Mittelstand-Digital
Zentrum
Chemnitz

NACHGELESEN

Authentifizierung: Schutz durch sichere Passwörter und erweiterte Sicherheitsmaßnahmen

ROLAND HALLAU

Mittelstand-Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Digitale Sicherheit ist heute wichtiger denn je, da Passwörter oft das erste Ziel von Hackerangriffen sind. Doch warum genau sind Passwörter so wichtig und wie können sie sicher gestaltet werden? In diesem Nachgelesen gehen wir auf diese und weitere Fragen ein und bieten praxisnahe Tipps für mehr Sicherheit im digitalen Alltag. Lesen Sie im Folgenden, welche Maßnahmen Sie ergreifen können, um Ihre Daten zu schützen und welche Technologien Ihnen dabei helfen können:

- Warum sind Passwörter und deren Schutz so wichtig?
- Was passiert, wenn Kriminelle an Ihr Passwort gelangen?
- Möglichkeiten zur Erstellung komplexer Passwörter
- Einsatz eines Passwortmanagers
- Was sind Passkeys und wie funktionieren sie?
- Die Mehrfachauthentifizierung mit dem Passwortmanager in einem Tool verbinden.

Impressum

HERAUSGEBER
Mittelstand-Digital Zentrum Chemnitz
Tel: 0371 531 19935
Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

REDAKTION Anikó Lessi

GESTALTUNG
PUNKT191 – Marketing und Design
www.punkt191.de

BILDNACHWEIS TITEL Dan Nelson auf Unsplash
VERÖFFENTLICHUNG Juli 2024

© Kenny Eliason auf Unsplash

Authentifizierung: Schutz durch sichere Passwörter und erweiterte Sicherheitsmaßnahmen

Warum sind Passwörter und deren Schutz so wichtig?

Passwörter sind oft das erste Ziel für Hackerangriffe[1], da sie einen direkten Zugang zu persönlichen Informationen und sensiblen Daten bieten. Schwache Passwörter, die leicht zu erraten sind oder häufig verwendet werden, erhöhen das Sicherheitsrisiko erheblich. Ein häufiges Problem ist die Verwendung von einfachen Wörtern, Geburtsdaten oder Namen, die leicht zu erraten sind. Solche Passwörter sind anfällig für Brute-Force-Angriff[2], bei denen automatisierte Programme systematisch verschiedene Kombinationen durchprobieren, um Zugang zu einem Konto zu erhalten.

Was passiert, wenn die Angreifer an das von Ihnen gesetzte Passwort gelangen?

Durch den Zugriff auf persönliche Konten können Kriminelle Identitätsdiebstahl begehen, indem sie sich als die betroffene Person ausgeben und in ihrem Namen handeln. Dies kann zu finanziellen Verlusten, Rufschädigungen und rechtlichen Problemen führen.

Gehackte Passwörter ermöglichen den Zugriff auf persönliche oder vertrauliche Daten wie E-Mails, Nachrichten, Fotos und Dokumente. Diese Informationen können für Erpressung, Betrug oder den Verkauf auf dem Schwarzmarkt genutzt werden.

Wenn ein gehacktes Konto verwendet wird, um betrügerische oder schädliche Aktivitäten durchzuführen, kann dies zu schwerwiegenden Rufschäden für den legitimen Kontoinhaber oder die legitime Kontoinhaberin führen, besonders wenn andere Personen dadurch geschädigt werden.

Möglichkeiten zum Schutz vor Passwortmissbrauch

Um sich effektiv zu schützen, sollten Sie robuste Passwörter verwenden, die aus einer Mischung von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen und mindestens eine Länge von zwölf Zeichen besitzen. Jetzt fragen Sie sich, warum genau diese Länge? Je länger und komplexer das Passwort ist, desto länger brauchen Hacker, um es knacken zu können und lassen ggf. ab, weil es nicht funktioniert. Die Beispiele in Tabelle 1 verdeutlichen dies.

Tabelle 1: Zeitaufwand zum Knacken von Passwörtern[3]

Passwort	Dauer bis zum erfolgreichen Angriff
Standard123	weniger als eine Sekunde
Fruehling2024	40 Minuten
NamelautetTasse24!	1.722 Jahre
+WvMkz3V,weuPg4&	Mehrere Millionen Jahre

Möglichkeiten zur Erstellung komplexer Passwörter

Zur Erstellung komplexer Passwörter stehen Ihnen verschiedene Optionen zur Verfügung. Beispielweise reihen Sie mehrere Wörter aneinander, nutzen einen Passwortsatz und ersetzen hier Zeichen durch Sonderzeichen oder Zahlen bzw. nutzen einen Passwortmanager, welcher anhand Ihrer Vorgaben ein Passwort generiert

Die vielen komplexen Passwörter für alle Anwendungen im privaten und beruflichen Kontext lassen sich nur schwer merken. Doch dafür gibt es eine Geheimwaffe. Sie wollen wissen welche? Wir beantworten Ihnen die Frage. Es handelt sich hierbei um den Passwortmanager. Zu den bekanntesten Passwortmanagern[4] gehören zum Beispiel KeePass oder Enpass.

Einsatz eines Passwortmanagers

Ein wichtiger Schritt ist die Nutzung eines Passwortmanagers[4], um die komplexen Passwörter sicher speichern und automatisch für verschiedene Konten generieren zu können. Mit ihrer Hilfe müssen Sie sich die komplizierten Passwörter nicht merken und auch nirgends aufschreiben. Ein Passwortmanager erfordert zum Schutz der gespeicherten Passwörter ein Masterpasswort, das natürlich ein qualitativ gutes Passwort sein sollte und welches Sie sich dann merken müssen.

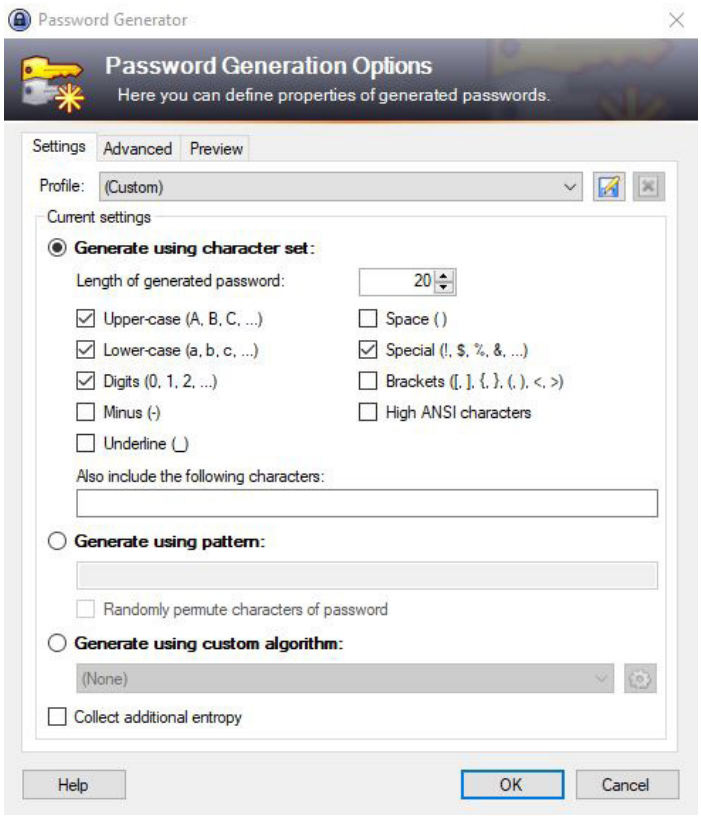

Abbildung 1: Beispiel für die Passworterstellung mit eigenen Vorgaben in KeePass

Sie verwenden komplexe Passwörter und einen Passwortmanager und fühlen sich dennoch nicht vollends abgesichert? Dann können Sie zusätzlich Passkey[5] und/oder eine Mehrfachauthentifizierung[6] einrichten. Auch wenn Kriminelle ihr Passwort besitzen, kommen sie nicht an die Daten heran, da Ihnen der zusätzliche Faktor für die Authentifizierung fehlt.

Was sind Passkeys und wie funktionieren sie?

Passkey ist ein Begriff, der sich oft auf eine Methode zur Authentifizierung oder zum Zugang zu einem System bezieht. Im Allgemeinen bezeichnet Passkey einen speziellen Schlüssel oder Code, der verwendet wird, um Zugriff auf etwas zu erhalten.

Passkey ist ein physischer Schlüssel, den man verwendet, um symbolisch eine Tür zu öffnen. Er passt genau zu einem bestimmten Schloss und ermöglicht nur autorisierten Personen den Zugang.

Im digitalen Bereich kann ein Passkey ein spezieller Code oder ein Passwort sein, das benötigt wird, um auf ein Computer-System, eine App oder ein Online-Konto zuzugreifen. Dieser Code dient als Sicherheitsmaßnahme, um sicherzustellen, dass nur berechtigte Benutzerinnen und Benutzer Zugriff haben.

Passkeys funktionieren meist in Verbindung mit anderen Sicherheitsmethoden wie Benutzername und Passwort oder

sogar mit zusätzlicher Sicherheit wie Fingerabdruck- oder Gesichtserkennung. Sie sind eine wichtige Maßnahme, um sicherzustellen, dass nur die richtigen Personen Zugriff auf geschützte Bereiche oder Informationen erhalten.

Zusammengefasst ist ein Passkey also ein Schlüssel oder Code, der verwendet wird, um Zugriff zu gewähren, sei es physisch oder digital, und der dazu dient, Sicherheit und Zugangskontrolle zu gewährleisten.

Die Mehrfachauthentifizierung mit dem Passwortmanager in einem Tool verbinden

Die Mehrfaktorauthentifizierung (MFA) oder auch Zwei-Faktor-Authentifizierung (2FA)[7] ist ein Sicherheitsmechanismus, der zusätzlich zum traditionellen Benutzername und Passwort verwendet wird, um den Zugang zu einem Konto oder einer Anwendung zu schützen. Sie funktioniert folgendermaßen:

Statt sich nur mit einem Passwort anzumelden, erfordert die MFA eine zweite Form der Authentifizierung. Dies könnte etwas sein, das der Nutzende besitzt (z. B. ein Einmalcode per SMS, eine Authentifizierungs-App oder ein physischer Sicherheitsschlüssel) oder etwas, das der Nutzende ist (z. B. biometrische Daten wie Fingerabdruck oder Gesichtserkennung).

Nachdem die nutzende Person ihr Passwort eingegeben hat, wird sie aufgefordert, einen zweiten Faktor zu liefern. Dies kann durch eine Benachrichtigung an das Mobilgerät geschehen, die einen Einmalcode enthält, den der Benutzer eingeben muss. Alternativ kann eine Authentifizierungs-App wie Google Authenticator, privacyIDEA oder ein physischer Sicherheitsschlüssel verwendet werden, um einen Code zu generieren oder zu überprüfen.

MFA erhöht die Sicherheit, da selbst, wenn ein Hacker das Passwort kennt oder stiehlt, er zusätzlich Zugriff auf den zweiten Faktor benötigt, um sich erfolgreich anzumelden. Dies macht es schwieriger für unbefugte Personen, auf Konten oder Informationen zuzugreifen, selbst wenn das Passwort kompromittiert ist.

Insgesamt bietet die Mehrfaktorauthentifizierung eine wichtige zusätzliche Sicherheitsebene und wird daher von vielen Online-Diensten und Unternehmen empfohlen, um die Sicherheit von Benutzerkonten zu verbessern und unbefugten Zugriff zu verhindern.

Fazit

Insgesamt ist die Sicherheit von Passwörtern von entscheidender Bedeutung für den Schutz persönlicher Daten und Online-Identitäten. Durch die Nutzung sicherer Praktiken und Technologien können Nutzer ihre Sicherheit im Internet erheblich verbessern und das Risiko von Hackerangriffen minimieren.

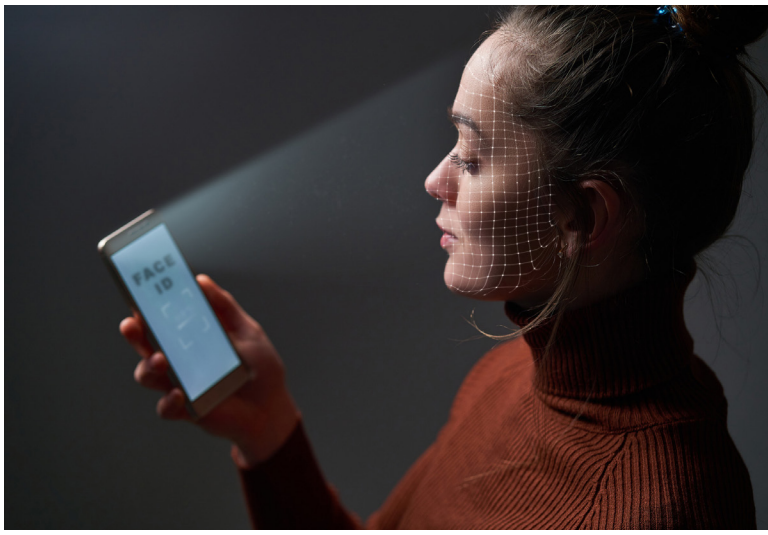

Abbildung 2: Gesichtserkennung für zusätzliche Sicherheit

Anmerkungen/Quellen

1 Reinstädtler, G. (2018, 15. November). Definition: Cyberangriff. Gabler Banklexikon. https://www.gabler-banklexikon.de/definition/cyberangriff-81516/version-347718

2 Schmitz, P. & Luber, S. (2019, 19. März). Was ist ein Brute-Force-Angriff? Security-Insider. https://www.security-insider.de/was-ist-ein-brute-force-angriff-a-677192

3 Lucid. (o. D.). Passwortcheck. passwortcheck.ch. https://www.passwortcheck.ch/

4 Passwort-Manager im Vergleich - Infos & Tipps | datenschutz.org. (2024, 22. Februar). Datenschutz. https://www.datenschutz.org/passwort-manager-vergleich

5 Schafft die Passwörter ab?! (o. D.). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/passkeys-anmelden-ohne-passwort_node.html

6 Wikipedia-Autoren. (2018, 12. Oktober). Multi-Faktor-Authentisierung. https://de.wikipedia.org/wiki/Multi-Faktor-Authentisierung

7 Zwei-Faktor-Authentisierung. (o. D.). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html

Autor

ROLAND HALLAU ist Projektmanager bei der tti Technologietransfer und Innovationsförderung Magdeburg GmbH. Im Mittelstand-Digital Zentrum Chemnitz ist er als Fachkoordinator im Bereich IT-Sicherheit tätig.
roland.hallau@digitalzentrum-chemnitz.de

Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

WAS IST MITTELSTAND-DIGITAL?

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren, der Initiative IT-Sicherheit in der Wirtschaft und Digital Jetzt umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Mittelstand-Digital
Zentrum
Chemnitz

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages