Pressemitteilung

1. Februar ist „Ändere dein Passwort“-Tag

Aachen, 1. Februar 2022 – Die Zahl der Datenlecks klettert Jahr für Jahr auf neue Rekordhöhen, immer öfter werden digitale Identitäten gestohlen. Kein Wunder, denn schließlich heißen die beliebtesten Passwörter der Deutschen laut Hasso-Plattner-Institut „123456“ oder einfach „passwort“. Das ist viel zu einfach und nicht individuell genug. Der „Ändere dein Passwort“-Tag am 1. Februar soll jährlich daran erinnern, wie wichtig sichere Passwörter für den digitalen Alltag sind.

Die Themen dieser Pressemeldung:

- **Die beliebtesten Passwörter**
- **Wichtige Hinweise des BSI**
- **Die Faustregel: individuell, lang und komplex**
- **Die Satz-Methode**
- **Zwei-Faktor-Authentifizierung**

Die beliebtesten Passwörter

Auch wenn absoluter Schutz im Internet nicht möglich ist, sollten Nutzer ein paar Grundregeln beachten. Dazu zählt unter anderem die Wahl von langen, individuellen und komplexen Passwörtern. Doch nur wenige Deutsche nehmen diesen Rat ernst. Das Hasso-Plattner-Institut wertete 2021 eine Datenbank aus, in der mehr als 600 Millionen digitale Identitäten enthalten sind, die deutschen Accounts zugeordnet werden können und insgesamt 263 Datenlecks entstammen. Neben „123456“ (Platz 1), „passwort (Platz 2) und „12345“ (Platz 3) erfüllten auch die anderen Passwörter in der Bestenliste die wichtigsten Passwortkriterien nicht. In den Datenlecks fanden sich so simple und kurze Passwörter wie „hallo“, „schatz“, „basteln“ und „berlin“. Mit ein wenig Fantasie könnten die eigenen Accounts wesentlich sicherer sein.

Wichtige Hinweise des BSI

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) weist darauf hin, dass wichtige Lebensdaten und Namen tabu sind. Tastaturanschlagmuster wie beispielsweise „1234abcd“ oder Wörter, die nur am Ende Sonderzeichen enthalten, sind für Hacker zu leicht zu knacken. Ein wenig mehr Kreativität darf es schon sein. Wem es schwerfällt, sich komplexe Passwörter zu merken, kann einen Passwortmanager verwenden. Die Programme speichern alle Passwörter wie ein sicherer Tresor ab und bei Bedarf werden die verschlüsselten Daten automatisch eingesetzt. Das ist praktisch und sicher. Nutzer merken sich nur noch das Passwort für die Software an sich.

Die Faustregel: individuell, lang und komplex

Je nachdem was der Dienst erlaubt, sollten Passwörter für Online-Dienste Klein- und Großbuchstaben, Zahlen und Sonderzeichen enthalten. Je individueller, länger und komplexer das Passwort ist, umso besser. Das BSI erklärt, dass ein Passwort sicher ist, wenn es entweder 20 bis 25 Zeichen lang ist und zwei Zeichenarten nutzt oder wenn es acht bis zwölf Zeichen verwendet, die mindestens vier Zeichenarten nutzen. Auch kürzere Passwörter mit acht Zeichen sind möglich, sollten aber dann mindestens drei Zeichenarten verwenden und zusätzlich durch eine Zwei-Faktor-Authentifizierung abgesichert werden.

Auf dem Smartphone ist ein Sperrbildschirm das Mindeste – ob mit Passwort, Zahlen-PIN, Muster, Fingerabdruck oder Face-ID. Für unterschiedliche Dienste sollten unterschiedliche Passwörter verwendet werden, außerdem sollten sie regelmäßig geändert werden.

Die Satzmethode

Wer sich Passwörter nicht merken kann, dem hilft vielleicht die Satzmethode. Zunächst wählt man einen Satz, der leicht zu merken ist – beispielsweise „Pünktlichkeit ist die Höflichkeit der Könige“. Im ersten Schritt verkürzt man diesen Satz auf die Anfangsbuchstaben. In unserem Beispiel wäre dies demnach „PidHdK“. Jetzt noch ein Sonderzeichen einfügen und einen speziellen Buchstaben durch eine Zahl ersetzten: „Pi1H1K?“. Fertig! So lässt sich ein einfaches wie merkbares Passwort kreieren.

Zwei-Faktor-Authentifizierung

Ein weiteres zentrale Sicherheitstool ist die Zwei-Faktor-Authentifizierung. Viele große Internetfirmen bieten sie kostenlos an. Meldet sich ein Nutzer auf einer Internetseite an, muss anschließend noch ein Zufallscode, der per SMS zugesendet wird, eingegeben werden. Dies bedeutet: Selbst wenn Hacker das Passwort kennen, können sie sich nicht einloggen und den Account ausspähen oder sogar übernehmen. Aber aufgepasst! Beim Rufnummernwechsel müssen alle Profile aktualisiert werden, sonst können Hacker das Passwort theoretisch über eine SMS zurücksetzen.

Pressekontakt

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

Weitere Informationen: www.devolo.de

Über devolo

devolo sorgt für smarte Vernetzung und inspiriert Privatkunden sowie Unternehmen, die Möglichkeiten unserer digitalen Welt zu nutzen. Millionenfach bewährte Heimvernetzungslösungen von devolo bringen Highspeed-Internet und perfektes Mesh-WLAN in jeden Winkel von Haus und Wohnung – ganz einfach über das Stromnetz. Im professionellen Bereich wird mit devolo die Vision des umfassend vernetzten Internet of Things Realität. Ob in Industrieprojekten oder in der sich wandelnden Energiebranche: Wo hoch sichere, leistungsstarke Datenkommunikation gefragt ist, setzen Partner auf devolo. Das Unternehmen wurde 2002 gegründet und ist mit eigenen Niederlassungen sowie über Partner in 19 Ländern vertreten.