Pressemitteilung

„Ändere dein Passwort“-Tag 2023: Passwort-Sicherheit anders gedacht

Aachen, 31. Januar 2023 – Jedes Jahr am 1. Februar soll uns der „Ändere dein Passwort“-Tag daran erinnern, wie wichtig die Sicherheit unserer Passwörter ist. Dieses Jahr gibt es gute Nachrichten für alle, denen viele Regeln zur Vergabe von Passwörtern zu kompliziert sind: Sichere Passwörter müssen gar nicht viel Arbeit machen.

Die Themen dieser Pressemeldung:

- **So geht es nicht: die beliebtesten Passwörter 2022**
- **Wichtig: unterschiedliche Passwörter**
- **Aufschreiben erlaubt**
- **Zwei-Faktor-Authentifizierung (2FA)**
- **Der Türsteher für das WLAN**
- **Preise und Verfügbarkeit**

So geht es nicht: die beliebtesten Passwörter 2022

Zuerst die schlechte Nachricht für Passwort-Muffel: Ein Minimum an Sicherheit und damit auch Komplexität sollten Kennwörter erfüllen. Das war auch im vergangenen Jahr viel zu oft nicht der Fall, wie das Hasso-Plattner-Institut zeigt. Das IT-Institut wertet Jahr für Jahr die in Deutschland am häufigsten verwendeten Passwörter aus und kommt dabei auch 2022 zu einem ernüchternden Ergebnis. Auf Platz 1 landet die wenig komplexe Zahlenkombination „123456“ – gefolgt von der nur bedingt fortgeschrittenen Fassung „123456789“. Die Top Ten deutscher Passwörter 2022 zeigt: Hier ist viel Luft für Verbesserungen.

Jetzt aber die gute Nachricht für alle, die bereits Schweißausbrüche beim Gedanken an das bekommen, was oftmals als Sicherheitsstandard propagiert wird: Sichere Kennwörter müssen nicht aus 20 Zeichen bestehen und nicht monatlich geändert werden. Viele altbekannte Passwortregeln gelten heutzutage als nicht mehr zeitgemäß. Und zwar vor allem, weil sie im Alltag kaum umsetzbar sind.

Wichtig: unterschiedliche Passwörter

Das liegt vor allem daran, dass wir immer mehr Kennwörter benötigen und benutzen. Mit der steigenden Zahl der genutzten Online-Shops, Streaming-Dienste und Mobile-Apps steigt schließlich auch die Anzahl von Account-Passwörtern. Da ist es unrealistisch zu erwarten, irgendjemand könnte sich ohne Gedächtnisstütze diverse vielstellige Passwörter auswendig merken – die zudem noch permanent geändert werden. Das wäre zwar theoretisch die sicherste Methode, scheitert jedoch schlichtweg an der Realität. Das bemerkt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI), das in den aktuellen Handlungsempfehlungen für die Kommunikation über Sicherheit bei Passwörtern mit einigen Klassikern der gut gemeinten Ratschläge Schluss macht.

Heutzutage gilt vor allem: Für unterschiedliche Accounts unterschiedliche Passwörter verwenden. Der Grund leuchtet schnell ein, denn gelangt ein Passwort mal in falsche Hände, so ist das schlimm genug. Der Schaden lässt sich jedoch schnell begrenzen, wenn die Eindringlinge damit zum Beispiel nur kurzzeitig Zugriff auf einen Streaming-Dienst erhalten. Öffnet die erbeutete Kombination aus E-Mail-Adresse und Kennwort hingegen den gesamten digitalen Aktenschrank, ist der Schaden groß. Durch die Isolierung der einzelnen Zugangsdaten ist eine Passwort-Änderung höchstens dann wirklich erforderlich, wenn es bei einem verwendeten Dienst zu einem Datendiebstahl kam.
Im Gegenzug dürfen die einzelnen Passwörter, je nach Wichtigkeit des Accounts, dafür auch mal etwas simpler ausfallen – sollten aber selbstredend komplexer sein als „123456789“. Da stellt sich natürlich die Frage, wie man sich so viele unterschiedliche Kennwörter merken soll.

Aufschreiben erlaubt

Klingt verrückt, dient aber der Alltagstauglichkeit: Das viele Jahre lang absolut verpönte Aufschreiben von Kennwörtern soll dem BSI zufolge „nicht als per se negativ dargestellt werden.“ Wichtig ist stattdessen, Passwörter richtig aufzuschreiben. Nämlich so, dass sie nicht sofort von jedermann zu finden sind. Post-It-Zettel mit den Zugangsdaten fürs Online-Banking direkt am Monitor sind entsprechend immer noch tabu. Sicher verwahrte Abschriften der wichtigsten Logins hingegen können die Online-Sicherheit stärken, wenn sie dazu ermutigen, hochwertige Kennwörter zu verwenden.
Noch komfortabler wird die Verwaltung durch Passwort-Manager, denen viele Menschen laut BSI-Informationen jedoch noch skeptisch gegenüberstehen. Diese Tools speichern Kennwörter ab, vergessen nichts und übernehmen auch die Erstellung garantiert zufälliger Zeichenfolgen. Durch die passenden Apps für Mobilgeräte oder Erweiterungen für Internetbrowser erleichtern sie sogar die Eingabe. Es gibt inzwischen eine riesige Auswahl derartiger Tools mit unterschiedlichsten Methoden zum Datenabgleich und Geschäftsmodellen für vielfältige Einsatzzwecke.

Zwei-Faktor-Authentifizierung (2FA)

Besonders empfehlenswert ist der Einsatz der sogenannten Zwei-Faktor-Authentifizierung. Diese Methode sorgt dafür, dass bei einem Login neben der Kombination aus Anmeldename und Kennwort noch eine weitere Komponente hinzugezogen wird, um die Identität des Nutzers zu bestätigen. Das können beispielsweise E-Mails mit Bestätigungslinks oder SMS-Nachrichten mit einmaligen Codes sein. Den meisten von uns dürfte diese Art des Logins vor allem durch das Online-Banking bekannt sein. Aber auch immer mehr Anbieter anderer Dienste bieten eine optionale Zwei-Faktor-Authentifizierung an. Diese sollte stets aktiviert werden, da die entsprechenden Accounts selbst mit schwächeren Kennwörtern gut geschützt bleiben. Denn zusätzlich zu den Login-Daten benötigen Dritte dann auch Zugriff zum Beispiel auf das Mobiltelefon, um sich einwählen zu können.

Der Türsteher für das WLAN

Nicht zu vergessen ist bei solchen Überlegungen das Kennwort für das private WLAN. Schließlich verbirgt sich dahinter das Heimnetzwerk mit allen angeschlossenen Geräten. Neben einem sicheren Passwort ist

deshalb auch auf moderne Sicherheitsfunktionen zu achten. Dazu gehört beispielsweise eine Verschlüsselung nach aktuellen Standards (mindestens WPA2). Diesen Anforderungen müssen neben dem Router auch alle anderen Geräte standhalten, die das Internet durch die heimischen vier Wände leiten – wie zum Beispiel Repeater. Die deutschen Netzwerkspezialisten von devolo aus Aachen liefern mit der Produktreihe devolo Magic WiFi eine sichere Netz-Verstärkung. Die flexibel einsetzbaren Adapter verwandeln jede Steckdose in einen pfeilschnellen Zugang für kabelgebundenes oder kabelloses Internet und erfüllen modernste Sicherheitsstandards: WP3 sowie WPA2 mit 128-Bit-Verschlüsselung sichern das Heimnetzwerk gegen Eindringlinge. Und durch clevere Extras wie zum Beispiel den Gästezugang per QR-Code oder App können Nutzer ebenso komplexe wie sichere Passwörter vergeben und ihren Gästen trotzdem bequem Zugriff gewähren.

Preise und Verfügbarkeit

Den idealen Einstieg in sichere Heimnetze mit devolo bildet das Starter Kit devolo Magic 1 WiFi mini mit zwei Adaptern zum Preis von 99,90 Euro. Anspruchsvolle Anwender erhalten mit dem devolo Magic 2 WiFi next Starter Kit für 199,90 Euro eine starke Kombination aus WLAN und Gigabit-LAN. Mit dem devolo Magic 2 WiFi 6 Starter Kit zieht zum Preis von 239,90 Euro modernstes Mesh-WLAN in die eigenen vier Wände ein.
Alle genannten Preise verstehen sich inklusive Mehrwertsteuer und alle der genannten Produkte sind miteinander kompatibel, um eine flexible Erweiterung des Heimnetzwerks zu ermöglichen. Zudem gewährt devolo auf alle Produkte eine Garantie von drei Jahren.

Pressekontakt

devolo AG
Marcel Schüll
Charlottenburger Allee 67
52068 Aachen
T: +49 241 18279-514
marcel.schuell@devolo.de

Diesen Text und aktuelle Produktabbildungen finden Sie auch im Pressebereich der devolo-Webseite unter www.devolo.de.

Über devolo

devolo entwickelt intelligente Heimvernetzungslösungen, die Highspeed-Internet in jeden Winkel von Haus und Wohnung bringen. Kernprodukt ist devolo Magic, eine Technologie, die smarte wie flexible Netzwerke über die Stromleitung ermöglicht. Komplettiert wird das Produktportfolio durch innovative Mesh-WLAN-Systeme und Lösungen für Glasfaseranschlüsse. Mit mehr als 45 Millionen verkauften Powerline-Adaptern zählt devolo zu den Marktführern weltweit. Über 700 internationale Testsiege und Auszeichnungen belegen die Innovationsführerschaft. devolo wurde 2002 in Aachen gegründet und ist in mehr als 10 Ländern vertreten.