Cyber-Sicherheitsrat Deutschland e.V.

Werkzeugkasten Cybersicherheit

Passwortmanagement

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen**, **unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

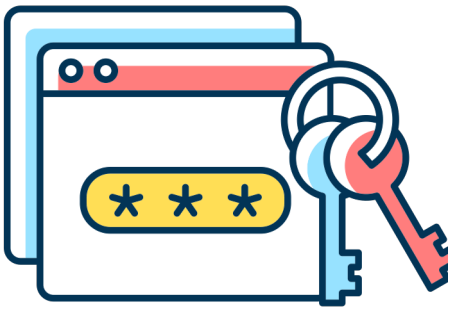
Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.
Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

Passwortmanagement – Was ist das?

Passwortmanagement ist ein essenzieller Aspekt der Informationssicherheit in Unternehmen und Institutionen. Es bezeichnet den Prozess, durch den **Passwörter erstellt, gespeichert, verteilt und aktualisiert** werden, um den unautorisierten Zugang und Zugriff auf **schützenswerte Informationen** und IT-Systeme zu verhindern und zu steuern.
Das Passwortmanagement umfasst **Richtlinien, Verfahren und Technologien**, die dazu beitragen, die Vertraulichkeit von Passwörtern sowie deren ausreichende Passwortstärke zu gewährleisten.



Welche Maßnahmen sind erforderlich?

Um ein effektives Passwortmanagement einzuführen, sollten Unternehmen und Institutionen zunächst eine **Bedarfsanalyse** durchführen. Dies beinhaltet die Evaluierung der aktuellen Sicherheitsanforderungen, Richtlinien und Praktiken, um den Bedarf in der Organisation zu bestimmen. Basierend auf der Bedarfsanalyse kann anschließend das passende **Passwortmanagementsystem** ausgewählt werden

Als nächster Schritt sollten klar definierte **Passwortrichtlinien** entwickelt werden, die die Passworterstellung, -speicherung, -änderung und -wiederherstellung betreffen. Sie beinhalten Regeln zur Komplexität, Länge und Gültigkeitsdauer von Passwörtern. Dabei gilt die Grundregel: je länger ein Passwort ist, desto sicherer ist es und kann so die Wahrscheinlichkeit ein Passwort durch Ausprobieren zu erraten (sogn. Brute-Force-Angriff) erheblich verringern.

Ein sicheres Passwort soll nach Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) **mindestens 12 Zeichen** lang sein, und **Sonderzeichen, Zahlen sowie Groß- und Kleinbuchstaben** enthalten. Um ein sicheres Passwort zu generieren, empfiehlt sich die Anwendung der **Merksatzregel**, bei der das Passwort aus den Anfangsbuchstaben und Sonderzeichen eines Satzes gebildet wird. Für den letzten Satz wäre dieses z.B. das Passwort:

UesPzg,esdAdM,bddPadAuSeSgw.

Solche sicheren Passwörter sollen dann, nach Auffassung des BSI, nur noch geändert werden, wenn der Verdacht besteht, dass es unberechtigten Personen bekannt geworden ist. Ferner ist empfehlenswert, einen **Passworttresor** wie die Software Keepass zu nutzen, in dem man Passwörter automatisch generieren und sicher speichern kann.

Um sicherzustellen, dass alle Mitarbeiter die Bedeutung von Passwortsicherheit verstehen und die festgelegten Richtlinien befolgen, sind Schulungen und **Sensibilisierungskampagnen** unerlässlich. Nur mit dem Beitrag aller Beteiligten kann ein umfassendes Sicherheitskonzept langfristig umgesetzt werden. Darum ist es wichtig, Unternehmensangehörige für die Bedeutung von Passwortsicherheit sowie den korrekten Umgang mit Passwörtern zu sensibilisieren. Ferner sollen sichere Passwörter wenn möglich bereits durch die IT-Systeme selbst über **technische Passwortrichtlinien** erzwungen werden.

Nach der Implementierung des ausgewählten Passwortmanagementsystems ist es wichtig, dessen Nutzung durch alle Benutzer sicherzustellen. Durch regelmäßige Überwachung und **Prüfung der Passwortpraktiken** und -sicherheit in der Organisation können potenzielle Schwachstellen aufgedeckt und Verbesserungen vorgenommen werden. Hierzu helfen Passwort-Audits, die mit Hilfe von Tools durchgeführt werden können.

Um die Zugangssicherheit zu IT-Systemen weiter zu erhöhen, ist die Implementierung der **Zwei-Faktor-Authentifizierung** (2FA) zu empfehlen. Bei der 2FA muss zusätzlich zum Passwort ein weiteres Authentisierungsmerkmal, z. B. ein Einmalcode, zur Anmeldung an ein System eingegeben werden.

Schließlich sollte das Passwortmanagement **kontinuierlich angepasst** werden, um auf neue Sicherheitsbedrohungen oder Compliance-Anforderungen zu reagieren und die Effektivität des Systems aufrechtzuerhalten. Dieser Prozess der ständigen Verbesserung trägt dazu bei, das Sicherheitsniveau in der Organisation dauerhaft hoch zu halten.

Welche Chancen gibt es?

Ein effektives Passwortmanagement bietet Unternehmen und Institutionen zahlreiche Vorteile. Durch die Verwendung starker Passwörter und Richtlinien wird das **Risiko von Cyberangriffen** und **unbefugtem Zugriff** auf sensible Informationen und Systeme erheblich verringert. Viele **Cyberversicherungen** verlangen mittlerweile zusätzlich die 2FA, um überhaupt ein Unternehmen auf Cyberrisiken zu versichern. Dieses zeigt die zentrale Bedeutung der Verwendung sicherer Passwörter zur Steigerung der Informationssicherheit.

Welche Risiken gibt es?

Trotz der vielen Vorteile können auch einige Risiken und Nachteile im Zusammenhang mit Passwortmanagement auftreten. Mitarbeiter können Passwortrichtlinien als zu **restriktiv oder lästig** empfinden, was zu Widerstand oder schlechter **Einhaltung der Richtlinien** führt. Die **Verwaltung von Passwörtern** kann insbesondere bei großen Organisationen komplex und zeitaufwendig sein. Passworttresore können anfällig für Angriffe oder **Sicherheitslücken** sein, die von Cyberkriminellen ausgenutzt werden können.

Wem nutzt ein Passwortmanagement?

Der Adressatenkreis von Maßnahmen zum Passwortmanagement umfasst im Wesentlichen alle Personen, die innerhalb eines Unternehmens oder einer Institution mit sensiblen Informationen oder Systemen in Berührung kommen. Dies schließt **Mitarbeiter auf allen Ebenen, IT-Administratoren, Führungskräfte, externe Dienstleister und sogar Kunden** oder Endbenutzer mit ein.

Fazit

Passwortmanagement ist ein weithin unterschätztes Gebiet in der Kultur vieler Organisationen, bildet jedoch einen **Grundpfeiler** für eine sichere Nutzung von Konten und Systemen. Zur Absicherung der IT-Infrastruktur sollten dazu **organisatorische und technische Maßnahmen** ergriffen werden, um die Integrität der Daten und dadurch der Organisation zu gewährleisten.