Probieren Sie es aus!