

Tipps gegen Datenklau

Auszug MM Geld&Markt 11.09.26

„Angesichts der Wellen von Hackerangriffen verschärft die EU Meldepflichten, Hersteller müssen ab sofort binnen 24 Std Angriffe auf Hard- und Softwareprodukte melden. Doch meist greifen Kriminelle die Verbraucher direkt an“

Prävention

Datenschutz:

Bereits mit einer eMail-Adresse oder einer Handynummer lässt sich viel Unheil anrichten. Am besten verteilt man so wenig Daten im Internet wie möglich. Auch lohnt es sich den Zugriff von Apps zu beschränken, denn nicht nur Werbekunden können gesammelte Daten für kleines Geld kaufen. Deshalb:

Sichere Passwörter:

Gerade durch KI ist es sehr einfach, simple Passwörter zu erraten. Besonders Passwörter, die einen Familienbezug enthalten, sind schnell zu „entziffern“. Deshalb ist zu empfehlen, zufällige Passwörter mit verschiedenen Zeichenklassen – Buchstaben, Ziffern, Sonderzeichen – zu verwenden. Denn jede Variable senkt die Wahrscheinlichkeit, das Passwort zu erraten. So liegen die Dechiffrierungschancen bei nur einem Buchstaben und einer Ziffer bei 260 Möglichkeiten, bei 2 Ziffern erhöht sich dieser Wert auf 2600 Möglichkeiten. So empfiehlt das Bundesamt für Sicherheit in der Informationstechnik Passwörter mit **mindestens 8 Stellen** zu verwenden. Wer es ernst meint, kann aber auch z.B. 30 Stellen und mehr verwenden. Je höherwertig dieser Schlüssel ist, um so geringer ist die Dechiffrierungschance. Eine Entschlüsselung ist sehr schwierig, u.U. praktisch unmöglich. Die Verwaltung der Schlüssel stellt ein eigenes Kapitel dar.

Passwortmanager:

Wollen Sie eine schriftliche Dokumentation Ihrer Passwörter vermeiden, empfiehlt sich ein Passwortmanager. Diese Programme erzeugen lange, sichere Passwörter und speichern sie. Bei Anmeldung auf einer Web-Site wird eine Maske dann automatisch ausgefüllt. Eine weitere Möglichkeit besteht in der Nutzung von Passkeys.

Passkey:

Passkeys sind kryptographische Schlüssel – also Dateien -die auf dem Gerät oder einer App hinterlegt sind. Praktisch rufen Smartphones den Passkey selbstständig ab. Oft müssen zur Freigabe Fingerprints eingesetzt werden.

ZweiFaktor-Prüfung.

Wo möglich, ist zum besseren Einsatz die 2Faktor- Prüfung angeraten. Hier wird neben dem Passwort über ein zweites nicht eingebundenes Gerät ein Code - den man über eine SMS erhält – versandt. Erst bei Bestätigung dieses Einmal-Codes erhalten Sie Zugang zu der „verriegelten“ Seite.

Notfall:

Es gibt kostenlose Prüfdienste wie in diesem Menü unter dem Punkt „**Identitätsbetrug und Passwortüberprüfung Pkt. 14**“ beschrieben. Damit können Sie prüfen, ob eigene Dateien von bekannten Lecks betroffen sind. Sofern das der Fall ist, bitte **umgehend** Ihr Passwort ändern. Es empfiehlt sich dann eine Konto- und Kreditkartenbewegung im Auge zu behalten.