Letzte Prüfung auf Aktualität: 31.03.2025 Summer Daniela

Account Sicherheit: Was tun im Schadensfall?

Beschreibung

Prävention ist der beste Schutz vor einem Schadensfall und unangenehme Konsequenzen Sollten Sie dennoch Opfer eines Angriffs werden, ist schnelles Handeln entscheidend, um Schäden zu minimieren. Ändern Sie so schnell wie möglich die Passwörter, auch bei anderen von Ihnen genutzten Benutzerkonten. Bleiben Sie wachsam! Sicherheit beginnt bei der eigenen Vorsicht und Wachsamkeit.

Bedeutung von Account-Sicherheit

- Digitale Benutzerkonten enthalten sensible persönliche und finanzielle Daten
- Ein ungesicherter Account kann zu Identitätsdiebstahl, finanziellen Verlusten und Datenmissbrauch führen
- Proaktiver Schutz ist essenziell, um Schäden zu minimieren

Häufige Gefahrenquellen

- Phishing-Angriffe: Betrügerische E-Mails oder Webseiten, die sensible Daten stehlen
- Schwache Passwörter: Leicht zu erratende oder wiederverwendete Passwörter
- Datenlecks: unzureichend geschützte Datenbanken bei Drittanbieter
- Malware: Schadsoftware, die Zugangsdaten ausliest
- Social Engineering: persönliche und manipulative Beeinflussung der Opfer (oftmals durch telefonische Anrufe), um eine freiwillige Preisgabe von persönlichen oder unternehmerischer Daten herbeizuführen.

Maßnahmen zur Vorbeugung

- Starke Passwörter verwenden: Mindestens 12 Zeichen, bestehend aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
- Zwei-Faktor-Authentifizierung: Ergänzung des Passworts durch einen zweiten Authentifizierungsfaktor
- Datenleck überprüfen: auf Seiten wie Have I Been Pwned: Check if your email has been compromised in a data breach regelmäßig überprüfen, ob Account-Zugänge geleakt wurden
- Regelmäßige Updates: Software und Geräte immer aktuell halten. Sicherheitslücken werden durch Updates geschlossen
- Phishing-Schutz: E-Mails und Links vor dem Klicken immer prüfen, keine sensiblen Daten unaufgefordert angeben
- Liste erstellen: im Vorfeld eine Liste erstellen, wo E-Mail-Adressen hinterlegt wurden

  - Stellen Sie eine Liste mit den Benutzerkonten zusammen, über die Sie bereits verfügen
  - Welche Daten wurden bei welchem Benutzerkonto hinterlegt?
  - Erstellen Sie eine Liste von E-Mail-Adressen von Personen aus Ihrem Umfeld

Sofortmaßnahmen bei einem Schadensfall

- Zugang sperren: Sofort das Passwort ändern. Falls kein Zugriff mehr möglich ist, den Anbieter kontaktieren
- Überprüfung der Aktivitäten: Unbekannte Anmeldungen oder Transaktionen prüfen und melden
- Betroffene Plattformen informieren: Verdächtige Aktivitäten dem Support melden und Anweisungen befolgen
- Zwei-Faktor-Authentifizierung (2FA) aktivieren: Falls noch nicht geschehen, 2FA einrichten, um weiteren Missbrauch zu verhindern
- Finanzielle Kontrolle: Entdecken Sie ungerechtfertigte Abbuchungen vom Konto oder Belastungen der Kreditkarte
- Rechtliche Schritte prüfen: Erstatten Sie Anzeige bei einer Polizeidienststelle, insbesondere bei Identitätsdiebstahl! Bringen Sie das Gerät, auf dem Sie die strafbare Handlung wahrgenommen haben nach Möglichkeit zur Anzeigeerstattung (zB Handy, Laptop) mit.

Wichtige Ansprechpartner im Schadensfall

- Kundensupport des betroffenen Dienstes: Erste Anlaufstelle für Zugangssperrung und Wiederherstellung
- Banken/Kreditkartenunternehmen: bei finanziellen Schäden
- Polizeidienststelle: Für rechtliche Schritte und Meldungen
- Datenschutzbehörde: bei Verletzungen der Datenschutzrichtlinien

Präventionsempfehlungen der Polizei

- **Starke Passwörter verwenden** – Verwenden Sie einzigartige Passwörter – vermeiden Sie Passwortwiederholungen und erstellen Sie für jedes Benutzerkonto individuelle Passwörter.
- **Zwei-Faktor-Authentifizierung**: Aktivieren Sie Zwei-Faktor-Authentifizierungen für einen zusätzlichen Schutz vor unbefugten Zugriffen.
- **Verwenden Sie Passkeys oder einen Passwort-Manager:** Dadurch werden Ihre Passwörter sicher gespeichert bzw. generieren Sie automatisch starke Passwörter
- **Vermeidung von Phishing und social engineering:** Überprüfen Sie die Absenderadresse von E-Mails sorgfältig. Keine Links in verdächtigen E-Mails anklicken oder Anhänge öffnen. Geben

Sie sensible Daten nur auf vertrauenswürdigen Websites ein (Achten Sie auf „https://“ in der URL)

- **Überwachung von Datenlecks:** Nutzen Sie Dienste wie Have I Been Pwned: Check if your email has been compromised in a data breach, um zu überprüfen, ob Ihre E-Mail-Adresse oder Passwörter in Datenlecks veröffentlicht wurden. Ändern Sie Passwörter sofort, falls ein Datenleck bekannt wird.
- **Reaktionsvorbereitung:** Entwickeln Sie Sicherheitspläne, um im Falle eines Sicherheitsvorfalles schnell zu handeln

Weiterführende Links

- BSI - Passkeys - anmelden ohne Passwort
- Sichere_passwoerter_faktenblatt.pdf
- Have I Been Pwned: Check if your email has been compromised in a data breach
- Check your hack | politie.nl