HORNETSECURITY

INFOPAPER:
PASSWORTSICHERHEIT RICHTIG UMGESETZT

Inhalt

Warum Passwortsicherheit so wichtig ist

Jeder kennt die grundsätzlichen Empfehlungen zum Thema Passwortsicherheit, aber nur die wenigsten halten sich an diese Vorgaben. Stattdessen tauchen regelmäßig Geburtsdaten, Namen von Kindern, Ehepartnern oder aneinandergereihte Tastaturkürzel, wie z.B. „qwertz" oder „123456789" auf, die einfach zu knacken sind.

Wiedererkannt? Dann sollten sich die **Passwortgewohnheiten schnellstens ändern,** um es Hackern so schwer wie möglich zu machen! Ein geknacktes Passwort kann schnell ernsthafte Konsequenzen haben und zu Identitätsdiebstahl sowie finanziellen Einbußen führen. Häufig gelingt es Hackern mit sogenannten Brute-Force-Attacken Passwörter zu entschlüsseln. Mit bestimmten Tools probieren Angreifer einfach eine große Anzahl an möglichen Kombinationen durch. Die Methode führt garantiert zum Erfolg, es ist nur eine Frage der Zeit. Selbst ein handelsüblicher Computer kann **in einer Sekunde mehrere Millionen solcher Kombinationen durchtesten.**

Wie man sich erfolgreich gegen Passwortdiebstahl zur Wehr setzt, wird im Folgenden beschrieben.

Safety first – Passwörter sicher erstellen

Angenommen ein gewöhnliches Passwort besteht aus sechs Zeichen und lediglich aus Kleinbuchstaben. Dies wären maximal 308.951.776 mögliche Kombinationen, die ein Brute-Force-Tool testen müsste, um die richtige Zeichenfolge zu entschlüsseln. Das klingt zwar erstmal viel – ist aber in wenigen Sekunden möglich. Um wirklich eine sichere Passwortkombination auszuwählen, sollte das **Passwort daher aus mindestens 12 bis 16 Stellen bestehen.**

Brute-Force-Attacken haben dann keine Chance mehr. Zudem ist es wichtig, dass das gewählte Passwort **Sonderzeichen wie beispielsweise Kommata, Bindestriche oder Ähnliches** beinhaltet.

Die Hornetsecurity-Sicherheitsexperten raten dringend dazu, auch Klein- und Großbuchstaben sowie Ziffern zu verwenden. Ein sicheres Passwort, bestehend aus 16 Stellen, wäre z.B. „s~;u+.LT`"tmP?;y".

Ein Passwort für alle Accounts — bequem, aber unsicher!

Das zuvor vorgeschlagene Passwort ist sicherlich nicht einfach zu merken und doch sollte eine solch komplizierte Kombination verwendet werden. Allerdings gibt es noch mehr zu beachten: **Viele Nutzer nutzen dasselbe Passwort für viele verschiedene Benutzerkonten.** Gelangt ein Cyberkrimineller an ein Passwort, würde es bedeuten, dass er mit nur einem Passwort auf E-Mail-Accounts, Online-Banking-Konten oder möglicherweise sogar auf das Firmennetzwerk zugreifen könnte. Es sollte daher immer **nur ein individuelles Passwort pro Benutzerkonto** verwendet werden. Dies erschwert einen etwaigen Angriff deutlich.

Passwort vergessen? Sicherheitsfragen mit Bedacht hinterlegen

Jeder hat schon einmal den einen oder anderen Zugangscode vergessen. Glücklicherweise lässt sich bei den meisten Online-Services das Passwort per Mail zurücksetzen. Ein Klick genügt, um mittels Bestätigungslink, der per Mail zugeschickt wird, eine neue Passwortvergabe vornehmen zu können.

Daneben gibt es ebenfalls die Möglichkeit, sich durch die sogenannte **Sicherheitsabfrage** Zugriff zum eigenen Account zu verschaffen. Fragen wie „Wie ist der Name Ihres Haustiers?" oder „Wie viele Kinder haben Sie?" gehören zum Standardrepertoire. Viele Nutzer schätzen diese Option sehr. Doch in Wahrheit handelt es sich auch hierbei um eine Sicherheitslücke.

Denn zumeist dreht es sich bei den ausgewählten Sicherheitsfragen **um personenbezogene Abfragen, deren Antworten auch völlig fremden Personen bekannt sein können** und sich schneller knacken lassen als das eigentliche Passwort. Aus diesem Grund ist es sinnvoll, Sicherheitsfragen auszuwählen, deren Lösung nur man selbst kennt.

Immer häufiger verzichten Online-Plattformen auf diese Funktion auch gänzlich. Google unterstützt diese Art der Wiederherstellung bereits seit längerer Zeit nicht mehr und seit 2019 wird die Sicherheitsfrage beispielsweise auch bei den E-Mail-Anbietern GMX und Web.de nicht mehr zur Registrierung abgefragt.

Aufbewahrung des Passworts

Die Hornetsecurity-Sicherheitsexperten empfehlen,das **Passwort unter keinen Umständen in einer Textdatei auf der Festplatte aufzubewahren.** Ebenfalls sollte nicht auf die automatische Passwortspeicherung im Browser zurückgegriffen werden. Denn wenn der Rechner in die falschen Hände gerät, haben Kriminelle leichtes Spiel. Insbesondere wenn man sich in einem öffentlichen Netzwerk, z.B. in einem Café oder in der Bahn, befindet, muss darauf geachtet werden, dass Dritte keinen Zugang zum Rechner erlangen.

Der Passwort-Manager als Lösung

Einen großen **Vorteil für die Passwortsicherheit birgt ein Passwort-Manager** wie KeePass. Es handelt sich hierbei um eine Verwaltungssoftware, die es ermöglicht Passwörter sicher abzulegen. Dabei wird lediglich ein Master-Key benötigt, um sich in das Programm einzuloggen und auf die anderen Passwörter zuzugreifen. Dies ist zwar praktisch, aber auch hier gibt es gewisse Punkte, die man bedenken muss: Der Master-Key für das Verwaltungsprogramm sollte ein überdurchschnittlich langes Passwort von 24 Zeichen sein. Auch beim **Master-Key gilt es, eine Kombination aus Buchstaben, Zahlen und Sonderzeichen** zu verwenden, die bisher noch an keiner anderen Stelle zum Einsatz kam.

Dritte und auch Personen, die sich einem gegenüber als Vertrauensperson oder Autorität ausgeben, haben kein Recht, die gewählte Passwortkombination zu erfahren.

Checkliste

Sofern man die oben aufgeführten Punkte berücksichtigt, wird es **Cyberkriminellen dank der hohen Passwortsicherheit erheblich erschwert,** Zugang zu privaten Accounts zu erhalten. Anhand der folgenden Checkliste kann sich jeder **regelmäßig die wichtigsten Aspekte für einen sicheren Passwortumgang in Erinnerung rufen.**

- ☑ **Die Passwortlänge** sollte mindestens 12 Zeichen betragen, inklusive Sonderzeichen und Groß- und Kleinschreibung.
- ☑ Ein Passwort **nur für einen Account** verwenden.
- ☑ Nur **persönliche Sicherheitsfragen** auswählen, deren Antworten niemand herausfinden kann.
- ☑ Passwörter **nicht in Textdateien** auf dem Rechner oder im Browser speichern.
- ☑ Passwörter **niemals mit anderen Personen teilen.**
- ☑ **Passwort-Manager** wie KeePass verwenden.