Ratgeber: Passwörter sicher wählen und verwalten

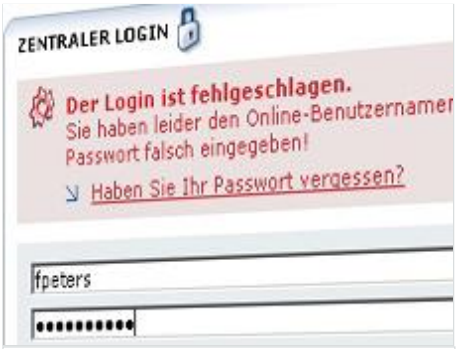
Viele Nutzer sind bedroht: So einfach lassen sich Passwörter umgehen

Nachdem Microsoft, Google, Yahoo und AOL vor kurzem eingestehen mussten, dass Tausende ihrer E-Mail-Konten geknackt wurden, ist die Verunsicherung bei vielen Internetnutzern groß. Was ist zu tun, wenn der E-Mail-Dienst den Zugriff auf Ihr Postfach verweigert oder bei Ebay jemand in Ihrem Namen Artikel ersteigert? Lesen Sie hier, wie es dazu kommen kann und wie Sie sich schützen.

Wo können Angreifer überall einbrechen?

Im schlimmsten Fall bei allen Internetdiensten, für die ein Nutzer Zugangsdaten braucht. Das E-Mail- Postfach des Opfers ist der Ausgangspunkt für den Angriff. Ist das Postfach geknackt und mit einem neuem Passwort gesichert, stehen alle anderen genutzten Internetdienste wie Ebay, Amazon und PayPal sperrangelweit offen: Die meisten Dienste verschicken auf Wunsch ein neues Kennwort an die E-Mail-Adresse. Welche Zugangskonten das Opfer hat, verrät in vielen Fällen schon das Postfach. Newsletter, Bestellbestätigungen und Foren-Nachrichten geben genügend Hinweise.

» Betrug: E-Mail-Konten mit Phishing-Attacke geknackt



Haben Sie das Passwort vergessen oder wurde etwa das Postfach gekapert?

Warum ist das Knacken von Konten so einfach?

Der Hauptgrund: E-Mail-Dienste wollen es ihren Kunden möglichst einfach machen. Hat ein Nutzer sein Kennwort vergessen, muss er nur eine Sicherheitsfrage beantworten. Die richten viele Nutzer bei der Anmeldung ein. Schließlich will niemand ein geschlossenes Postfach haben. Die große Gefahr dabei: Viele „geheime Fragen“ lassen sich auch von anderen Personen beantworten. Angreifer legen dann bei einigen Diensten im nächsten Schritt sofort ein neues Passwort fest. Viele Dienste bieten nur vorgegebene Fragen, etwa: „Wie heißt Ihr Haustier?“ oder „Wie ist der Mädchenname Ihrer Mutter?“ Die richtige Antwort wissen Sie auch noch nach Jahren, aber auch Freunde und Bekannte kennen womöglich die Antwort. Und selbst Wildfremde können leicht einbrechen, da mehrfache Anmeldeversuche meist kein Problem sind.

So lassen sich Passwörter umgehen

Wie können Fremde die Fragen beantworten?

- In vielen Fällen liefert eine normale Suchmaschine wie Google die nötigen Informationen.
- Angaben zum Lebenslauf gibt es bei Personen-Suchmaschinen wie 123people und Yasni.
- Antworten auf Fragen nach der Lieblingsband oder dem Haustier liefern Communitys wie StudiVZ oder Facebook. Dort geben viele Nutzer selbst Infos über ihr Leben und ihre Vorlieben preis. Führt das Internet bei einer Frage mal nicht zum Ziel, hilft in vielen Fällen der Griff zum Telefon: Ein Anruf bei Freunden oder der Familie, eine erfundene Geschichte und eine scheinheilige Frage.

Welche Internetdienste sind betroffen?

Ein Test von COMPUTER BILD (Stand: September 2009) ergab: Bei sechs von acht E-Mail-Anbietern hatten Angreifer Zugriff auf alle E-Mails und Einstellungen, wenn sie die vorgegebene „Geheimfrage“ richtig beantworteten. Die betroffenen Anbieter waren Google Mail, T-Online, Freenet, Microsoft Hotmail, Yahoo Mail und AOL. Besser machen es in dieser Disziplin web.de und GMX.

So schützen Sie sich vor Hacker-Angriffen

- **Legen Sie bei den Sicherheitsfragen Ihrer genutzten Internetdienste Antworten fest, die wirklich nur Sie wissen können. Alternative: Schalten Sie die Sicherheitsfrage ab.**
- **Ob E-Mail-Postfach, Internetshop, Bahn oder Reiseanbieter: Vergeben Sie für jeden Dienst ein eigenes Passwort.**
- **Nutzen Sie einen Passwort-Manager wie KeePass 2. Er generiert sichere Passwörter, verwaltet alle Ihre Zugangsdaten und erlaubt Ihnen, die Benutzernamen und Passwörter an den gewünschten Stellen (also etwa in der Eingabemaske auf einer Internetseite) zu übernehmen. Der Zugang ist nur mit einem Master-Kennwort oder einem Schlüssel möglich, den Sie auf einem USB-Stick speichern.**

KeePass 2: Installation und erste Schritte




» Ratgeber: Vier Regeln für mehr Kennwort-Sicherheit
» COMPUTER BILD stoppt die Internet-Abzocke!
» Ratgeber: E-Mails verschlüsseln
» Ratgeber: Spuren auf dem PC löschen

Finden Sie mehr zu folgenden Begriffen: Ratgeber, Tipps, Internet, Passwörter, Sicherheit, KeePass 2