5 Tipps für ein sicheres Passwort

Welt-Passwort-Tag

von ASCONSIT | Veröffentlicht am 05. Mai 2022

Sichere Passwörter sind in der IT ein Dauerthema. Ob Privatperson oder Mitarbeitende in Unternehmen bzw. öffentlichen Institutionen: Jeder benötigt Passwörter, jeden Tag. Beispielsweise beim Zugang zum E-Mail-Account, der Anmeldung auf Social-Media-Plattformen oder beim Online-Shopping. Fakt ist aber auch: Nicht jedes Passwort schützt die Daten gleichermaßen gut und 100-prozentige Sicherheit gibt es ohnehin nicht. Wir User können nur versuchen, es einem Angreifer so schwer wie möglich zu machen. Leider sind in Zeiten von Digitalisierung und DSGVO unsichere Passwörter noch immer weit verbreitet. Dabei sind sichere Passwörter ganz einfach zu generieren und es gibt zahlreiche Hilfen bei deren Erstellung und Verwaltung. Die wichtigsten Tipps haben wir hier noch einmal für Sie zusammengestellt.

Tipp 1: Komplexe Passwörter

Dieser Tipp dürfte allen bekannt sein: Verwenden Sie möglichst „starke“ Passwörter. Doch was genau bedeutet stark? Im Zusammenhang mit Passwörtern steht „stark“ in der Regel für möglichst komplexe Passwörter. So gilt bei der Passwortgenerierung das Motto: Desto länger, umso sicherer. Daher wählen Sie am besten ein Passwort, das aus mindestens 14 Zeichen und vier Zeichenarten besteht. Bei dieser Länge ist das Passwort selbst ohne Zahlen und Sonderzeichen nur in mehreren Jahren Brute-Forcing zu knacken. Durch den Wechsel von Groß- und Kleinbuchstaben und die Verwendung von Zahlen und Sonderzeichen lässt sich die Passwortsicherheit noch weiter erhöhen.

Kurze Passwort-Checkliste

- Mindestens 14 Zeichen
- Wechsel von Groß- und Kleinbuchstaben (z. B. H, i, J, k)
- Zahlen (1, 2, 3, …)
- Sonderzeichen (Leerzeichen, ?, !, :, #)

Vermeiden Sie darüber hinaus die Verwendung von aufeinander folgenden Zeichen z. B. „aaaa“ oder „1234abcd“ genauso wie die Wahl einer Buchstabenabfolge auf der Tastatur (z. B. xcvb, rtzu). Auch sollten Sie keine offensichtlichen oder bekannten Begriffe wie die Namen von Familienmitgliedern, Haustieren, Freunden, Lieblingsstars oder Geburtsdaten verwendeten. Einzelbegriffe aus dem Lexikon bieten ebenfalls nur unzureichenden Schutz. Erst aus einer Kombination von mindestens vier Wörtern (mehr sind noch besser) lässt sich ein sicheres Passwort erstellen. Die einzelnen Wörter können Sie zufällig auswählen und zur Stärkung der Sicherheit noch jeweils mit einem Leerzeichen oder einem anderen Sonderzeichen verbinden.

Tipp 2: Ein individuelles Passwort je Zugang

Verwenden Sie für alle Zugänge und Accounts unterschiedliche Passwörter. Das macht das verwendete Passwort an sich zwar nicht sicherer, minimiert aber den Schaden, wenn das Passwort gehackt wird. Lauten mehrere Accounts eines Users auf die gleiche E-Mail-Adresse und ein Konto wird kompromittiert, haben Hacker bei mehrfach verwendeten Passwörtern leichtes Spiel und Zugang zu all diesen Accounts. Deshalb sollte man für jeden Zugang ein individuelles Passwort festlegen.

Tipp 3: Passwort-Generator und -Manager

Unser 3. Tipp ist die Verwendung eines Passwort-Managers. Dieser speichert Passwörter, wodurch man sich nicht mehr an jedes einzelne Passwort erinnern muss. Das macht es viel einfacher, für jedes Konto ein anderes Passwort zu verwenden. Auch erlauben die meisten Passwort-Manager, komplexe Passwörter zu generieren. So ist gewährleistet, dass das Passwort nicht mit einem einfachen Algorithmus bzw. der Brute-Force-Methode geknackt werden kann. Am besten ist es, den Passwort-Manager lokal zu installieren. So gibt man die Passwörter nicht aus den Händen, weil sie nicht in der Cloud abgelegt werden. Setzen Sie beim Master-Passwort auf ein starkes Kennwort, das den Zugriff auf die gespeicherten Passwörter schützt.

Besonders wichtig ist, die Passwörter geheim zu halten und niemanden weiterzusagen. Für weniger relevante Konten (z. B. bei Xing oder LinkedIn) eignen sich Wegwerfpasswörter. Das heißt, man nutzt für jedes Login ein Passwort nur einmal und erneuert es dann wieder (z. B. über die Passwort-Vergessen-Funktion). Prüfen Sie am besten, wo schützenswerte Daten hinterlegt und einsehbar sind und wo nicht. Passwörter, die sensible Daten schützen, sollten ohnehin nur an vertrauenswürdigen Rechnern eingegeben werden.

Tipp 4: Änderung des Passwortes

Grundsätzlich ist es wichtig zu wissen, dass das regelmäßige Ändern des Passwortes allein, das Passwort an sich nicht sicherer macht. Hier sei noch einmal auf Tipp 1 verwiesen. Dennoch kann es wichtig sein, dass Passwort zu ändern. Beispielsweise wenn Sie vermuten, dass Ihr Passwort in die Hände von unbefugten Dritten gelangt ist oder Ihr Computer mit Schadsoftware identifiziert ist. Sie sollten Ihr Gerät dann zunächst bereinigen und anschließend Ihre Zugangsdaten erneuern. Nach einer Passwortwiederherstellung durch ein System oder eine Applikation ist es ebenfalls sinnvoll, ein neues Passwort zu erstellen. Denn niemand weiß, wer das automatisch generierte Passwort ggf. mitlesen kann.

Tipp 5: Zwei-Faktor-Authentifizierung

Heutzutage bieten viele Plattformen eine sogenannte Zwei-Faktor-Authentifizierung (2FA) an. Diese sorgt dafür, dass nach dem Login mit Passwort eine weitere Hürde für mögliche Eindringlinge errichtet wird. Viele kennen das bereits von ihrem E-Banking-Konto. Der zweite Faktor ist dabei sehr variabel (z. B. Code via SMS, TAN-Generator), er erhöht die Zugriffssicherheit jedoch maßgeblich.

So funktioniert die Brute-Force-Methode: Der Begriff Brute-Force steht für das simple Ausprobieren einer großen Zahl möglicher Passwörter durch einen Angreifer. Oft werden Passwörter mit kryptografischen Hashfunktionen verschlüsselt, denn die Entschlüsselung eines Passworts, welches mit einem aktuellen Hashwert-Verfahren gebildet wurde, ist praktisch unmöglich. Allerdings kann der Angreifende die Hashwerte vieler einfacher Passwörter schnell berechnen. Stimmt ein Wert mit dem Wert des hinterlegten Passwortes überein, hat er das Passwort entschlüsselt. Die Brute-Force-Methode führt immer zum Erfolg. Es ist lediglich eine Frage der Zeit, denn bereits ein handelsüblicher Computer kann in einer Sekunde mehrere Millionen Kombinationen durchtesten. Der beste Schutz vor einem Brute-Force-Angriff ist ein langes Passwort mit hoher Komplexität, sodass das Ausprobieren aller möglichen Kombinationen so aufwendig wird, dass sich der Angriff erst gar nicht lohnt.

Fazit: Nutzer sollten Wert auf ein möglichst komplexes Passwort legen. Wenn dieses dann noch z. B. quartalsweise geändert wird, erhöht dies die Datensicherheit und den Schutz vor einem Cyberangriff erheblich. Darüber hinaus helfen ein Passwortgenerator und -Manager bei der Erstellung und Verwaltung von Passwörtern. All dies trägt dazu bei, Ihre Identität im Netz und Ihre Daten bestmöglich vor Angreifern zu schützen!