Single Sign-On: **Wir entlarven vier verbreitete Mythen**

Immer mehr Unternehmen erkennen die Vorteile von Single Sign-On (SSO). Eine vor Kurzem von Okta in Auftrag gegebene Umfrage zu SSO zeigt:

88%
der befragten Unternehmen verwenden bereits eine SSO-Lösung.

95%
der befragten IT-Entscheider sehen SSO als einen wichtigen Teil ihrer IT-Infrastruktur.

20
oder mehr Anwendungen werden in der Regel mit einer SSO-Lösung geschützt, in vielen Unternehmen mehr als 30.

Trotz des offensichtlichen Nutzens von SSO gibt es immer noch Mythen dazu. Sehen wir uns einige der häufigsten Irrtümer an.

Mythos
SSO ist teuer

Einige IT-Entscheider sind nach wie vor der Meinung, dass SSO unnötig und seinen Preis nicht wert ist. Aber was kostet es, SSO nicht zu verwenden?

Die Realität

In Unternehmen *ohne* SSO-Lösung:

Die IT-Abteilung verbringt die meiste Zeit mit der Bearbeitung von Anfragen zur Passwortrücksetzung. Im Durchschnitt kostet dies 8 $ pro Anfrage, was sich bei einem wachsenden Unternehmen schnell summiert.[1]

Mehrere Anmeldedaten zu verwalten, frustriert die Mitarbeiter, reduziert die Produktivität und verlangsamt das Geschäft. Eine Passwortrücksetzung verursacht 10 $ an Produktivitätsverlust; jeder Mitarbeiter braucht im Durchschnitt eine pro Jahr.[2]

Das Hacking-Risiko ist höher. Eine Datensicherheitsverletzung kostet in den USA durchschnittlich 7,9 Mio. $,[3] und 81 % der Verletzungen sind Folge von Anmeldedaten-Diebstahl;[3] diesen kann SSO erheblich reduzieren.

Mythos
SSO schafft einen Single Point of Failure

Da SSO ein einziges Passwort für alle Anwendungen zur Verfügung stellt, wird es als Single Point of Failure angesehen – Hacker müssen nur ein Passwort stehlen statt viele.

Die Realität

Ein Single Point of Failure existiert bereits: der Benutzer. Viele Menschen verwenden ein einfaches Passwort für mehrere Konten, sodass Hacker damit auf diese zugreifen können.
Modernes SSO behebt diesen Single Point of Failure durch zusätzliche Sicherheitsmaßnahmen, wie ein MFA-Tool (Multi-Faktor-Authentifizierung):

Mit SSO kann die IT-Abteilung für jedes Passwort folgende Richtlinien festlegen:

- **Läuft** nach einer festgelegten Zeit ab.
- **Unterscheidet sich** von früheren Passwörtern.
- Entspricht nicht **gehackten Anmeldedaten.**
- **Sperrt** den Benutzer nach einigen erfolglosen Versuchen.

SSO betrachtet den Kontext einer Anmeldeanfrage und berücksichtigt folgende Aspekte:

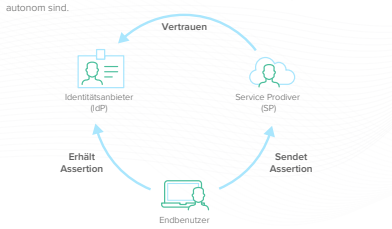
- Auf welche **Anwendung** wird zugegriffen?
- Welcher **Gruppe** gehört der Benutzer an?
- An welchem **Standort befindet sich der Benutzer**? Ist das plausibel?
- Welches **Gerät** wird verwendet? Wurde es schon früher benutzt?
- Welche **IP-Adresse hat der Benutzer**? Ist sie verdächtig?

Mythos
SSO ist dasselbe wie ein Passwortmanager

Da SSO über ein einziges Passwort den Zugriff auf verschiedene Anwendungen ermöglicht, kann es wie ein Passwortmanager wirken.

Die Realität

Bei SSO liegt der Schwerpunkt nicht auf Passwörtern, sondern auf dem Zugriff. SSO nutzt die föderierte Identität – die gemeinsame Nutzung von Identitätsattributen durch Systeme, die als vertrauenswürdig eingestuft, aber autonom sind.

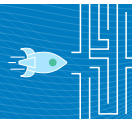


Modernes SSO verwendet Föderationsprotokolle wie SAML 2.0 und OpenID Connect. Von unseren Umfrageteilnehmern verwenden 91 % diese Protokolle für ihre SSO-Lösung.

Modernes SSO umfasst auch Integrationen für:

Mythos
SSO ist schwierig zu implementieren

Die meisten Unternehmen benötigen sowohl Cloud-Anwendungen als auch eine lokale Infrastruktur, und es ist schwierig, eine SSO-Lösung für beides zu implementieren.



Die Realität

Moderne SSO-Lösungen umfassen vorgefertigte Integrationen für alle IT-Ressourcen, sowohl lokal als auch in der Cloud, und erfordern weder zusätzliche lokale Server noch Änderungen an der Firewall.

- Umfassende, vorgefertigte Integrationen für Tausende beliebte Anwendungen
- Auf Standards – wie SAML, OIDC und SCIM – basierende Integrationen für lokale und Cloud-Anwendungen
- Toolkits, mit denen individuelle Anwendungen leicht SAML unterstützen können
- Möglichkeit einer Verbindung zu einem bestehenden AD- oder LDAP-Verzeichnis mit automatischer Benutzeranbindung

Weitere Informationen

Unsere SSO-Blog-Reihe:

- Faktencheck: SSO ist das Gleiche wie ein Passwortmanager
- Faktencheck: SSO schafft einen Single Point of Failure
- Faktencheck: SSO verlangsamt die IT
- Faktencheck: SSO zu implementieren ist ein schwieriges Unterfangen

Unser Webinar:

- Things You Don't Know About Single Sign-On (Dinge, die Sie nicht über Single Sign-On wissen)

Oder besuchen Sie unsere SSO-Produktseite

okta

Quellen
1 Forrester, Making The Business Case For Identity And Access Management, August 2018
2 Ponemon 2019, https://databreachcalculator.mybluemix.net/assets/2019_Global_Cost_of_a_Data_Breach_Report.pdf
3 Verizon