Was sind Vor- und Nachteile einer SSO-Lösung im Vergleich zu einem Passwortmanager?

Tolleiv Nietsch - 2024-09-08 - Fragen zum Produkt

In der digitalen Welt sind Datensicherheit und Cybersecurity wichtiger denn je. Die steigende Anzahl von Cyberangriffen macht es unabdingbar, die private und geschäftliche Online-Identität zu schützen. Eine der wichtigsten Maßnahmen hierbei ist das Verwenden sicherer Passwörter. Allerdings ist es oft schwierig, sich an viele verschiedene Passwörter zu erinnern und sie regelmäßig zu ändern. Zudem ist es aus der Perspektive von Unternehmen kaum möglich, die Passwortsicherheit aller Mitarbeitenden zu überprüfen und zu gewährleisten. Um sicherzustellen, dass sichere und verschiedene Passwörter verwendet werden gibt es diverse Tools am Markt, vor allem Passwort-Manager und Single Sign-On Lösungen. Im Nachfolgenden betrachten wir diese Lösungen im Detail und zeigen auf, welche Wahl die beste ist, um sichere Login-Prozesse zu gewährleisten.

Funktionsweise, Vorteile und Herausforderungen beim Einsatz eines Passwort-Manager Tools

Passwort-Manager sind digitale Tools, die es dem Nutzer ermöglichen, alle Passwörter an einem sicheren Ort zu speichern. Die Funktionsweise eines Passwort-Managers ist relativ einfach, der Nutzer muss lediglich ein Masterpasswort für den Manager festlegen und alle anderen Passwörter für die verschiedenen Konten und Anwendungen, welcher er im beruflichen Alltag benötigt, hinzufügen. Anschließend kann er sich mit den unterschiedlichen gespeicherten Passwörtern bei all seinen Anwendungen anmelden, ohne sich jedes Mal das Passwort merken zu müssen.

Passwort-Manager sind ein praktisches Tool und bieten eine Reihe von Vorteilen für Nutzer:

• **Höhere Sicherheit der Passwörter:** Die Verwendung von sicheren und einzigartigen Passwörtern für alle Konten und Anwendungen ist ein wichtiger Teil der Cybersicherheit. Mit einem Passwort-Manager kann sichergestellt werden, dass alle Passwörter bestimmte Kriterien erfüllen und verhindert, dass Mitarbeitende aus Komplexitätsgründen einfache Passwörter mehrfach verwenden.

• **Zeitersparnis & Benutzerfreundlichkeit:** Der Nutzer muss sich nicht länger an jedes Passwort einzeln erinnern und es eintippen. Außerdem gibt es eine zentrale Anlaufstelle zur Verwaltung all seiner Passwörter. Passwörter können schnell und einfach hinzugefügt, geändert oder gelöscht werden.

Trotz all dieser Vorteile gibt es natürlich auch einige Nachteile, die berücksichtigt werden sollten, wenn die (alleinige) Verwendung eines Passwort-Managers (als Absicherung) für Unternehmen in Betracht gezogen wird:

• **Ungenügende Sicherheit:** Trotz eines grundsätzlich steigenden Sicherheitsniveaus durch einzigartige und sichere Passwörter anstelle von unsicheren und geteilten, ist ein einfacher Login über Benutzername und Passwort nicht mehr ausreichend. Passwörter ohne zusätzliche Mehr-Faktor-Authentifizierung bleiben weiterhin eine riskante Schwachstelle – zusätzliche MFA für jeden Login kann zwar individuell eingerichtet werden, revidiert dann aber jegliche Benutzerfreundlichkeitsvorteile durch erhöhte Komplexität.

• **Fehlende Transparenz:** Unternehmen können Ihren Mitarbeitenden einen Passwort-Manager einrichten und die Anweisung geben, diesen für alle nötigen Anwendungen zu verwenden. Einige Anbieter für Unternehmen ermöglichen außerdem die Vorgabe von Passwortrichtlinien und die Überwachung der Passwortverwaltung. Nichtsdestotrotz reicht ein einfacher Passwort-Manager nicht aus, das Verhalten der Mitarbeitenden und sicherheitsrelevante Aktivitäten zu monitoren.

• **Anfälligkeit für Phishing:** Verwalten Mitarbeitende ihre Passwörter individuell über den Passwort-Manager besteht auch weiterhin eine erhöhte Gefahr für erfolgreiche Phishing-Versuche. Wenn Mitarbeitende eine Vielzahl an Accounts pflegen und ihre Passwörter regelmäßig aus Sicherheitsgründen aktualisieren müssen, können sie schnell auf gezielte Fake-Mails reinfallen, welche sich zum Beispiel fälschlicherweise als Passwortaktualisierungserinnerungen mit direktem Link einer Anwendung ausgeben.

• **Abhängigkeit von einem einzigen Anbieter:** Der Nutzer muss sich auf den Anbieter des Passwort-Managers verlassen, um Zugang zu all seinen Passwörtern zu haben. Außerdem gibt es wie bei jeder Technologie auch bei Passwort-Managern immer ein gewisses Risiko. Es ist wichtig, sorgfältig zu prüfen, ob ein bestimmter Anbieter sicher ist und ob er regelmäßig Sicherheitsupdates bereitstellt.

Funktionsweise, Vorteile und Herausforderungen beim Einsatz einer Single Sign-On (SSO) Lösung

Single Sign-On (SSO) Lösungen sind Authentifizierungsdienste, die es dem Benutzer ermöglichen, sich mit einem einzigen Konto bei mehreren Anwendungen anzumelden. Die Funktionsweise von SSO ist auf maximale Benutzerfreundlichkeit und Sicherheit ausgelegt. Der Nutzer bzw. Mitarbeitende muss sich nur einmal registrieren bzw. von der IT angelegt werden und ein Passwort erstellen, um Zugang zu allen Anwendungen zu erhalten, die Teil des SSO-Systems sind. Diese Anmeldung gilt dann bei jeder Anwendung, welche die Mitarbeitenden im beruflichen Alltag benötigen und Teil des SSO-Systems sind, ohne dass der Benutzer jedes Mal ein neues Passwort eingeben muss.

Der Einsatz einer SSO-Lösung als Teil der Cybersecurity-Strategie bietet eine Vielzahl an Vorteilen für Unternehmen:

• **Sichere Login-Prozesse:** Da der Nutzer nur ein Passwort verwenden muss, um auf mehrere Anwendungen zuzugreifen, kann hier ein hochsicheres Passwort gewählt werden nach vorgegeben Sicherheitskriterien. SSO-Lösungen bieten häufig integrierte Mehr-Faktor-Authentifizierung, welche vom Unternehmen verpflichtet vorgegeben werden kann und je nach Verfahren maximale Sicherheit des Login-Prozesses bietet.

• **Benutzerfreundlichkeit:** Die Mitarbeitenden benötigen nur einen, sicheren Login für alle Anwendungen anstatt einer Vielzahl von Anmeldungen. Sie können dadurch effizienter arbeiten und haben allgemein eine bessere Benutzererfahrung.

• **Zentralisierte Verwaltung:** SSO ermöglicht es Unternehmen, alle Anmeldungen von Mitarbeitenden zentral zu verwalten und zu überwachen. Somit können alle nötigen Zugriffsberechtigungen an einer Stelle eingerichtet, erfasst und geändert werden. Außerdem wird die Verantwortung über die Zugriffsverwaltung ehemals über mehrere Passwörter an die verwaltende Abteilung übergeben – Mitarbeitende werden somit entlastet und weniger anfällig für Phishing-Versuche, welche Passwortänderungen oder ähnliches vortäuschen.

• **Transparenz und Kontrolle:** Durch die zentrale Benutzeroberfläche entsteht ebenso eine bessere Übersicht über alle Mitarbeitenden, Anwendungen, Zugriffsberechtigungen und Anmeldeaktivitäten. Zudem werden Auffälligkeiten, wie z.B. eine erhöhte Zahl gescheiterter Login-Versuche, als Indiz eines potenziell versuchten Passwortknackens, direkt erkannt und können mit erforderlichen Maßnahmen abgewehrt werden.

Trotz all dieser Vorteile gibt es auch beim Einsatz einer SSO-Lösung Bedenken, welche dagegensprechen können:

• **Abhängigkeit von einem einzigen Anbieter:** Unternehmen befürchten, dass sie zu abhängig von einem einzelnen Anbieter für alle Login-Prozesse werden. Die Einrichtung mit allen Anwendungen und Zugriffsberechtigungen erfordert zudem Zeit und es besteht die Sorge, zu viel Aufwand mit einem potenziell gewünschtem Anbieterwechsel zu haben.

• **Integration:** Um die Vorteile von SSO zu nutzen, müssen die benötigten Anwendungen zunächst an den SSO-Dienst angebunden werden. Bei einer Vielzahl von Anwendungen scheint dies zunächst ein enorm hoher Aufwand zu sein, hinzu kommt die Einrichtung des vollständigen Nutzerverzeichnisses inklusive Rollen und Rechtestruktur.

• **Kosten:** Es gibt verschiedene Anbieter am Markt mit sehr unterschiedlichen Kostenstrukturen. Teilweise sind die Preismodelle je nach Anbieter vor allem für kleinere und mittelständige Unternehmen nicht tragbar, um eine solche Lösung einzuführen.

Die passende SSO-Lösung

Die Bedenken beim Einsatz einer Single Sign-On Lösung lassen sich mit dem richtigen Anbieter auflösen. Unsere Cloud SSO-Lösung Bare.ID nutzt das etablierte Open Source IAM Framework Keycloak im Kern, was bedeutet, dass es keinen Vendor Lock-In gibt und man

jederzeit zu einem anderen Anbieter wechseln kann, ohne alles neu aufsetzen zu müssen. Außerdem ist die Lösung durch georedundantes Hosting hochverfügbar und entwickelt nach höchsten Compliance und Sicherheitsstandards, so dass die Sicherheit der Kundendaten immer gewährleistet ist. Die Tarife von Bare.ID, welche alle höchste Compliance- und Sicherheitsstandards sowie integrierte hochsichere Mehr-Faktor-Authentifizierung als proaktive Maßnahme zum Schutz vor erfolgreichen Cyberangriffen gewährleisten, sind dennoch auch für KMUs tragbar. Zudem gilt es hier zu kalkulieren, was die Folgen von erfolgreichen Cyberangriffen für Kosten und Reputationsschäden mit sich bringen würden – eine Investition in die Cybersicherheit zahlt sich somit nachhaltig aus. Da Bare.ID eine SaaS-Lösung ist, sind Integration und Setup einfach und benutzerfreundlich und nach einmaligem Aufsetzen mit keinem Aufwand mehr für Unternehmen verbunden. Außerdem sind alle nötigen Anwendungen bereits vorkonfiguriert verfügbar und können mit wenigen Klicks eingerichtet werden.

Beide Lösungen sind ein guter Schritt in die richtige Richtung

Zusammenfassend lässt sich sagen, dass sowohl Passwort-Manager als auch Single Sign-On Lösungen eine Verbesserung der Login-Security hervorrufen, denn beide Optionen bieten einen besseren Schutz gegenüber unkontrollierten und unsicheren Passwörtern. Während Passwort-Manager allerdings eher als ein nützliches Tool zur Steigerung der Benutzerfreundlichkeit zu sehen sind, bieten Single Sign-On Lösungen mit integrierter Mehr-Faktor-Authentifizierung eine höhere Sicherheit und Transparenz und sind ein wichtiger Bestandteil einer starken Cybersicherheitsstrategie. Zudem sind Single Sign-On Lösung die zukunftsfähigere Alternative, wenn es in Richtung passwortlose Authentifizierung über kryptografische Mehr-Faktor-Authentifizierung geht. Wenn es um den Schutz sensibler Daten und die Einhaltung gesetzlicher Vorschriften geht, sollten Unternehmen also langfristig definitv über die Investition in eine zuverlässige Single Sign-On Lösung, wie Bare.ID, nachdenken.