Landesamt für Sicherheit in
der Informationstechnik

LSI-Info A#03

UMGANG MIT PASSWÖRTERN

Version 1.01 vom: 04.03.2022

Management Summary

Passwörter sind das Vorhängeschloss für die Nutzung von IT-Services und für den Zugriff auf Daten. Entsprechend wichtig ist, dass Passwörter bereits getroffene Sicherheitsmaßnahmen flankieren und das erzielte Sicherheitsniveau nicht unterwandern. Neben den Anforderungen, die ein Passwort erfüllen sollte, um einen adäquaten Schutz der IT-Infrastruktur zu gewährleisten, ist auch der Umgang mit Passwörtern durch Mitarbeiter und Dienstleister ein wichtiger zu regelnder Faktor.

HINTERGRUND

Vor 2020 wurde dazu geraten die Passwörter regelmäßig in einem definierten Zeitintervall zu ändern, um so die Systemsicherheit zu erhöhen. Die Bedeutung der Komplexität eines Passworts stand dabei erst an zweiter Stelle. Dies führte dazu, dass die Passwörter möglichst einfach gehalten wurden. Seit Anfang 2020 wurde die Empfehlung Passwörter regelmäßig zu ändern auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) revidiert.
Der Komplexität von Passwörtern wird nun wesentlich mehr Bedeutung beigemessen, als einem Änderungszyklus. Tatsächlich können die Komplexitätsanforderungen mathematisch nachgewiesen werden. So ergibt ein Passwort aus 6 Zeichen mit einer Mischung aus Groß- und Kleinbuchstaben (52 mögliche Zeichen) eine mögliche Kombination von 19.770.609.664 unterschiedlichen Passwörtern (52 hoch 6). Teilt man dies durch die maximal pro Sekunde verglichenen Kennwörter, erhält man die Zeit, welche benötigt wird, um das Passwort herauszufinden. Oft werden beim Versuch das Passwort zu erhalten Brute-Force- (raten durch Kombinatorik) und Rainbow-Table-Attacken (Nutzung gängiger Passwortkombinationen) genutzt.

GENERELLE ANFORDERUNGEN AN DIE KOMPLEXITÄT VON PASSWÖRTERN

Es sollten daher unbedingt Mindestanforderungen für Passwörter definiert werden, die ein hohes Maß an Komplexität erreichen.
Ein Passwort sollte generell keine Rückschlüsse auf den Besitzer durch persönliche Daten (z.B. Geburtsdatum, Namen, KFZ-Kennzeichen, etc.) ermöglichen. Das Passwort sollte zudem kein Tastaturmuster (z.B. „qwertz“) enthalten und nicht in Wörterbüchern vorkommen.
Als Grundregel sollte ein Passwort aus verschiedenen Zeichenbereichen zusammengesetzt sein. Folgende Zeichenbereiche stehen dabei zur Verfügung:

- Großbuchstaben (A bis Z)
- Kleinbuchstaben (a bis z)
- Ziffern (0 bis 9)
- Sonderzeichen (z.B. !, $, -, %, @)

Gegebenenfalls müssen bei den Sonderzeichen, aufgrund einer speziellen Bedeutung eines Zeichens in einer Systemumgebung, Ausschlusskriterien definiert werden.

Generell sollte für externe Dienste jeweils ein eigenes Passwort verwendet werden. Dieses Verfahren empfiehlt sich auch intern für kritische Bereiche mit einem hohen Schutzbedarf.
Benutzername und Passwort (Credentials) sollten nicht zusammen und nicht über unverschlüsselte Kanäle versendet werden. Sollen Zugangsdaten bspw. über E-Mail versendet werden, empfiehlt sich der Versand von zwei verschlüsselten E-Mails. Steht eine E-Mail-Verschlüsselung nicht zur Verfügung, kann auf zwei Passwort-geschützte ZIP-Archive zurückgegriffen werden. Eine weitere Möglichkeit wäre unterschiedliche Kanäle für Zugangsdaten und Passwort zu verwenden. In Kombination mit einem Medienbruch ist dies ein sehr sicherer Übermittlungsweg. So könnte bspw. der Versand der Zugangskennung in einer verschlüsselten oder Passwort-geschützten E-Mail erfolgen und das Passwort in einem Brief mit geschwärztem Couvert übermittelt werden.

ANFORDERUNGEN AN DIE KOMPLEXITÄT VON PASSWÖRTERN BEI VERSCHIEDENEN BENUTZERGRUPPEN

Generell sollten sich die Komplexitätsanforderungen von Passwörtern an den benötigten Rechten auf den IT-Systemen und in den IT-Anwendungen orientieren – je mehr Rechte benötigt werden, desto komplexer sollte das Passwort sein.

Nutzer von IT-Systemen und IT-Anwendungen

Nutzer von IT-Systemen sollten ein Passwort haben, das neben den oben genannten Anforderungen mindestens 10 Zeichen lang ist und aus drei der vier Zeichenbereiche besteht.

Administratoren von IT-Systemen und IT-Anwendungen

Passwörter von Administrations-Accounts sollten ebenfalls, neben den oben genannten Anforderungen, mindestens 10 Zeichen lang aber aus allen vier Zeichenbereiche bestehen.

Passwörter sollten nicht über unverschlüsselte Kanäle übertragen bzw. für diese genutzt werden. Für die Administration bedeutet dies, dass bspw. keine ftp- und keine telnet-Verbindungen genutzt und angeboten werden sollten. Alternativen hierfür wäre die Verwendung von sftp- oder ssh-Verbindungen.

HILFSMÖGLICHKEITEN FÜR DIE KOMPLEXITÄTSANFORDERUNGEN VON PASSWÖRTERN

Komplexere Passwörter, wie „VX91N=%I@vh“, können sich Nutzer und Administratoren von IT-Systemen schwer merken. Eine Hilfe kann dabei, sofern technisch möglich, ein Passwort-Safe/-Manager sein. Dort können vom System vorgeschlagene komplexe Passwörter generiert und hinterlegt werden.
Sollte eine technische Unterstützung bei Generierung und Speicherung nicht möglich sein, kann unter Beachtung der bisherigen Anforderungen ein Merksatz, auch Passphrase genannt, verwendet werden. So könnte der Satz:
„Wir sind eine Gemeinde mit 750 Einwohnern und leben da, wo andere Urlaub machen!“ zum Passwort „WseGm750Euld,waUm!“ führen.

Sollten im Falle der Nutzung verschiedener externer Dienste mehrere Passwörter benötigt werden, so empfiehlt es sich, wie bereits erwähnt, für jeden Dienst ein eigenes Passwort zu wählen. Um dies praktikabel zu halten, könnte der Merksatz um den Dienst erweitert werden.
Für den externen Dienst „OK.EWO“ könnte dies unter Austausch von „O“ mit der „0“ und der Nutzung des erwähnten Merksatzes das Passwort „WseGm750Euld,0K.EW0,waUm!“ ergeben.

Hinweis: Die hier genannten Beispiel-Passwörter dürfen auf keinen Fall verwendet werden!

Wie bereits erwähnt können die Komplexitätsanforderungen mathematisch bewiesen werden. Bei einem nach diesen Empfehlungen zusammengestellten Passwort aus drei der vier oben genannten Zeichenbereiche eines Nutzers von IT-Systemen bräuchte ein leistungsstarker Rechner bis zu 12 Jahre, um alle möglichen Kombinationen zu generieren. Bei einem Administrator, der im Passwort neben den Groß- und Kleinbuchstaben, die Zahlen und 10 Sonderzeichen verwendet, bräuchte ein leistungsstarker Rechner bis zu 1808 Jahre.[1]
Wie zu sehen ist, sind die Faktoren Passwortlänge und Variation an Zeichen ein entscheidender Komplexitätsfaktor.

[1] Für diese Berechnung wird von den hier beschriebenen Keys/Sekunde ausgegangen: https://www.1pw.de/brute-force.php

AUSNAHMEN VON KOMPLEXITÄTSANFORDERUNGEN

Sollten technische Einschränkungen eine Abweichung von dieser Richtlinie erfordern, sollte dies mit dem Informationssicherheitsbeauftragten abgestimmt, dokumentiert und begründet werden. Der Informationssicherheitsbeauftragte kann auf dieser Basis eine Ausnahmegenehmigung erteilen. Diese Ausnahmegenehmigung sollte sich an der max. möglichen Komplexität von Passwörtern orientieren.

UMGANG MIT PASSWÖRTERN

Die Komplexitätsanforderungen allein garantieren nicht, dass ein Passwort nicht missbraucht werden kann. Neben den Anforderungen bei der Erstellung eines Passworts, ist auch der richtige Umgang damit entscheidend. Es sollten daher alle Bereiche des Lifecycles eines Passworts berücksichtigt werden. Vor allem sollte darauf geachtet werden, dass bei einer Kompromittierung dringend und unmittelbar reagiert wird.

Passwörter sollten nur dessen Besitzer bekannt sein und nicht mit anderen geteilt werden. Das Aufschreiben von Passwörtern sollte nur für Notfälle gestattet und das Medium in einem verschlossenen Umschlag in einem Tresor aufbewahrt werden.
Der Benutzer sollte bei der Eingabe von Passwörtern darauf achten, dass er von Niemandem beobachtet wird. Dazu zählen z.B. auch geteilte Bildschirme bei Videokonferenzen oder die Eingabe des Passworts während eines Bürgergesprächs.

Voreingestellte Initial- oder Standardpasswörter sind bei Erstnutzung der Anwendung unverzüglich, unter Beachtung der Komplexitätsanforderungen, durch ein neues Passwort zu ersetzen.
Im privaten Umfeld genutzte Passwörter dürfen dienstlich nicht verwendet werden. Dies gilt auch im umgekehrten Fall.

AUFBEWAHRUNG VON PASSWÖRTERN

Passwörter sollten verschlüsselt gespeichert und zugleich sicher vor dem Zugriff Dritter aufbewahrt werden. Dies kann entweder elektronisch in einem Passwort-Safe oder analog in einem Tresor geschehen.
Falls das Speichern von Passwörtern außerhalb eines Passwort-Safes notwendig sein sollte, muss das Passwort unbedingt verschlüsselt abgelegt werden (SALT/PEPPER gehasht).

Die unverschlüsselte Speicherung von Passwörtern in IT-Anwendungen oder im Dateisystem sollte nicht gestattet werden (betrifft auch mit eigenen Bordmitteln verschlüsselte Office-Dokumente). Die Speicherung in Webbrowsern sollte ebenfalls untersagt sein, da die Passwörter dort oft unverschlüsselt abgespeichert werden. Trotz möglicher verschlüsselter Speicherung der Passwörter im Webbrowser ist die Verschlüsselung schwach und kann umgangen und entschlüsselt werden. Zudem füllt der Browser beim Anmelden die Passwörter oft im Voraus aus. Es gibt einige Anwendungen mit denen die Verschlüsselung mittels Word-Bordmitteln oder in Webbrowsern aufgehoben werden kann.[2]
Die Speicherung von Passwörtern auf programmierbaren Funktionstasten von Tastatur und Maus sollte auch nicht gestattet werden.

KOMPROMITTIERUNG VON PASSWÖRTERN

Falls der Verdacht besteht, dass ein Passwort fremden Personen bekannt oder zugänglich geworden ist, sollte das Passwort sofort und unmittelbar an allen Systemen, an denen dieses verwendet wurde geändert werden. Dieser Vorfall sollte dem Informationssicherheitsbeauftragten und dem IT-Leiter bekannt gemacht werden. Falls technisch möglich, sollte eine Passwort-Änderung beim nächsten Login erzwungen werden.

ZURÜCKSETZTEN VON PASSWÖRTERN

Falls ein Passwort vergessen wurde, sollten geeignete Verfahren zum Zurücksetzen des Passworts vorgehalten werden. Es sollte dabei sichergestellt werden, dass der Nutzer zweifelsfrei authentifiziert wird, dass der Empfänger des neuen Initialpassworts zweifelsfrei der anfragende Nutzer ist und dass die Passwort-Übermittlung auf einem sicheren Kanal verschlüsselt erfolgt.
Beim Zurücksetzen der Passwörter sollten – soweit technisch realisierbar – Einmalkennwörter verwendet werden.

[2] Um ein paar Anwendungen zu nennen:
https://www.nirsoft.net/password_recovery_tools.html
https://www.elcomsoft.de/einpb.html
https://www.elcomsoft.de/aopr.html

SENSIBILISIEREN DER MITARBEITER IM UMGANG MIT PASSWÖRTERN

Der Umgang mit Passwörtern – auch im Kontext von Sicherheitsvorfällen – sollte fester Bestandteil der verpflichtend zu besuchenden Sensibilisierungskurse sein. In den regelmäßig stattfindenden Sensibilisierungskursen können Quizze oder Quizfragen gestellt oder auch bewiesene Fakten im Umgang mit Passwörtern dargelegt werden. Wichtig ist dabei der Hinweis, dass keine externen Webseiten mit Passwortchecks genutzt werden dürfen. Passwörter sollten, vor allem im Web, nur bei dem dafür vorgesehenen Dienst in die dafür bestimmten Felder eingegeben werden.

BETREIBER VON IT-SYSTEMEN

IT-Systeme können extern oder intern betrieben und betreut werden. Die Systembetreiber haben Sorge zu tragen, dass die Anforderungen einer zu definierenden Passwortrichtlinie in den jeweiligen IT-Systemen eingehalten werden. Die Komplexität der Passwörter für Fernzugänge sollte mindestens die gleiche Komplexität wie die der im betreuenden System besitzen. Es sollten auch technische Umsetzungsmöglichkeiten für die Komplexitätsanforderungen an die Passwörter für die jeweiligen IT-Systeme in Betracht gezogen werden (z.B. eine Default Domain Policy).

ACCOUNT-SPERREN

Um Passwortattacken in Form von Brute-Force- oder Rainbow-Table-Angriffen, vor allem bei Zugriffen über das Internet (bspw. VPN) frühzeitig zu unterbinden, sollte nach 5 Fehlversuchen pro Minute eine Account-Sperre und ein Abbruch der Verbindung erfolgen.
Generell sollte nach 5 Fehlversuchen pro Tag der Zugang für 30 Minuten temporär gesperrt werden. Erfolgen daraufhin weitere 3 Fehlversuche am gleichen Tag, wird der Account gesperrt.
Freischaltungen sollten nur unter Kenntnisnahme des Informationssicherheitsbeauftragten beim IT-Support erfolgen.

ZWEI-FAKTOR-AUTHENTIFIZIERUNG

Generell soll versucht werden, den Stand der Technik abzubilden und in diesem Kontext eine Zwei-Faktor-Authentifizierung (2FA) anzubieten. Diese nutzt neben dem Faktor Wissen (Kenntnis des Kennworts) noch den Faktor Besitz (physikalisch Chipkarte, Token oder Smartphone bzw. biometrisch Fingerabdruck oder Gesichtserkennung). 2FA geschieht vorzugsweise bei exponierten Systemen mit erhöhtem Schutzbedarf.

Ein Softzertifikat mit PIN-Schutz stellt keine 2FA dar. Im Vergleich zur Kombination Zugangskennung mit physikalischen oder biometrischen Besitztümern erfolgt die Speicherung der Zertifikate – auch für Dritte zugänglich - im Filesystem oder im Windows-Zertifikatsspeicher (analog der Zugangskennung). Die PIN (analog zum Passwort) kann ebenso unbemerkt kompromittiert werden. Obgleich ein Softzertifikat im Vergleich zu klassischen Login-Verfahren eine deutliche Verbesserung darstellt, wird empfohlen, sich beim Besitzfaktor an einem materiellen oder biometrischen Gegenstand zu orientieren.

Bei der Verwendung von biometrischen Daten ist dringend darauf zu achten, wie und wo diese vom System gespeichert werden. Biometrische Daten sollten vor dem Zugriff Dritter geschützt und nicht in der Cloud abgelegt werden. Vielmehr sollte auf eine verschlüsselte lokale Speicherung in speziellen Chips im Gerät geachtet werden.[3]

[3] Eine mögliche Problematik beim Umgang mit biometrischen Daten: https://www.security-insider.de/mehr-datenschutzklagen-zu-biometrischen-daten-bis-2025-a-1096725/?cmp=nl-15&uuid=b600a0567fbc66d3f47e58df39322d2a

PASSWORTRICHTLINIE

Es wird dringend empfohlen über eine Passwortrichtlinie den Umgang mit Kennwörtern explizit zu regeln und die Benutzer zu sensibilisieren. Die folgenden Aspekte sollen dabei als Orientierung dienen:

- Denken Sie beim Erstellen der Passwortrichtlinie an die Personengruppe, die diese Richtlinie im Arbeitsalltag an den jeweiligen IT-System (Nutzer von IT-Systemen, Administratoren usw.) umzusetzen hat.
- Erklären Sie die Hintergründe und das verwendete Fachjargon, sodass die Benutzer die Anforderungen verstehen, nachvollziehen und mittragen können.
- Versuchen Sie den Benutzer als Stütze in das Zentrum der IT-Sicherheitsmaßnahmen zu rücken (z.B. durch aktive Unterstützung bei der Einhaltung der Passwortrichtlinie).
- Schreiben Sie die Anweisungen „bestimmend“ aber auf keinen Fall im „Befehlston“.
- Heben Sie den Nutzen für die Informationssicherheit in Ihrer Behörde deutlich hervor.
- Ggf. sollte ein Geltungsbereich der Passwortrichtlinie festgehalten werden.
- Denken Sie daran, die Passwortrichtlinie auch externen Betreibern von IT-Systemen oder externen Dienstleistern bekannt und verpflichtend zu machen.
- Definieren sie klare Zuständigkeiten, Prozesse und Verfahren. Nehmen Sie Kontaktangaben in die Passwortrichtlinie auf.
- Machen Sie die Richtlinie für jeden Mitarbeiter zugänglich (z.B. im Intranet oder im Dateisystem, ggf. auch auf Papier).
- Weisen Sie auf die Gefahren von Online-Passwortchecks hin.
- Sperrcodes (nicht Kennwörter) von mobilen Geräten wie Smartphones und Tablets sollten separat geregelt werden.

Ein Template für eine Passwortrichtlinie kann beim LSI angefordert werden.

QUELLEN UND WEITERE INFORMATIONEN

- BSI IT-Grundschutz: Baustein ORP.4: Identitäts- und Berechtigungsmanagement
- BSI-Artikel: „Sichere Passwörter erstellen“ und „Umgang mit Passwörtern“
- BayIT-SiR 13 (nur im Behördennetz abrufbar): https://bayernrecht.beck.de/Dokument?vpath=bibdata%2Fges%2FBAYVV_2003_4_F_988_217%2Fcont%2FBAYVV_2003_4_F_988_217.ANRNR5.htm
- LSI-Info T#06a (v1.0): Windows Domänen Teil 1: https://www.lsi.bayern.de/mam/aktuelles/lsi-info_t06a_domaenenadministratoren.pdf

KONTAKT

Weitere Informationen finden Sie unter:

https://lsi.bayern.de/kommunen/

Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:

Beratung-Kommunen@lsi.bayern.de.

Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911 21549-523 für Sie erreichbar.