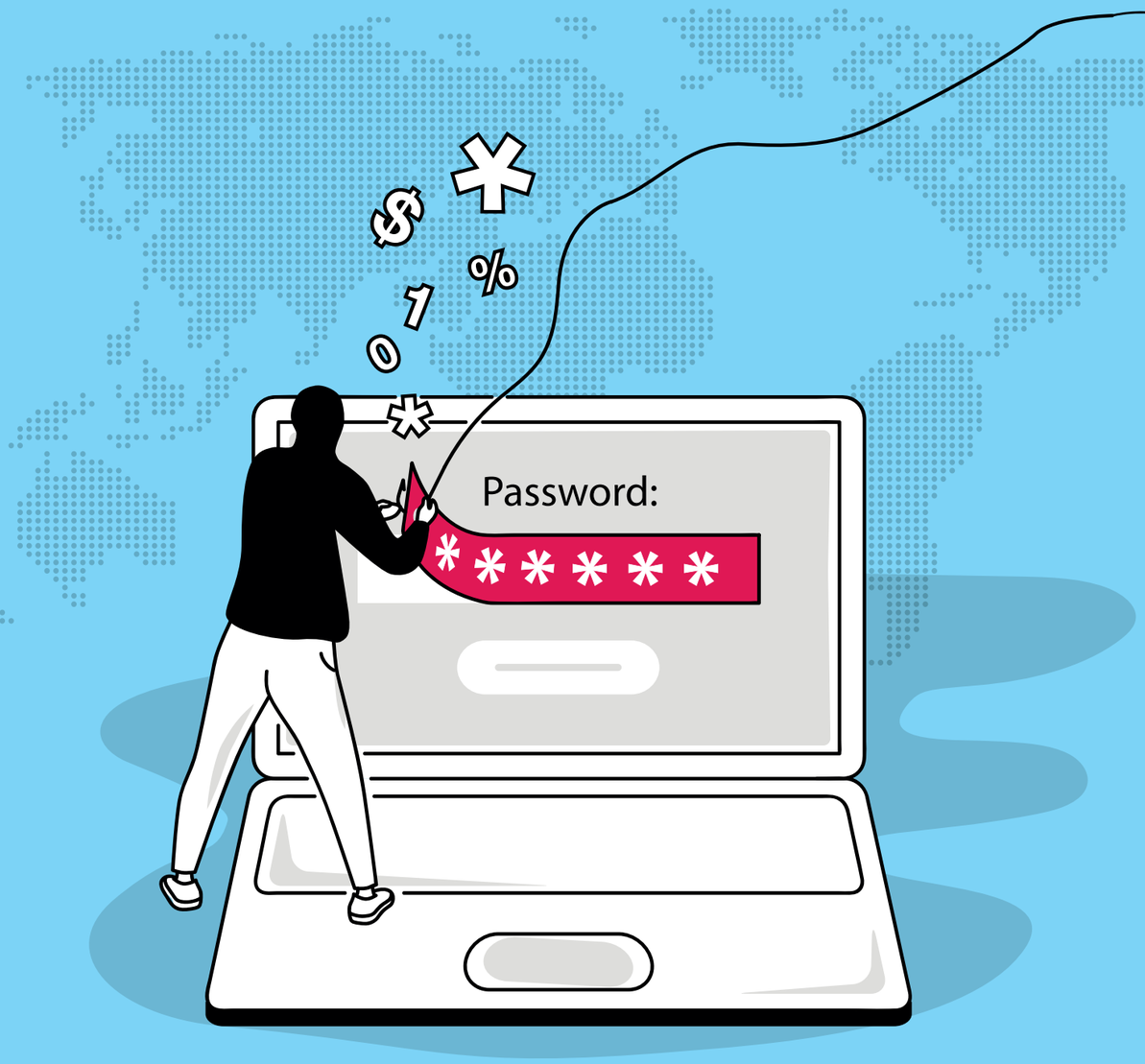
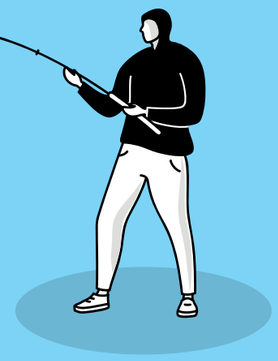
Wie erstelle ich eine Passwortrichtlinie?



Sichere Passwörter sind für den Schutz unserer IT-Systeme und vor allem der personenbezogenen Daten, die wir verarbeiten, von elementarer Bedeutung. Eine Passwort-Richtlinie bildet hierzu die Grundlage für Ihr Unternehmen und beschreibt verbindlich die Mindestanforderungen an die Qualität von Passwörtern und die Regeln im Umgang mit ihnen.



Eine Richtlinie allein wird nicht automatisch zu optimalen Passwörtern führen, denn nach wie vor sind wir Menschen die größte Schwachstelle. Damit ein Passwort als sicher gilt und eine Passwortrichtlinie effektiv eingeführt werden kann, sollten ein paar simple Regeln eingehalten werden.

Wir geben Ihnen drei Aspekte an die Hand, die in keiner Passwortrichtlinie fehlen sollten.

1 Rahmenbedingungen einer wirksamen Passwortrichtlinie festlegen

Mit diesen Tipps gelingt es Ihnen, einheitliche Rahmenbedingungen für Ihre Passwort-Richtlinie zu schaffen:

- Eine Passwort-Richtlinie sollte klar und verständlich für alle sein. Vermeiden Sie technische und juristische Fachsprache, damit alle Nutzer:innen Sie verstehen können.
- Veröffentlichen Sie die Passwort-Richtlinie im Mitarbeitendenhandbuch oder im Intranet, damit sie für alle leicht zugänglich ist.
- Stellen Sie sicher, dass die Passwort-Richtlinie immer auf bewährten Maßnahmen basiert, zum Beispiel auf der Verwendung eines Passwortmanagers oder der Zwei-Faktor-Authentifizierung.
- Richten Sie die Passwort-Richtlinie so ein, dass sie keine häufig wechselnden Passwörter oder Sicherheitsfragen erfordert.
- Die Passwortrichtlinie dient der IT-Abteilung als zentrale Möglichkeit, die Passwortsicherheit im Unternehmen zu verwalten und zu überwachen.
- Sollte sich die Bedrohunglage ändern, ist die IT-Abteilung die richtige Stelle, um die Passwort-Richtlinie zu aktualisieren.
- Eine Passwort-Richtlinie ist für alle da. Sie sollte deshalb regelmäßig den Mitarbeitenden in Schulungen nahegebracht werden.
- Achten Sie darauf, dass die Passwort-Richtlinie effektiv umgesetzt und vor allem regelmäßig überwacht wird. Änderungen gilt es gegebenenfalls einzuarbeiten.

2 Formale Anforderungen an Passwörter bestimmen

Wir alle wissen, wie schwierig es ist, sich immer wieder neue Passwörter für all die verschiedenen Dienste auszudenken, die wir heutzutage nutzen. Um Ihre Mitarbeitenden zu unterstützen, sollten ihnen folgende formale Anforderung vorgegeben werden:

- Je länger das Passwort ist, desto sicherer ist es: Geben Sie eine Mindestlänge von 8 Zeichen vor. Für WLAN wie zum Beispiel WPA2 oder WPA3 sollte das Passwort sogar 20 Zeichen haben.
- Für Passwörter können alle verfügbaren Zeichen genutzt werden: Groß- und Kleinschreibung, Ziffern und Sonderzeichen. Mindestens drei dieser vier Anforderungen müssen erfüllt sein, um das Passwort möglichst sicher zu machen.
- Ein vollständiges Passwort sollte nicht im Wörterbuch vorkommen, weil Hacker es relativ schnell durch einen sogenannten Wörterbuchangriff entschlüsseln können. Passwörter wie „password", „iloveyou" oder „admin" sind also tabu.
- Wenig originell und ebenso leicht von Hackern zu knacken sind gängige Zahlenfolgen (z.B. 123456789) oder Tastaturmuster (z.B. asdfgh). Auch hier gilt: Diese Passwörter werden besser nicht gewählt.
- Noch ein Klassiker: Namen von Familienmitgliedern, Haustieren, Freunden oder Geburtsdaten. Lassen Sie Ihre Mitarbeitenden wissen, dass das keine gute Wahl ist.
- Die Ergänzung von einfachen Ziffern oder Sonderzeichen nach einem „normalen Wort", also einem Wort aus dem Wörterbuch, ist ebenfalls nicht zu empfehlen. Jeder Mitarbeitende sollte wissen, dass zum Beispiel „admin!" kein sicheres Passwort ist.
- Um die Sicherheit zu erhöhen: Aktivieren Sie die Zwei-Faktor-Authentifizierung[1].
- Die gleiche Kombination von Benutzername und Passwort für verschiedene Dienste sollte nie verwendet werden! Die wichtigsten Passwörter sollten immer individuell und stark sein.

Generell sollten Sie auch den direkten Umgang mit Passwörtern in der Richtline deutlich machen und Ihre Mitarbeitenden durch Schulungen sensibilisieren:

- Geben Sie Passwörter nicht an Dritte weiter und versenden Sie sie nicht per E-Mail!
- Bewahren Sie Ihre Passwörter nicht in der Nähe Ihres Schreibtischs auf, falls Sie sie noch auf Papier festhalten.
- Ersetzen Sie voreingestellte Passwörter umgehend durch ein persönliches!

3 Technische Anforderungen für Ihre IT-Abteilung definieren

Ihre IT-Abteilung kann durch bestimmte Vorkehrungen dafür sorgen, dass der Missbrauch von Passwörtern zumindest erschwert, im besten Falle natürlich gar nicht erst ermöglicht wird. Durch folgende Maßnahmen setzen IT-Mitarbeitende die Standards, um unerwünschte Eingriffe zu vermeiden:

Änderungsintervall festlegen:

- Sollte der Verdacht bestehen, dass das Passwort unbefugten Dritten bekannt sein könnte, ist es zwingend sofort zu ändern!
- Zu Empfehlen ist das Festlegen einer Passwort-Historie[2]: Empfehlung: Die letzten zehn Passwörter sollten nicht wiederverwendet werden.
- **Anzahl falscher Anmeldeversuche festlegen:**
  1. Beispiel: Zehn Versuche bis zum Sperren der Kennung des Benutzers/der Benutzerin
  2. Beispiel: Fünf Versuche bis zum Sperren der Kennung des Benutzers/der Benutzerin + automatisches Entsperren durch das System/der Anwendung nach 30 Minuten
  3. Beispiel: Drei Versuche bis zum Sperren der Kennung des Benutzers/der Benutzerin + Freigabe durch ein Administratorpasswort
- Konfigurieren Sie ergänzend zur Passworthistorie ein minimales Passwortalter. Auf diese Weise wird vermieden, dass Benutzer ihre Passwörter in kurzer Zeit mehrmals ändern und sie dadurch versehentlich oder absichtlich alte Passwörter verwenden.

[1] Die Zwei-Faktor-Authentisierung gibt es in mehreren Varianten, einige ergänzen das zuvor eingegebene Passwort um einen zusätzlichen Faktor, andere ersetzen das vorherige Log-In mit Passwort komplett durch eine direkte Kombination zweier Faktoren. Dabei bieten vor allem hardwaregestützte Verfahren ein hohes Maß an Sicherheit und sollten ergänzend/ersetzend zu einem starken Passwort genutzt werden.

[2] Die Passworthistorie beinhaltet die letzten Passwörter. Der Benutzer/die Benutzerin kann diese so lange nicht wiederverwenden, bis diese nicht mehr in der Passworthistorie stehen.

NICE TO KNOW
Passwortmanager

Um die Akzeptanz der Mitarbeitenden für strikte Passwortregularien zu stärken, wird generell der Einsatz von Passwortmanagern empfohlen. Hierbei muss sich nur ein einziges Passwort, das Masterpasswort, gemerkt werden. Passwörter für verschiedene Dienste können durch den Passwortmanager generiert werden. Ebenfalls gibt es die Möglichkeit, sich die Sicherheitsstufe des Passworts auszusuchen, je nachdem, wie stark der Passwortschutz sein soll. Außerdem können die generierten Passwörter in dem Passwortmanager gespeichert werden.

Vorteile Einbindung Passwort-Manager:

- **Mittels Verschlüsselung werden Passwörter verwahrt**
- **Hilfe bei der Passwortvergabe:** z. B. durch die Generierung starker Kombinationen und Kennzeichnung schon verwendeter oder schwacher Begriffe.
- **Warnung vor gefährdeten Websites und möglichen Phishing-Attacken**, z. B. wenn sich die URL der aufgerufenen Webseite von der gespeicherten unterscheidet.
- **Synchronisieren möglich,** wenn Online-Dienste auf mehreren Geräten wie Computer und Smartphone mit unterschiedlichen Betriebssystemen genutzt werden.

Nachteile Einbindung Passwort-Manager:

- Beim Vergessen des Masterpassworts sind im schlechtesten Fall alle Daten verloren: Das bedeutet oftmals viel Arbeit, da die einzelnen Zugänge zu den Konten individuell wiederhergestellt werden müssen.
- Bei einem Cyber-Angriff auf den Passwort-Manager können alle Passwörter auf einmal gestohlen werden.
- Es sollten grundsätzlich die AGB und Datenschutzerklärungen geprüft werden, insbesondere bei cloudbasierten Diensten. Vor allem im Hinblick auf den Unternehmensstandort des Cloud-Dienst-Anbieters und den Standort des Servers, welcher zusätzlich Informationen darüber gibt, welchem Datenschutzrecht die Daten unterworfen sind.

Die Einführung einer einheitlichen Passwortrichtlinie, um die Sicherheit der IT-Systeme zu gewährleisten, ist für ein Unternehmen eine große Herausforderung. Mit den oben aufgeführten Aspekten und Empfehlungen wird Ihnen und Ihren Mitarbeitenden der Einstieg zur optimalen Umsetzung erleichtert. Nur das Zusammenspiel aus allen Aspekten stellt starke Passwörter und somit ein hohes Sicherheitsmaß in Ihrem Unternehmen sicher.

Die Angaben entsprechen den aktuellen Standards des BSI.

Über die Autorin Kim Kurzhals:
Kim Kurzhals ist seit Juli 2021 als Beraterin im Bereich Datenschutz bei der DATATREE AG angestellt. Zuvor absolvierte Sie ihr Masterstudium im Bereich Wirtschaftsrecht an der Westfälischen Hochschule. Durch Ihr fachliches Know-how gehören u.a. AV-Verträge zu ihrem Spezialgebiet.