Spiel und Sport Rhede e.V.

susrhede@outlook.de

So schützen Sie sich vor Datendiebstahl

Komplizierte Passwörter, regelmäßige Updates: Experten geben Tipps für mehr Sicherheit im Netz und warnen vor Nachlässigkeiten.

Adressen, Telefonnummern, Kontoverbindungen, persönliche Nachrichten und Bilder – solch sensible Daten sind bei der aktuellen Hackerattacke auf Online-Konten von Politikern und Prominenten entwendet worden. Wie Sie sich am zuverlässigsten vor Datenklau durch Hacker schützen können, verraten Ihnen unsere Tipps:

Seien Sie sparsam mit Daten:

Wer allzu freizügig mit seinen Daten umgeht, muss nicht nur damit rechnen, dass sie im Netz an unerwünschter Stelle auftauchen. Ihm droht auch Identitätsdiebstahl. Um einer anderen Person die Identität zu stehlen und zu missbrauchen, etwa beim Onlineshopping, bedarf es oft nur weniger Informationen, warnt das Portal „iRights.info“. Allein Geburtsdatum, Name und Adresse einer Person öffneten Missbrauch häufig Tür und Tor. Deshalb sollte man nach dem Prinzip der Datensparsamkeit verfahren.

Für jedes Online-Konto ein anderes Passwort:

Sichere Passwörter sind ein guter Schutz vor Identitätsdiebstahl im Internet. Deswegen braucht jedes einzelne Online-Konto für Banking, Einkaufen oder Unterhaltung ein eigenes Passwort, erklärt Prof. Christoph Meinel, Direktor des Hasso-Plattner-Instituts an der Universität Potsdam.

So erstellen Sie ein sicheres Passwort:

Damit ein Passwort sicher ist, müssen einige Bedingungen erfüllt sein: 10 bis 15 Zeichen sollte es haben, darunter Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen, zum Beispiel „H$eEE5?-&e3“. Tabu sind leicht erratbare Informationen wie Namen, Geburtsdaten, Haustier- oder Partnernamen oder der Name des Dienstes oder Programms, für den das Passwort gewählt wird. Wörter aus dem Wörterbuch oder andere gewöhnliche Zeichenfolgen sollten nicht genutzt werden. Auch gelegentliches Ändern der Passwörter kann helfen, sagt Meinel.

Nutzen Sie die Zwei-Faktor-Authentifizierung:

Viele Onlinedienste bieten die doppelte Authentifizierung, die Hackern die Übernahme eines Accounts maßgeblich erschwert. Ein Beispiel: die SMS-Tan beim Internet-Banking. Um eine Transaktion zu bestätigen, wird ein Zahlencode auf das Handy geschickt. Erst nach dessen Eingabe wird die Zahlung ausgelöst. „Ähnliche Funktionen gibt es unter anderem bei Google, PayPal, Dropbox und Facebook“, sagt Sebastian Barchnicki vom Institut für Internet-Sicherheit if(is) der Westfälischen Hochschule in Gelsenkirchen. Neben erhöhtem Schutz hat dieser Mechanismus eine Warnfunktion: „Bekommen Nutzer einen Authentifizierungscode, obwohl sie selbst gerade keinen Log-in-Prozess auf dem betreffenden Konto durchführen“, erläutert Barchnicki, „sollte ihnen umgehend klar werden, dass hier jemand versucht, sich unbefugten Zugriff zu verschaffen“.

Vorsicht bei Cloud-Speichern:

Sogenannte Cloud-Dienste sind praktisch, bergen aber ein Datendiebstahl-Risiko. Vor allem sensible Daten sollten Nutzer deshalb nicht unverschlüsselt in einem Onlinespeicher ablegen, rät das Bundesamt für Sicherheit in der Informationstechnik (BSI).

So sichern Sie Ihren W-Lan-Router ab:

Die meisten W-Lan-Router haben einen Standard-Netzwerkschlüssel. Dieser reicht aber oft nicht aus. „Wechseln Sie den Schlüssel regelmäßig, am besten alle drei Monate“, empfiehlt Viktor Schröder, Leiter IT-Services von der Gesellschaft für Informatik.

Schützen Sie Ihren Browser:

Der Browser zählt zu den größten Schwachstellen eines Rechners. Erweiterungen für den Browser wie „Noscript“ verhindern das Ausführen von schadhaften Skripten.

Kleben Sie Ihre Webcam ab:

Die Webcam oder Selfie-Kamera des Smartphones als Spion? Unbegründet ist diese Sorge nicht, wie Nabil Alsabah vom Bitkom erklärt. Werden Hightech-Geräte mit schädlicher Software infiziert, könne die Kamera auch ohne Wissen der Nutzer aktiviert werden.

Updates, Updates, Updates:

Aktualisierungen für das Betriebssystem sowie für alle Programme sollten Anwender immer so schnell wie möglich installieren. Sonst können Angreifer Sicherheitslücken ausnutzen, um Daten abzugreifen.

So prüfen Sie, ob Ihr Online-Konto gehackt wurde:

Mit Angeboten wie dem Identity Leak Checker des HPI kann man verfolgen, ob persönliche Daten wie E-Mail-Adressen oder Passwörter von Kriminellen erbeutet und zum Verkauf angeboten werden. Allerdings können so nur bereits bekannte Lecks geprüft werden.

Quelle: NOZ vom 05.01.2019 (Mit dpa)