# Verwendung und Änderung von Windows-Kennworten

Der richtige Umgang mit Zugangsdaten (insbesondere Passwörter) ist eine effektive Schutzmaßnahme, die alle betrifft. Daher sind Passwörter generell sicher zu gestalten. Das war schon immer wichtig, wird aber immer wichtiger. Bitte beachten Sie daher die unten stehenden Regeln, um ein sicheres Kennwort zur Anwendung zu bringen. Die Windows-Kennwörter werden in der ActiveDirectory (AD) verwaltet. Die AD unterstützt Sie auch bei der Erstellung eines sicheren Kennwortes und lehnt zu einfache Kennwörter ab.

Ihr Windows-Kennwort wird auch von Online Services, wie z.B. Office 365 oder Jira/Confluence bzw. Salesforce verwendet. Bei einer Änderung des Kennwortes wirkt sich dieses aber auch auf diese Dienste aus. Insbesondere Office 365 kann hier eine Hürde darstellen, wenn diese Produkte in Verbindung mit einem VPN-Tunnel (HomeOffice) verwendet werden. Es empfiehlt sich dann eines der beiden im Folgenden beschriebenen Verfahren zur Kennwort-Änderung:

A) Änderung des Passwortes ohne aktivem VPN-Tunnel, direkt im Netzwerk bzw. im Büro

B) Änderung des Passwortes mit aktivem VPN-Tunnel, z.B. im HomeOffice

**Hinweis zu Jira und Confluence:** Nach dem Passwortwechsel kann es sein, dass eine sofortige Anmeldung an Jira und Confluence nicht sofort klappt. Dann bitte noch einmal das alte Kennwort versuchen und am nächsten Tag mit dem neuen Kennwort starten. Diese beiden Systeme gleichen die Logindaten mehrfach am Tag mit der Active Directory, dem Speicherort der Windows-Anmeldedaten, ab. Es kann aber sein, das der nächste Abgleich erst in ein paar Stunden erfolgt. VPN, Office 365, das WLAN Portal und viele andere Anwendungen gleichen das nicht ab, sondern sind direkt verbunden, daher ist dort das neue Kennwort sofort aktiv.

## Regeln für sichere Kennwörter

Damit das Kennwort als sicher eingestuft werden kann, sind die folgenden Regeln bei der Einrichtung von Passwörtern einzuhalten:

- Das Passwort muss mindestens eine Länge von 12 Stellen aufweisen, laut BSI Empfehlung eher länger, also mind. 12 Zeichen.
- Die Passwörter müssen jeweils mindestens ein Zeichen der folgenden Zeichenklassen enthalten:
  - Großbuchstaben des lateinischen Alphabets
  - Kleinbuchstaben des lateinischen Alphabets
  - Ziffern
  - Sonderzeichen
- Ein Passwort darf nicht zwei aufeinanderfolgende Buchstaben des jeweiligen Benutzernamens (Initialen) enthalten.
- Passwörter müssen so gewählt werden, dass sie nicht erraten werden können. Unzulässig sind beispielsweise Namen oder Vornamen, Geburtsdaten oder Kfz-Nummernschilder, Telefonnummern oder vergleichbare Daten aus dem persönlichen Umfeld sowie Wörter, die üblicherweise in einem Wörterbuch (Sprach- oder Fachwörterbuch) zu finden sind. Triviale Passwörter sind unzulässig.
- Die vorgenannten Negativbeispiele dürfen auch dann nicht verwendet werden, wenn diese um Präfixe oder Suffixe ergänzt werden. Beispielsweise gilt das Passwort "geheim" auch dann noch als schwach, wenn man daraus "$Geheim12" macht: In diesem Beispiel wurde die obige Regel gebrochen, dass keine Begriffe aus einem Wörterbuch verwendet werden dürfen.

Für unterschiedliche Dienste und Programme sind, sofern möglich, unterschiedliche Zugangsdaten zu nutzen.

Passwörter zur Anmeldung am Arbeitsplatz oder an Systemen sind personenbezogen. Sie sind damit in keinem Fall an andere weiterzugeben. Dies gilt auch für eine etwaige Weitergabe an externe Dienstleister.

Notizzettel mit Passwörtern dürfen in keinem Fall an Monitoren, unter der Tastatur oder anderswo ohne angemessenen Zugriffsschutz angebracht oder aufbewahrt werden.

**Eine unverschlüsselte Speicherung von Passwörtern bzw. Zugangsdaten ist untersagt. Für die Speicherung sollte ein verschlüsselter Passwortmanager verwendet werden. Rückfragen hierzu beantwortet die IT-Abteilung.**

Bei der Eingabe von Passwörtern oder sonstigen Zugangsdaten ist darauf zu achten, dass kein Unbefugter Kenntnis darüber erlangen kann. Beispielsweise sollte sichergestellt werden, dass niemand das Eingabefeld einsehen kann (vergleichbar mit den üblicherweise für die Zahlung mit EC-Karte geltenden Sicherheitsvorkehrungen). Auf die Eingabe ist zu verzichten, solange die Einsichtnahme durch Unbefugte nicht ausgeschlossen werden kann.

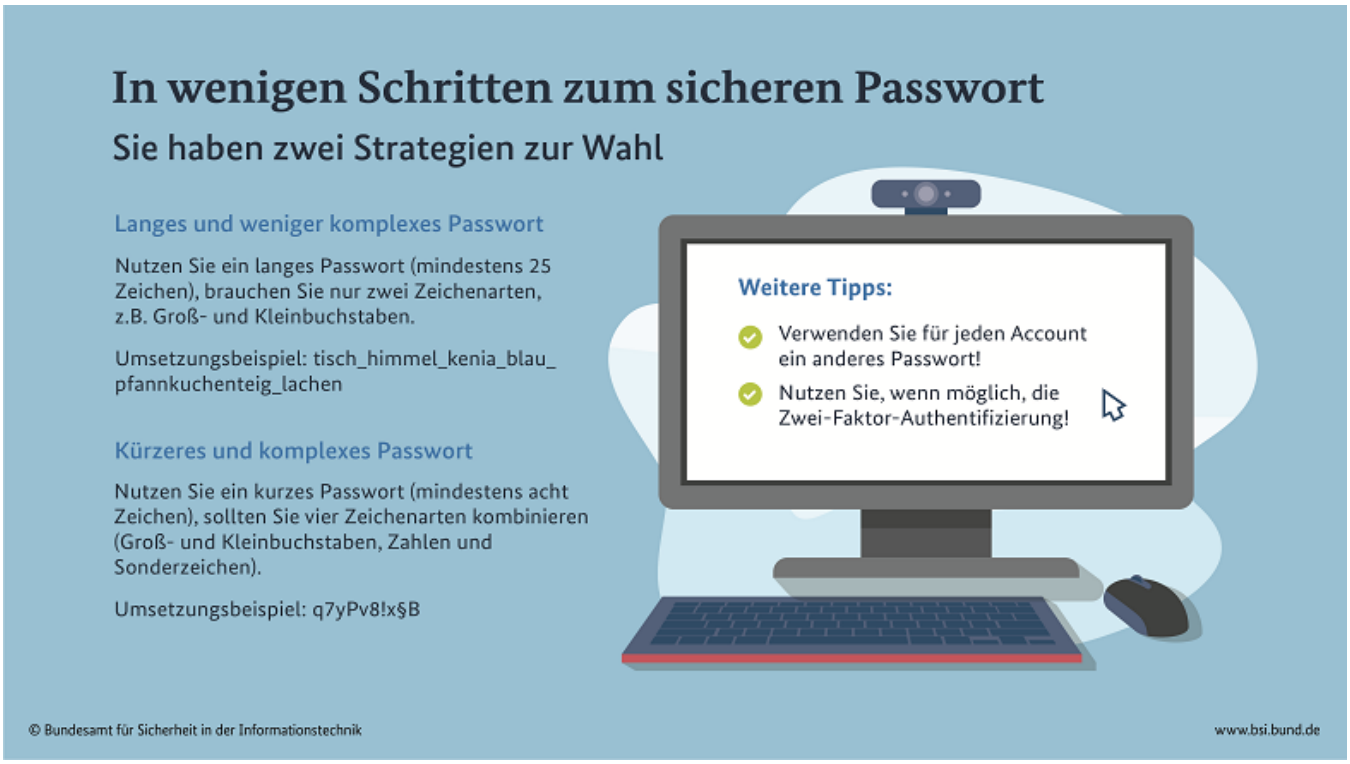
Für Anwendungen Dritter, die passwortgeschützt sind und von mehreren Mitarbeitern genutzt werden, ist ein Verantwortlicher zu benennen, der das Passwort ändert, wenn beispielsweise Dritte Kenntnis davon erlangt haben könnten. Die Organisation der Passwortvergabe obliegt den Abteilungsleitern, die hier in der Verantwortung stehen.

Bei der Vergabe von Initialpasswörtern für Mitarbeiter oder Kunden ist darauf zu achten, dass diese unverzüglich geändert werden. Browsereinstellungen sind so zu konfigurieren, dass Passwörter nicht unverschlüsselt gespeichert werden.

### Praxistipp zur Findung von sicheren Kennwörtern

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Empfehlung veröffentlicht, wie ein sicheres Passwort zu gestalten ist:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html




**ACHTUNG:** Nicht dieses Kennwort aus dem Beispiel verwenden! (Das haben viele schon gemacht 😞).

Alternativ kann ein Passwortgenerator verwendet werden.

**Hinweis:** Viele Dienste bieten bereits eine Multi-Faktor-Authentifizierung (MFA), oft auch Zwei-Faktor-Authentifizierung (2FA) genannt, an. Nach Möglichkeit ist diese zu verwenden. Ein Kennwort kann ein Angreifer ggf. erraten, Abfischen (Phishing), oder auch auf anderen Wegen bekommen. Den zweiten Faktor dann auch zu bekommen, ist deutlich aufwendiger. Daher wird der Angreifer bis auf Weiteres erstmal Accounts angreifen, die nicht ausreichend gesichert sind.

# Weitere Hinweise

## Verschiedene Portale/Systeme

Für unterschiedliche Services, Portal, etc. sind auch unterschiedliche Kennwörter zu verwenden. Ist ein Kennwort inkl. Login (z.B. E-Mail-Adresse) abhandengekommen, wird auch an andern Stellen versucht dieses zu verwenden. Daher ist ein generell unterschiedliches Kennwort wichtig. Nicht einfach nur eine Stelle im Kennwort ändern, das ist schnelle geraten.

## Weitergabe von Kennwörtern

Passwörter zur Anmeldung am Arbeitsplatz oder an Systemen, wie z. B. SAP, sind immer personenbezogen und werden nicht weitergegeben. Dies gilt auch für Dienstleister (auch MSP).