Passwortrichtlinie für KMU

Die Sicherheit von Computer-Systemen und -Netzwerken hängt entscheidend vom korrekten Umgang mit Passwörtern ab. Eine implementierte Passwortrichtlinie, oder eben PW-Policy regelt im Unternehmen die Erstellung, Aufbewahrung und Verwendung von Passwörtern.

Wichtigste Merkpunkte:

- Erstellen Sie eine Übersicht über sämtliche passwortgeschützten System- und Anwendungszugänge in Ihrem Unternehmen.
- Legen Sie für alle identifizierten System- und Anwendungszugriffe in einer PW-Policy die Anforderungen an die Erstellung, Aufbewahrung und Verwendung der Passwörter fest.
- Prüfen Sie periodisch die strikte Einhaltung der PW-Policy.
- Sensibilisieren Sie alle Mitarbeitenden für die Gefahren durch unsachgemässen Umgang mit Passwörtern.

Warum braucht es eine PW-Policy?

Die Kombination von Benutzername und Passwort ist noch immer die meistverwendete Methode der Authentisierung und Autorisierung im digitalen Arbeitsumfeld. Damit werden etwa beim Zugang zu Netzwerken, bei der Anmeldung an Computer-Systemen oder bei der Nutzung von Diensten und Anwendungen die Identität der Benutzer festgestellt und der Zugriffschutz implementiert. Benutzernamen und Passwörtern kommt dadurch eine zentrale Rolle für die Cybersicherheit zu.

Da erstaunt es nicht, dass Cyberkriminelle Vieles daransetzen, um mittels Hacking, Phishing oder Social Engineering an diese wertvolle Information heranzukommen und damit die digitale Identität der betroffenen Person zu übernehmen.

Der Umgang mit Passwörtern ist Benutzern heute jedoch so vertraut, dass sie sich oft der damit verbundenen Gefahren zu wenig bewusst sind. Gerade im Unternehmensumfeld ist daher eine klare PW-Policy, welche die Benutzer genau anleitet und vor Fehlern in diesem Zusammenhang bewahrt, unerlässlich.

Was ist eine PW-Policy und wie erstellt man eine wirksame PW-Policy?

Unter einer PW-Policy versteht man ein Regelwerk, das die Cybersicherheit erhöhen soll, indem es die Mitarbeitenden dazu anhält, sichere Kennwörter zu erstellen, diese sorgsam aufzubewahren und ordnungsgemäss zu verwenden. Die PW-Policy ist Teil der offiziellen Regeln einer Organisation und sollte in die Schulung zum Sicherheitsbewusstsein (Awareness-Programm) aufgenommen werden.

Die PW-Policy soll massgeschneidert auf die Bedürfnisse (komplette Systemlandschaft) und Anforderungen (Sicherheitslevel) der betreffenden Organisation ausgelegt werden, um mit angemessenem Aufwand eine optimale Wirkung zu entfalten. In einem ersten Schritt muss daher eine Übersicht über sämtliche passwortgeschützten System- und Anwendungszugänge im Unternehmen erstellt werden sowie eine Abschätzung des erforderlichen Schutzlevels erfolgen. Alle so identifizierten Zugänge werden danach in der PW-Policy mit entsprechenden Regelungen berücksichtigt.

Um der sich stetig ändernden Bedrohungslage begegnen zu können, muss die Aktualität und Wirksamkeit der PW-Policy periodisch überprüft werden.

Welches sind die wichtigsten Punkte der PW-Policy?

Die PW-Policy regelt umfassend den Umgang mit Passwörtern in der Unternehmung. Den Benutzern liefert sie konkrete Handlungsanweisungen und macht Aussagen zu folgenden Punkten:

1. Verwendung von Passwörtern

Wie oben erwähnt ist die Kenntnis eines Passworts häufig bereits ausreichend, um die digitale Identität einer Person vollständig zu übernehmen. Generell sind deshalb alle Vorkehrungen zu treffen, welche eine missbräuchliche Verwendung dieser Information verhindern.

Passwörter sind somit strikt persönlich und unterliegen der Geheimhaltung. Insbesondere gilt es folgende Punkte zu beachten:

1. Passwörter dürfen weder aktiv weitergegeben oder geteilt, noch offen zugänglich abgelegt werden.
2. Ablage und Übertragung von Passwörtern müssen stets verschlüsselt erfolgen.
3. Bei der Eingabe von Passwörtern ist darauf zu achten, dass der Vorgang nicht durch Dritte einsehbar erfolgt.

Die PW-Policy legt die Richtlinien zur Verwendung von Passwörtern im Sinne einer Weisung fest.

2. Passwortstärke

Die Passwortstärke ist ein Mass für die Schwierigkeit eines Angreifers, ein ihm nicht bekanntes Passwort durch blosses Erraten oder Ausprobieren zu ermitteln. Je unvorhersehbarer, komplexer und länger ein Passwort gewählt wird, desto stärker und damit sicherer ist es.

Eine gute PW-Policy legt Wert auf die Erstellung von starken Kennwörtern, indem es die Benutzer anhält, ihre Passwörter länger und unvorhersehbar zu machen (Anleitung «Sichere Passwörter» (http://www.ebas.ch/step4#passwords)).

Zudem sollte die Erstellung von starken Passwörtern durch technische Hilfsmittel, wie z.B. der Zurverfügungstellung eines Passwortmanagers (http://www.ebas.ch/step4#passwords) unterstützt und in der PW-Policy geregelt werden.

3. Ablauf von Passwörtern

Passwörter können einfach übertragen werden. Dadurch können sie im Laufe der Zeit auch in falsche Hände geraten. Z.B. geben Mitarbeitende gelegentlich Passwörter unüberlegt an Dritte weiter oder notieren solche an ungeschützten Orten. Es können sich aber auch Datenpannen ereignen, bei denen Passwörter von Nutzern ungewollt offengelegt werden. Ein Rückruf von einmal abgeflossener Information ist grundsätzlich nicht möglich.

In solchen Fällen stellt das Ändern von Passwörtern die einzige wirksame Massnahme zur Wiederherstellung der Cybersicherheit dar, da die abgeflossene Information dadurch unbrauchbar wird.

Die Erneuerung und Verwaltung von Passwörtern sollte durch technische Hilfsmittel, wie z.B. der Zurverfügungstellung eines Passwortmanagers unterstützt und in der PW-Policy geregelt werden.

4. Passwort-Historie

Benutzer tendieren oft dazu, die Anzahl der zu merkenden Passwörter zu reduzieren, z.B. indem sie früher schon gebrauchte Passwörter wiederverwenden. Cyberkriminelle machen sich dieses Verhalten zu Nutze, indem sie bei ihren Angriffen regelmässig auch Listen mit alten Passwörtern einsetzen. Um dies zu vermeiden, sollten Benutzer

daran gehindert werden, alte Passwörter zu reaktivieren.

Die PW-Policy sorgt dafür, dass die Systeme eine Passwort-Historie der Benutzer führen und bei Passwortwechseln eine Überprüfung auf Wiederverwendung stattfindet.

5. Passwortänderung
Benutzern sollte es möglich sein, ihre Passwörter jederzeit und selbständig zu ändern. Hierbei muss jedoch sichergestellt sein, dass Passwortänderungen ausschliesslich vom legitimierten Eigentümer und nicht etwa von einem Angreifer veranlasst werden.

Die PW-Policy legt die technischen und organisatorischen Rahmenbedingungen fest, welche eine sichere Passwortänderung ermöglichen. So kann z.B. die Einführung einer Zwei-Faktor-Authentifizierung den Prozess der Passwortänderung wesentlich sicherer machen.

Passwörter sind nach wie vor die meistverwendeten Sicherheitselemente beim Zugriffsschutz im digitalen Umfeld. Da erstaunt es nicht, dass Cyberkriminelle Vieles daransetzen, um mittels Hacking, Phishing oder Social Engineering an die begehrte Information heranzukommen.

Eine Passwortrichtlinie (PW-Policy) sorgt für Klarheit und Sicherheit im Umgang mit Passwörtern!