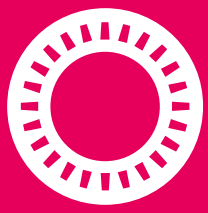


MATESO
PASSWORD SAFE

Passwort-Richtlinien

Zeit für einen Paradigmenwechsel?

Inhaltsverzeichnis

Einleitung

Immer mehr Sicherheitsexperten sind der Ansicht, dass vorgegebene Passwort-Richtlinien der IT-Sicherheit von Unternehmen eher schaden als nutzen. Das Bundesministerium für Sicherheit in der Informationstechnik (BSI) rät mittlerweile von festen Mindestvorgaben zu Komplexität und Länge von Passwörtern ab als auch davon, diese regelmäßig auszutauschen.[1] Auch das National Institute of Standards and Technology (NIST) tritt von seiner einstmaligen Empfehlung zurück, Passwörter alle 90 Tage zu wechseln und hat seine Komplexitäts-Anforderungen heruntergefahren.[2]

Dieses Whitepaper behandelt das Risiko- sowie das Sicherheitspotential von Passwort-Richtlinien für Unternehmen sowie die Entwicklung hin zu einer Lockerung, um daraus resultierende Handlungsempfehlungen abzuleiten.

> **Passwörter sollten nur bei einem validen Grund gewechselt werden.**
>
> Bundesamt für Sicherheit der Informationstechnik

Risikoanalyse

Um Transparenz über Art und Umfang potentieller Risiken durch Passwort-Richtlinien in der Praxis zu schaffen, werden im ersten Schritt die Anforderungen an ein sicheres Passwort und den Umgang damit definiert und im Anschluss mögliche Ursachen für einen Paradigmen-Wechsel identifiziert und bewertet.

Sicherheitsanforderungen an Passwörter

Bei der Erstellung von Passwörtern sind Komplexität und Länge zwei für die Sicherheit entscheidende Merkmale. Laut dem BSI muss für jede Anwendung ein eigenständiges, mindestens acht Zeichen langes Passwort definiert und dieses geheim gehalten und sicher aufbewahrt werden. Es darf nur dem Benutzer bekannt sein.[1]

7 goldene Passwort-Regeln

(UN?v*UG7p!9?aaQ/ — **Je komplexer und länger, desto besser**

Pro Zugang ein einzigartiges Passwort verwenden

ABC 123 !?$ — **Nicht sparen mit: Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen**

Regelmäßige Änderungsintervalle einführen

PASSWORD1234 — **keine Wörter sowie Abfolgen (123, abc, qwertz) nutzen**

Tabu sind: Infos wie Geburtsdatum, Haustiername & Co.

PASSWORD SAFE — **Hilfestellungen dringend empfohlen: Nutzen Sie Passwort-Generatoren und Password Manager!**

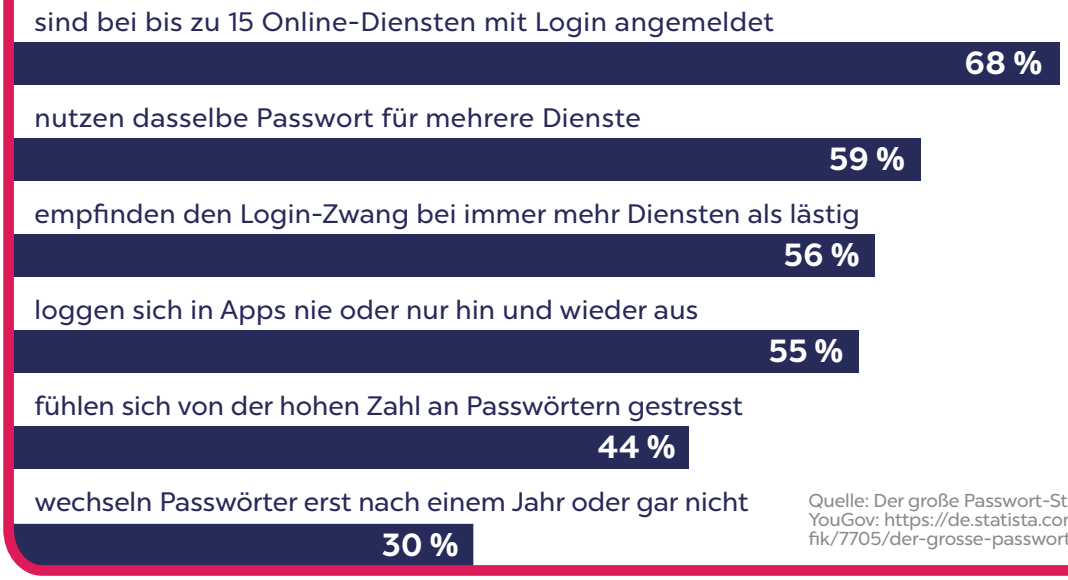
Dabei sollte das Passwort Sonderzeichen, Ziffern sowie abwechselnd Groß- und Kleinbuchstaben besitzen und keine Wörter aus dem Wörterbuch enthalten. No-Go`s sind Zahlen- und Buchstabenreihen sowie Tastaturmuster. Bisher wurde auch nahelegt, das Passwort nach einem bestimmten Zeitintervall zu wechseln.[3]

Verwirrung & Überforderung als Folge

Stellt man nun diese Anforderungen dem Fakt gegenüber, dass jeder Benutzer mindestens 15 Online-Zugänge zu verwalten hat, wird deutlich, dass die Einhaltung diverser Regeln den einzelnen Mitarbeiter in der Realität schnell überlasten kann.[4] Als Folge macht sich bei Mitarbeitern die so genannte „Password Fatigue“ breit – das Gefühl der Überforderung beim Erstellen und Merken von zu vielen, zu komplexen Passwörtern.

Der große Passwort-Stress

Befragte Internet-Nutzer zu ihrem Umgang mit Passwörtern



Quelle: Der große Passwort-Stress, YouGov: https://de.statista.com/infografik/7705/der-grosse-passwort-stress/“

Diese Last wächst noch durch automatische Log-outs, wodurch das Passwort erneut eingetippt werden muss sowie die Herausforderung, Kollegen die Zugangsdaten zur Verfügung zu stellen, ohne dabei gegen die Richtlinien zu verstoßen. Je mehr Regeln noch hinzukommen, desto höher wird die Wahrscheinlichkeit, dass Mitarbeiter kapitulieren und zu unsicheren Behelfslösungen greifen.

Unsichere Behelfslösungen in der Praxis

Wenn Mitarbeiter überfordert sind, greifen Passwort-Richtlinien ins Leere. Stattdessen wird zu unsicheren Mitteln gegriffen, die der internen IT oft gar nicht bekannt sind. Dem Marktforschungsunternehmens Ipsos zufolge merkt sich jeder zweite sich sein Passwort selbst. Im ersten Fall wird also erst gar kein sicheres Passwort erstellt.[5]

Im zweiten Fall erstellt der Mitarbeiter zwar ein komplexes Passwort. Da diese allerdings nur schwer zu merken sind, schreiben 1 von 5 es einfach auf und verwenden es zugleich für mehrere Dienste.[5] Gleichermaßen beliebt wie gefährlich sind zudem selbst gebastelte Lösungen wie das Speichern im Browser oder in unsicheren Dokumenten wie Excel-Listen. Dabei wechselt nur 1 von 3 sein Passwort regelmäßig. Wird das Kennwort doch ausgetauscht, wird getrickst, indem nur ein Zeichen ausgetauscht oder angehängt wird.

Niedrigere Vorgaben als Lösung?

Als Folge hat sich das Bundesamt für Sicherheit in der Informationstechnik dieses Jahr von genauen Mindestangaben zur Passworterstellung verabschiedet und empfiehlt nun eine Länge von 8 bis 25 Zeichen in Kombination mit zwei bis vier Zeichenarten.[1] Dabei gilt: Je kürzer, desto komplexer und umgekehrt. Auch NIST bezieht sich in seiner Änderung darauf, dass Benutzer Forschungen zufolge durch genau vorgegebene Angaben sehr vorhersehbare Änderungen vornehmen würden wie das bloße Anhängen eines Sonderzeichens.[2]

Es ist durchaus sinnvoll, keine allgemeingültigen Mindestvorgaben für jedes Unternehmen einzuführen, da diese daraufhin auch Hackern bekannt sind und von ihnen als Ausschlusskriterium verwendet werden um, um Passwörter zu knacken. Jedoch sind Unternehmen selbst in der Pflicht, präzise Mindest-Anforderungen an firmeninterne Passwörter zu stellen für deren Umsetzung Sorge zu tragen.

Auch distanziert sich das BSI vom regelmäßigen Passwort-Wechsel: „IT-Systeme oder Anwendungen SOLLTEN NUR mit einem validen Grund zum Wechsel des Passworts auffordern. Reine zeitgesteuerte Wechsel SOLLTEN vermieden werden. Es MÜSSEN Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen. Ist dies nicht möglich, so SOLLTE geprüft werden, ob die Nachteile eines zeitgesteuerten Passwortwechsels in Kauf genommen werden können und Passwörter in gewissen Abständen gewechselt werden.“ [6] Dabei wird nicht näher darauf eingegangen, wann ein solcher valider Grund vorliegt und welche Nachteile genau durch einen zeitgesteuerten Wechsel gemeint sind. Diese Änderung wird von Experten gefeiert, da Mitarbeiter nicht mehr mit Passwort-Wechseln gequält werden würden.[7]

Da Unternehmen oft gar nicht oder erst zu spät erfahren, wenn ihre Zugangsdaten in falsche Hände geraten, ist die Empfehlung, Passwörter nur bei Verlust oder Datendiebstahl zu verändern, hinfällig. Ein regelmäßiger Austausch von Passwörtern ist deshalb immer noch notwendig, da die Gefahr einer Kompromittierung mit der Dauer der Nutzung steigt.

Nachdem die Ursachen für die unsachgemäße Handhabung von Passwörtern aus zu hohen Anforderungen resultieren, ist der Paradigmen-Wechsel des BSI eher als aus der Not heraus einzustufen. Wenn auch der Zweck, Nutzer zu entlasten, wohlgemeint war, löst es nicht das Sicherheitsproblem, keinen Passwort-Wechsel mehr durchzuführen. Eher wird das Sicherheitsrisiko noch verschärft, wenn keine klaren Anweisungen an Mitarbeiter kommuniziert werden.

Risiko-Bewertung ohne Passwort-Richtlinien

Kennen Sie Ihre Mitarbeiter?

Wenn Sie diese Fragen nicht sofort mit „Ja“ beantworten können, können Passwort-Richtlinien die I T-Sicherheit in Ihrem Unternehmen sogar verschlimmern:

Sind Sie sicher, dass Ihre Mitarbeiter keine unsicheren Behelfslösungen wie das Speichern im Browser oder das Teilen von Passwörtern via Chat und E-Mail nutzen?

Können Sie verhindern, dass Ihre Mitarbeiter selbstständig unsichere Passwörter (neu) setzen?

Haben Sie noch Überblick über alle Anmeldedienste und Passwörter im Unternehmen?

Wissen Sie, wann welcher Mitarbeiter Zugriff auf welches Passwort hatte?

Wissen Sie, ob Ihre Mitarbeiter sich auch wirklich an Ihre Passwortvorgaben halten?

Aus der Analyse folgt, dass nicht Passwort-Richtlinien dafür verantwortlich sind, dass Mitarbeiter zu unsicheren Behelfslösungen greifen, sondern der Mangel an Tools und Prozessen. Richtig angewandt bieten Passwort-Richtlinien in Kombination mit einer Password Management Lösung essentiellen Schutz für Unternehmen.

Auf den regelmäßigen Austausch von Passwörtern zu verzichten, trifft deshalb weder den Kern des Problems, noch sorgt es für mehr Sicherheit. Vielmehr kann es dazu führen, dass noch schlechtere Passwörter über einen längeren Zeitraum verwendet werden und Angreifern dadurch mehr Zeit geben, diese zu erraten.

> **Selbst bei hochkomplexen Passwörtern ist ein stetiger Austausch unabdingbar, um Angreifer auszusperren und Sicherheitslücken zu schließen.**
>
> Sascha Martens, CTO MATESO GmbH

Werden Mitarbeiter allerdings gezwungen, ihre Passwörter regelmäßig auszutauschen, ohne ihnen das notwendige Know-how sowie Systeme zur Verfügung zu stellen, steigt das Risiko, dass dies auf Kosten der Passwort-Qualität durchgeführt wird als auch das einer Kompromittierung. Die Passwörter in Unternehmen nach selbst definierten Regeln zu setzen und nach einer bestimmten Zeit auszutauschen ist also weiterhin sinnvoll, da selbst bei starkem Passwort-Schutz immer ein Restrisiko bestehen bleibt.

Password Manager als essentieller Bestandteil im gesamten Unternehmen

Die Erfahrung sowie der Paradigmenwechsel bei der Vorgabe von Passwort-Richtlinien hat gezeigt, dass all diese Regeln oft in der Umsetzbarkeit scheitern. Im besten Fall nutzen Unternehmen deshalb Passwort-Generatoren, um den Menschen von diesem sicherheitskritischen Vorgang zu entkoppeln und sicherzustellen, dass die Richtlinien eingehalten werden.

Passwörter sind wie Zahnbürsten: Für einen spürbaren Effekt sollte man sie täglich verwenden, regelmäßig wechseln, mit niemandem teilen und nicht offen zugänglich herumliegen lassen.

So werden hochkomplexe Passwörter in Sekundenschnelle erstellt und im Idealfall automatisch im dazugehörigen Password Manager gespeichert und zum Login verwaltet. Das bedeutet: Der Mitarbeiter kennt das Passwort gar nicht, kann sich jedoch trotzdem sicher via Single-Sign-on einloggen. Durch die rollenbasierte Rechtevergabe kann eingestellt werden, dass Mitarbeiter Passwörter nur zum Login verwenden, bearbeiten oder sicher mit Kollegen teilen können.

Zudem können bestimmte Auslöser definiert werden, nach denen automatisch neue sichere Passwörter gesetzt werden – etwa nach temporären Freigaben für externe Dienstleister, was zu einer extremen Entlastung in der Passwort-Verwaltung führt.

Auch Sicherheits-Richtlinien bezüglich Mindestlänge und Komplexität können mithilfe eines Password Managers für die automatische Passwort-Erstellung vordefiniert werden. Die Vergabe von individuellen Sicherheitsstufen und die Einschränkung von Berechtigungen gewährleistet zudem, dass besonders sensible Konten und Zugänge ihren Anforderungen entsprechend geschützt sind.

Außerdem können Password Manager dazu beitragen, das Sicherheitsbewusstsein von Mitarbeitern zu stärken: Durch Benachrichtigungen in der Software werden diese darauf hingewiesen, wenn ihr vergebenes Passwort nicht stark genug ist, um sie beispielsweise automatisch dazu aufzufordern, ein neues, besseres Passwort zu setzen. So sind Benutzer bei der Erstellung von Passwörtern nicht allein gelassen und kommen erst gar nicht auf die Idee, aus der Not heraus zu noch unsichereren Mitteln zu greifen.

Umsetzung von Schutzmaßnahmen

Wir empfehlen, die Einführung von Passwort-Richtlinien mit folgenden Schutzmaßnahmen zu kombinieren:

- **Analysieren Sie, wenn vorhanden, die bisherige Umsetzung von Passwort-Richtlinien in Ihrem Unternehmen.**
- **Bewerten Sie das Sicherheitsniveau der bisherigen Mechanismen zur Passworterstellung und -verwaltung.**
- **Führen Sie regelmäßige Security Awareness Trainings durch.**
- **Definieren Sie mindestens einen konkreten Ansprechpartner für Sicherheitsfragen.**
- **Stellen Sie sicher, dass jeder Mitarbeiter die Notwendigkeit und richtige Umsetzung von Passwort-Richtlinien verstanden hat.**
- **Überprüfen Sie die Einhaltung dieser durch die Einführung von Password Management Tools und Prozessen.**

Fazit

Fest steht, dass Unternehmen auch die stärksten Passwort-Richtlinien nichts nützen, wenn Mitarbeiter bei der Erstellung und Verwaltung von Passwörtern alleine gelassen werden. Dass Behörden und Sicherheitsexperten nun die Richtlinien entschärft haben, ist trotzdem ein falsches Signal, das nicht die Ursache – die Überforderung der einzelnen Nutzer – bekämpft und Hackern sogar noch in die Hände spielen kann. Stattdessen sollte die Notwendigkeit eines Password Managers noch mehr herausgestellt werden, um Benutzer zu entlasten und weiterhin im Kampf gegen Cyber-Bedrohungen Schritt zu halten.

Das perfekte Passwort sollte ...

in einem digitalen Tresor liegen.

lang, komplex und schwer zu merken sein.

automatisch eingetragen werden.

am besten niemand kennen!

Geben Sie Ihren Mitarbeitern also lieber wertvolle Tipps an die Hand und stellen Sie ihnen einen Password Manager zur Umsetzung zur Verfügung. Zudem ist ein konkreter Sicherheitsexperte essentiell, um die Mitarbeiter stets in den Password Management Prozess miteinzubeziehen, sie aufzuklären und so verhindern, dass es zu unsicheren Lösungen wie „Password1“ und Excel-Listen kommt.

Quellenverzeichnis:

[1] Bundesamt für Sicherheit in der Informationstechnik 2020; Empfehlungen: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

[2] National Institute of Standards and Technology 2020; Digital Identity Guidelines: https://www.nist.gov/itl/tig/projects/special-publication-800-63

[3] Bundesamt für Sicherheit in der Informationstechnik; Pressebereicht 2011: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2011/Passwortsicherheit_27012011.html

[4] YouGov; Der große Passwort-Stress: https://de.statista.com/infografik/7705/der-grosse-passwort-stress/

[5] Ipsos Online-Umfrage 2005; Internetnutzer, die in den letzten drei Monaten etwas online gekauft haben: https://de.statista.com/statistik/daten/studie/3609/umfrage/uebersicht-ueber-eigene-online-passwoerter/

[6] Bundesamt für Sicherheit in der Informationstechnik 2020: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identitäts-_und_Berechtigungsmanagement.html

[7] Süddeutsche Zeitung 2020; Die Qual des ständigen Passwort-Wechsels endet: https://www.sueddeutsche.de/digital/passwort-wechseln-bsi-1.4784293

MATESO

Die MATESO GmbH ist ein führendes deutsches IT-Unternehmen, das sich seit der Firmengründung in 2006 erfolgreich im DACH-Raum etabliert hat. Die entwickelte Passwort-Sicherheitslösung Password Safe wird durch ihr weltweites Partnernetzwerk international vertrieben. Namhafte Referenzen bezeugen den Technologie- und Know-how-Vorsprung der IT-Software.

Heute verzeichnet das stetig wachsende Unternehmen branchenübergreifend über 10.000 Firmenkunden mit mehreren Millionen Anwendern weltweit – darunter 20 Firmen der Dax 30.

PASSWORD SAFE

Pioneer im Enterprise Password Management

Password Safe dient Unternehmen als zentraler digitaler Tresor zur Sicherung, Verwaltung und Überwachung von sensiblen Daten wie Passwörtern, Dokumenten und Geheimnissen.

> **Im Umgang mit Passwörtern ist der Mensch noch unerlässlich.**
>
> **Unternehmen sind deshalb in der Pflicht, diesen Prozess so sicher wie möglich zu gestalten.**

Sascha Martens
Autor und CTO der MATESO GmbH

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Web: www.passwordsafe.de
Email: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE