Verbraucherdaten im Visier von Kriminellen - Tipps für Internet-Nutzer

Surfen im Netz wird für Verbraucher immer gefährlicher. Kaum eine Woche vergeht, ohne dass eine kritische Sicherheitslücke in einem Internetprogramm oder ein groß angelegter Angriff auf Kundendatenbanken von Unternehmen bekannt wird. Datenlecks bei großen Firmen machen es Unbefugten leicht, sich Zugang zu unzähligen privaten Daten zu verschaffen. Auch Phishing-Mails mit falschen Absendern dienen dazu, Kundendaten abzugreifen.
Aktuell sind massenweise Trojaner-Mails unterwegs, die vermeintlich von der Gutscheinplattform Groupon stammen. Die Verbraucherzentrale gibt Tipps, wie man sich schützen kann.
Die Datendiebe haben es vor allem auf private Adressen, Informationen über Bankkonten wie Kontonummern, Kreditkarten-Transaktionsnummern (TANs) und Login-Daten abgesehen. Geschickt nutzen sie Sicherheitslücken auf privaten Computern, Smartphones und Tablets aus. Die Angriffe verlaufen im Hintergrund, von den Betroffenen oft völlig unbemerkt. Mit den abgegriffenen Informationen nehmen Kriminelle rechtswidrige Kontobelastungen unter fremder Identität vor. Durch Trojaner-Software können die Eindringlinge außerdem den Computer kapern und für illegales Handeln fernsteuern. „Grundsätzlich kann jeder Opfer eines Cyber-Angriffs werden“, warnt Martina Totz von der Verbraucherzentrale Rheinland-Pfalz. „Das Internet ist vergleichbar mit dem Wilden Westen. Betroffene sind beim Schutz vor digitalen Räubern größtenteils auf sich alleine gestellt“, so die Verbraucherschützerin. Wer den eigenen Rechner, das Smartphone oder Tablet vor Angriffen schützen will, kann die Gefahren für die eigenen Daten mit folgenden Maßnahmen verringern:

- Überprüfen Sie Kontoauszüge und Kreditkartenabrechnungen regelmäßig
- Nutzen Sie eine Sicherheitssoftware bzw. ein Antivirenschutzprogramm mit regelmäßigen Updates.
- Beziehen Sie Programme und Apps nur aus sicheren Quellen.
- Nutzen Sie lange und komplizierte Passwörter und geben Sie diese nicht weiter.
- Verwenden Sie unterschiedliche Dienste nicht mit dem gleichen Benutzernamen und Passwort.
- Lassen Sie keine Fernwartung durch angebliche Servicemitarbeiter von scheinbaren Computerfirmen zu.
- Reagieren Sie nicht auf Phishing-Mails, die um Bestätigung von Login-Daten oder Transaktionsnummern bitten
  und klicken Sie nicht auf den beigefügten Link in solchen Mails.
- Hinterlegen Sie bei Sicherheitsfragen keine einfachen Antworten.
- Öffnen Sie Datei-Anhänge, insbesondere in ungewöhnlichen Formaten wie ZIP oder PIF, von bekannten
  Unternehmen trotz persönlicher Ansprache nicht und überprüfen Sie diese mit einem aktuellen Schutzprogramm
- Richten Sie eine Firewall für ein- und ausgehende Datenverbindungen ein
- Deaktivieren Sie grundsätzlich die Bluetooth-Funktion.

Sensible Daten werden nicht nur auf dem eigenen Rechner oder auf mobilen Geräten verwendet und gespeichert. Viele Unternehmen speichern Informationen zum Beispiel in einer Kundendatenbank oder einem Online-Speicher, den sogenannten Cloud-Diensten. Verbraucherinnen und Verbraucher haben darüber keine Kontrolle und können nur darauf vertrauen, dass die Unternehmen persönliche Daten hinreichend schützen und dass sie über Datenlecks frühzeitig und vollständig informieren.
Wer bemerkt, dass sich Fremde Zugang zu einem Konto in einem Internet-Dienst, zum Beispiel einem E-Mail-Postfach oder zum Online-Banking, verschafft haben, sollte schnellstmöglich seine Passwörter ändern, seine Bank informieren und den Vorfall umgehend dem Diensteanbieter und der Polizei melden.
„Wir müssen davon ausgehen, dass die Internetkriminellen in Zukunft noch versierter vorgehen werden. Der technische Schutz wichtiger Daten ist zwar lästig, aber mittlerweile eine unumgängliche Daueraufgabe“, mahnt Verbraucherschützerin Totz von der Verbraucher-Zentrale-Rheinland-Pfalz.