Bitkom e.V. |

Jeder dritte Onliner nutzt dasselbe Passwort für mehrere Dienste

- **Bitkom gibt Tipps für sichere Passwörter**
- **Am 1. Februar ist der „Ändere-dein-Passwort-Tag“**

Berlin, 31. Januar 2020 - Wenn es um Passwörter geht, setzen viele Internetnutzer eher auf Bequemlichkeit als auf Sicherheit. Mehr als jeder dritte Onliner (36 Prozent) in Deutschland nutzt für mehrere Online-Dienste das gleiche Passwort. Das ist das Ergebnis einer repräsentativen Umfrage im Auftrag des Digitalverbands Bitkom unter mehr als 1.000 Internetnutzern in Deutschland. „Ein einziges Passwort für mehrere Online-Dienste ist ein großes Sicherheitsrisiko“, sagt Teresa Ritter, Bitkom-Expertin für IT-Sicherheit. „Wenn ein solches Universalpasswort einmal geknackt ist, können Cyberkriminelle gleich mehrere digitale Identitäten von Nutzern übernehmen.“

Die Mehrheit beschäftigt sich aber damit, sichere Passwörter zu verwenden. Fast zwei Drittel (63 Prozent) sagen: Ich achte bei der Erstellung neuer Passwörter auf einen Mix aus Buchstaben, Zahlen und Sonderzeichen. Drei von zehn Internetnutzern (31 Prozent) ändern ihre Passwörter in regelmäßigen Abständen. Und 8 Prozent sagen, dass sie einen Passwort-Generator beziehungsweise einen Passwort-Safe zur Erstellung und Verwaltung ihrer Passwörter nutzen. „Lange Wörter mit unterschiedlichen Zeichen – das ist eine einfache Faustregel für gute Passwörter“, so Ritter.

Einen perfekten Schutz vor Cyberkriminellen bieten auch die längsten Passwörter nicht. Doch wer folgende Hinweise beachtet, erschwert Cyberattacken deutlich:

Komplexe Passwörter nutzen

Je komplexer das Passwort, desto höher der Schutz. Trotzdem werden im Alltag oft simple Passwörter genutzt. Mit einem Trick lassen sich auch schwierige Passwörter leicht merken, indem clevere Eselsbrücken eingesetzt werden. Um Passwörter mit Buchstaben, Zahlen und Sonderzeichen zu generieren, werden dafür die Anfangsbuchstaben von ausgedachten Sätzen genommen, etwa: „Mein Verein gewann das entscheidende Spiel mit 3 zu 2!" Daraus lässt sich ein sicheres und gut zu merkendes Passwort erstellen: „MVgdeSm3z2!“.

Der Passwort-Manager als Kennwort-Tresor

Passwort-Manager speichern alle genutzten Kennwörter in einer verschlüsselten Datei. Nutzer müssen sich nur noch ein Passwort merken, das Master-Passwort. Dieses Passwort sollte höchste Standards erfüllen. Einmal eingegeben, erlangt man Zugang zu allen gespeicherten Kennwörtern. Einige Programme bieten sogar die Möglichkeit, nicht nur Passwörter, sondern auch die dazugehörigen Benutzernamen zu speichern. Auf Wunsch füllen die Programme die abgefragten Felder beim Login automatisch aus.

Doppelte Sicherheitsstufe

Einige Dienste bieten mittlerweile Mehr-Faktor-Authentifizierungen an. Das bedeutet, dass der Nutzer mehr als eine Sicherheitsabfrage beantworten muss, um auf einen Account zuzugreifen. Dazu erhält man nach der Passwortabfrage beispielsweise eine SMS auf das Mobiltelefon mit einem Code. Parallel erscheint ein Feld, das den übermittelten Code abfragt. Sofern verfügbar, sollte diese Option aktiviert werden.

Updates, Updates, Updates

Ohne einen aktuellen Virenscanner kann es sehr gefährlich sein, sich im Internet zu bewegen – gleich ob per Desktop-Computer oder Smartphone. Umso wichtiger ist es, die Virensoftware immer

aktuell zu halten. Nutzer sollten die Update-Hinweise ihrer Virensoftware ernst nehmen. Gleiches gilt für das Betriebssystem, den Browser, Add-Ons und die anderen Programme.

Phishing vorbeugen: Vorsicht bei dubiosen Mails

Beim Phishing verschicken Betrüger gefälschte Mails mit Links zu Online-Händlern, Bezahldiensten, Paketdiensten oder sozialen Netzwerken. Dort geben die Opfer dann nichtsahnend ihre persönlichen Daten preis. Häufig holt sich aber auch ein unerkannter Trojaner diese vertraulichen Informationen. Cyberkriminelle wollen so vor allem an die Identität der Opfer in Kombination mit den zugehörigen Zugangsdaten zu Online-Banking oder anderen Diensten kommen. Oberstes Gebot: den gesunden Menschenverstand nutzen. Banken und andere Unternehmen bitten ihre Kunden nie per E-Mail, vertrauliche Daten im Netz einzugeben. Diese Mails sind am besten sofort zu löschen. Das Gleiche gilt für E-Mails mit unbekanntem Dateianhang oder verdächtigen Anfragen in sozialen Netzwerken.

Backups einrichten

Durch regelmäßige Sicherungskopien, auch Backups genannt, bleiben persönliche Daten auch dann erhalten, wenn Geräte defekt sind oder verloren gehen. Die gesicherten Daten lassen sich anschließend auf einem neuen Gerät problemlos wiederherstellen. Daten-Backups lassen sich per Synchronisation mit einem Heim-PC aufspielen, mit Hilfe eines Massenspeichers wie einer Micro-SD-Karte oder über Cloud-Speicher.

Hinweis zur Methodik: Grundlage der Angaben ist eine repräsentative Umfrage, die Bitkom Research durchgeführt hat. Dabei wurden 1.004 Internetnutzer ab 16 Jahren telefonisch befragt. Die Fragestellung lautete: „Welche der folgenden Aussagen treffen auf Sie bei der Erstellung von Passwörtern für Ihre Online-Dienste, wie z.B. E-Mails, soziale Netzwerke oder Konten beim Online-Shopping, zu?“

Kontakt

Andreas Streim
Pressesprecher
Telefon: +49 30 27576-112
E-Mail: a.streim@bitkom.org
Download Pressefoto

Felix Kuhlenkamp
Leiter Sicherheit
Download Pressefoto
Nachricht senden

Direktlink: ***https://www.bitkom.org/Presse/Presseinformation/Jeder-dritte-Onliner-nutzt-dasselbe-Passwort-fuer-mehrere-Dienste***