Single Sign-On

Wunderwaffe SSO?

Passwort-Wildwuchs und eine steigende Akzeptanz der Cloud bewirken einen verstärkten Trend zu Single Sign-On. Doch hält die Authentifizierungsmethode auch, was sie bezüglich Sicherheit und Bedienkomfort verspricht?

Single Sign-On (SSO) ist ein zentralisierter Service zur Nutzer-Authentifizierung, bei dem ein einzelner Satz Login-Daten für den Zugriff auf mehrere Anwendungen verwendet werden kann. Der offensichtliche Nutzen liegt also in der Einfachheit. Die Authentifizierung geschieht einmalig über eine einzige Plattform, um Zugang zu einer Vielzahl an Services zu erhalten, ohne sich jedes Mal erneut an- und abmelden zu müssen.

› Wird Single Sign-On eingesetzt, ist das Sicherheitsniveau des Authentifizierungsprozesses entscheidend. Wird lediglich ein Passwort verwendet, sollte es also möglichst stark sein. (Foto: designer491, Shutterstock.com)

Im Alltag kennt man die Sign-In-Varianten etwa über soziale Netzwerke wie Google, Facebook oder Twitter als prominente SSO-Plattformen, wobei jede Plattform Zugang zu verschiedenen Services Dritter gewährt. Im Unternehmensumfeld wird SSO beispielsweise genutzt, um Nutzern Zugriff auf eigene Web-Anwendungen, die auf internen Servern gehostet werden oder ERP-Systeme in der Cloud zu gewähren.

SSO wird entweder als eigenständige Lösung angeboten, wie etwa Centrify Identity Service und Okta Single Sign-On, oder ist in Access-Management-Lösungen wie IBM Security Access Manager (ISAM) oder Oracle Access Management (OAM) enthalten. Letztere beinhalten in der Regel bereits fortschrittliche Authentifizierungsmechanismen oder zusätzliche Sicherheitskomponenten wie eine Web Application Firewall.

Richtig eingesetzt birgt SSO Vorteile für die Produktivität, das IT-Monitoring und Management sowie die Sicherheitskontrolle. Mit einem einzigen Sicherheits-Token (zum Beispiel Benutzername und Passwort), kann Nutzern der Zugriff auf mehrere Systeme, Plattformen, Anwendungen und andere Ressourcen gewährt und entzogen werden. Durch die Reduzierung auf einen Satz Zugangsdaten wird zudem die Gefahr gemindert, dass schwache, leicht zu entschlüsselnde Passwörter verwendet oder die Zugangsdaten vergessen werden.

Eine gut geplante und ausgeführte SSO-Strategie kann Kosten und Ausfallzeiten im Zusammenhang mit Passwort-Resets und Risiken durch Insider-Bedrohungen minimieren. Zudem lässt sich der Bedienkomfort für die Anwender sowie der Authentifizierungsprozess selbst verbessern und gibt letztendlich dem Unternehmen die absolute Kontrolle über die Zugriffsprivilegien der Nutzer.

Argumente für Single Sign-On

Insbesondere die stark wachsende Nutzung von Cloud-Anwendungen die eine zunehmende Zahl an Passwörtern mit sich bringt, führt zu einem vermehrten SSO-Einsatz. Das bedeutet sowohl eine Chance, als auch eine Hürde. Ergebnissen der „Trends in Cloud IT"-Umfrage von **BetterCloud** (*www.bettercloud.com/monitor/cloud-application-use-growth-impact/*) zufolge nutzten Unternehmen 2017 durchschnittlich 17 Cloud-Anwendungen um ihre IT-, Betriebs- und Geschäftsstrategien zu unterstützen. Da überrascht es nicht, dass 61 Prozent der Befragten glauben, Identity- und Access-Management (IAM) sei heutzutage wesentlich schwieriger umzusetzen als noch vor zwei Jahren.

Für Barry Scott, CTO bei Centrify EMEA, Anbieter von Identitätsdiensten für Rechenzentren, Cloud und mobile Endgeräte, sprechen zwei Gründe für SSO: *„Der erste ist, dass es den Bedienkomfort für die Anwender verbessert, da es den Wildwuchs an unterschiedlichen Benutzernamen und Passwörtern stoppt, den die explosionsartige Zunahme an Cloud-basierten Software-as-a-Service-Anwendungen (SaaS) zur Folge hatte."*

Der zweite Grund sei verbesserte Sicherheit. Die Hauptursache für Sicherheitsverstöße seien kompromittierte Zugangsdaten und je mehr Benutzernamen und Passwörter Mitarbeiter hätten, desto schlechter werde die Passwort-Hygiene. *„Wir fangen an, dieselben Passwörter überall zu verwenden und sie werden oft weniger komplex, was es einfacher macht, sie zu knacken,"* fasst Scott zusammen.

Joe Diamond, Director of Security Product bei Okta, Anbieter von Cloud-basiertem Identitätsmanagement, stimmt zu, dass Cloud-Anwendungen IT-Teams vor neue Herausforderungen stellen. IT-Abteilungen müssten sich mit Fragen bezüglich der Erstellung und Verwaltung von Nutzer-Accounts, Sicherstellung akkurater Berechtigungen (keine unnötigen Befugnisse) und korrekter Offboarding-Prozesse, wenn ein Mitarbeiter das Unternehmen verlässt, beschäftigen. Existieren verschiedene Identitätsspeicher/Silos über mehrere Lösungen hinweg, würde es unmöglich, diesen Wildwuchs zu managen.. *„Nur, weil ein Unternehmen Office 365, Box und Slack einsetzt, heißt das nicht, dass man auch drei unterschiedliche Logins und Passwörter für diese Services haben möchte,"* sagt Diamond und prognostiziert, dass SSO zu einer Grundvoraussetzung für Unternehmen werde, die Cloud-Lösungen nutzen möchten. Des Weiteren führt er auch Bring your own device (ByoD)-Richtlinien und eine zunehmende *„Always-on"- und „Arbeite von überall aus"*-Kultur als Triebkräfte hinter SSO an.

Immer mehr Menschen würden an Geräten arbeiten, die die IT nicht kontrollieren könne und in Netzwerken, bei denen die IT über keinerlei Sichtbarkeit verfüge. Das mache Authentifizierung zu einem entscheidenden, von Gerät und Standort unabhängigen Kontrollpunkt, um Sicherheitskontrollen wie Continuous Authentication, Multi-Faktor Authentifizierung (MFA), kontextbezogene Zugangskontrollen, Analyse von Nutzerverhalten und so weiter möglich zu machen.

Vorteile von Single Sign-On

Der größte Vorteil von SSO liegt in der gebotenen Skalierbarkeit. Durch automatisiertes Zugangsdaten-Management muss der System-Administrator sich nicht mehr händisch um all die verschiedenen Zugänge der Mitarbeiter für die einzelnen Services kümmern, die sie nutzen möchten. Das verringert wiederum die Gefahr für Fehler im Management der Authentifizierungsdaten und gibt der IT mehr Zeit, sich auf wichtigere Aufgaben zu konzentrieren. Weitere Mehrwerte liegen in der raschen Provisionierung für Cloud-Anwendungen. Wenn SSO offene Standards wie Security Assertion Markup Language (SAML) 2.0 unterstützt, kann die Anwendung, sofern die SSO-Lösung eine Schnittstelle für sie besitzt, schnell durch einen SSO-Admin provisioniert und an die Mitarbeiter ausgerollt werden. SSO kann zudem die Sicherheit verbessern, die Produktivität erhöhen und für weniger Helpdesk-Tickets sorgen.

Centrify EMEA CTO Scott sieht die Vorteile vor allem für das IT-Team und die Mitarbeiter. Der große Pluspunkt von SSO liege im Bedienkomfort für die Anwender, was wiederum zu weniger Helpdesk-Anrufen wegen Passwort-Resets führe. Es verbessere die Sicherheit, da weniger Zugangsdaten Risiken ausgesetzt seien, aber es bedürfe unbedingt einer Multi-Faktor-Authentifizierung (MFA) als Backup für Passwörter, falls sie gestohlen oder erraten werden. Hinzu käme, dass die Kunden von Centrify durch SSO auch den Onboarding-Prozess von Mitarbeitern für neue SaaS-Anwendungen schneller und einfacher gestalten könnten. *„Da die IT einfacher Zugriff gewähren kann, ist die Wahrscheinlichkeit, dass sich eine ‚Schatten-IT' entwickelt, weniger hoch,"* sagt Scott und ergänzt, dass gute SSO (oder Identity-as-a-solution, IDaaS)-Lösungen es Anwendern erlaubten, Zugriff auf neue Anwendungen anzufordern und einen schlanken Workflow für die Freigabe ermöglichen würden.

Francois Lasnier, SVP Identity and Access Management bei Gemalto, sagt, SSO könne *„den Druck mildern, indem es den IT-Teams mehr Kontrolle und den Mitarbeitern mehr Komfort gewährt."* Eine erfolgreiche SSO-Implementierung gebe der IT die Entscheidungshoheit darüber, wer auf welche Anwendungen, wann und wo zugreifen darf. Sie fördere Flexibilität und erlaube einem Unternehmen, Mitarbeiter auf alle Anwendungen zugreifen zu lassen, wenn sie im Büro sind, aber nur auf ein paar ausgewählte, wenn sie außerhalb arbeiten.

Entsprechende Lösungen schützten also das Business – während die Belegschaft gleichzeitig so arbeiten könne, wie es für sie am komfortabelsten sei. Alles in allem verbessere SSO, wenn es mit Mechanismen zum Risikomanagement (detaillierte, systematische Risikoanalyse aller Gruppen und Individuen vor der Rechtevergabe) kombiniert werde, die Zugangssicherheit und mindere die Bedrohung durch Datenlecks.

Nachteile von Single Sign-On

Den Argumenten, die für SSO sprechen, stehen aber auch einige problematische Aspekte gegenüber, die Unternehmen beachten sollten, wenn sie erwägen, eine solche zentrale Authentifizierungsmethode einzuführen. Ein wichtiger Punkt dabei ist, dass die Bündelung aller Zugänge unter einem Passwort dieses zu einer Art Single Point of Failure macht. Wird dieses Passwort geknackt, kann der Schaden potentiell enorm sein, da der Angreifer Zugang zu zahlreichen Services und Accounts erhält. Zwar kann die IT über das SSO-System das Passwort relativ schnell und einfach sperren. Dafür muss der Vorfall aber erst einmal bekannt sein, was unter Umständen lange dauern kann. Um dies zu verhindern, sind – wie weiter oben bereits erwähnt – komplexe, mehrstufige Sicherheitsmaßnahmen notwendig. Einfache Passwörter ohne zusätzliche Sicherheitsstufen sind einfach nicht mehr ausreichend.

Prominente Vorfälle wie der Equifax-Hack machen dies mehr als deutlich. Bei diesem Cyberangriff verschafften sich die Hacker über einen Website Exploit unbemerkt Zugriff auf das System des US-Finanzdienstleisters und stahlen im Laufe von etwa zweieinhalb Monaten unbemerkt Datensätze von über 143 Millionen Kunden – darunter Sozialversicherungsnummern, Adressen und Kreditkartendaten – bevor die Schwachstelle von der IT entdeckt und geschlossen wurde.

Um das Sicherheitsniveau anzuheben, ist eine mehrstufige Authentifizierung nötig, die neben dem Passwort noch weitere Identifikationsmerkmale umfasst. Das ist oft die berüchtigte Kontrollfrage nach dem *„Mädchennamen der Mutter"* oder Ähnlichem. Derlei Informationen können jedoch relativ einfach über Recherche in den sozialen Netzwerken, Social Engineering oder Phishing herausgefunden werden.

Auch die Verifikation via SMS-Code oder SIM-Karte ist fehleranfällig, da das SS7-Protokoll, das als Basis für den Nachrichtenaustausch über das Telefonnetz dient, bekannte Schwachstellen aufweist. Durch genau diese Schwachstelle wurde kürzlich die Zwei-Faktor-Authentifizierung (2FA) der Social-News-Site Reddit überwunden und ein zwar altes aber sehr umfangreiches Backup gestohlen, das auch kryptografisch geschützte Passwörter von Nutzern enthielt. Die sicherste Variante unter den „einfachen" 2FA-Methoden ist derzeit die Verifikation über ein Token in Form eines physischen Geräts oder einer Smartphone-App, die den Code anzeigt. Hier muss der Angreifer neben dem Passwort den tatsächlichen Gegenstand an sich bringen, um Zugang zu erhalten. Durch den relativ hohen Aufwand und punktuellen Angriffsvektor mit geringem Skalierungspotential ist das Risiko eines erfolgreichen Diebstahls hier sehr gering. Wird eine weitere .Sicherheitsabfrage in Form von risikobasierter Authentifikation, Verhaltensanalyse, Standort-Daten oder biometrischen Informationen hinzugefügt, spricht man von Multi-Faktor-Authentifizierung (MFA).

All diesen Methoden ist gemein, dass dem Authentifikationsprozess weitere Ebenen hinzugefügt werden, die das System für die IT und Anwender komplexer machen, was letztendlich der ursprünglichen Idee von SSO nach mehr Einfachheit entgegensteht.

Theorie und Praxis

Entscheidet sich ein Unternehmen, SSO einzuführen, sollte es sich laut Centrify-Manager Scott grob an folgenden Prozess halten:

- Definieren Sie eine Liste der relevanten Anwendungen und entscheiden Sie, welche geeignet sind.
- Sollten Anwendungen nicht SSO-fähig sein, weil sie zum Beispiel die von der Lösung verwendeten Standards zum Informationsaustausch nicht unterstützen, bewerten Sie deren Zukunft. Fordern Sie Ihre Software-Anbieter auf, SSO zu unterstützen.
- Legen Sie die hauptsächliche Identitätsquelle für Ihre Anwender fest. (Normalerweise handelt es sich um Microsoft Active Directory, aber es könnten auch LDAP, Google Directory oder andere enthalten sein.)
- Definieren Sie die erforderlichen Anwendungen und Richtlinien in der SSO-Lösung.
- Ermitteln Sie, wer Zugriff auf welche Anwendungen benötigt.
- Gewähren Sie – im Idealfall gruppenbasiert anstatt individuell für jede Person – Benutzern Zugriff auf Anwendungen. Dies sollte es vorhandenen Gruppenverwaltungsprozessen ermöglichen, den Zugriff auf Anwendungen in Zukunft zu regulieren.

So viel zur Theorie. In der praktischen Umsetzung gibt es jedoch noch einiges zu beachten. So fügt Lasnier von Gemalto hinzu, dass Unternehmen ihre aktuellen Authentifizierungsschemata berücksichtigen müssten. Für einige könnte das bedeuten, mehrere verschiedene Schemata einzusetzen, in der Regel nach Abteilung oder Anwendungsfall getrennt. All das sei jedoch irrelevant, wenn die von den Unternehmen implementierten Lösungen nicht alle Anwendungen unterstützen könnten, die sie verwenden oder wenn die Implementierungskosten zu hoch seien. Vorhandene Lösungen komplett zu ersetzen könne sehr kostspielig sein, daher müssten Unternehmen versuchen, diese Lösungen in einer einzigen Management-Lösung zu kombinieren, sodass sie die Möglichkeiten für Anwendungsfälle ausdehnen könnten. Darüber hinaus mahnt Diamond zur Vorsicht bei Legacy-Anwendungen: „Der Schlüssel liegt darin, Flexibilität ohne Kompromisse zu bieten." Für viele sei Active Directory (AD) der Authentifizierungs-Mechanismus der Wahl, aber man sollte trotzdem auf der Hut sein: Legacy-Anwendungen gebe es überall. Anwender müssten beispielsweise auch in der Lage sein, RADIUS, ein älteres Authentifizierungs-Protokoll für Clients in einem physischen oder virtuellen Netzwerk, zu unterstützen, um etwa kritische Anwendungsfälle abzudecken.

Fazit

SSO als Wunderwaffe zu bezeichnen, würde der Realität also nicht gerecht werden. Zu den Herausforderungen bei der Implementierung von SSO gehören Kosten, Kontrolle, Standardisierung (zum Beispiel Authentifizierung über eine Webanwendung mit SAML versus Token-basierte Autorisierung mit OAuth) und Schwachstellen.

So gab beispielsweise Anfang 2018 ein Validierungsfehler in dem offenen Protokoll SAML einem Angreifer die Möglichkeit, Systeme dazu zu bringen, eine für einen bestimmten Nutzer ausgestellte Authentifizierung auf einen anderen User zu übertragen – ohne dessen Passwort zu kennen. Centrify CTO Scott sieht darüber hinaus Probleme bezüglich der Kompatibilität in Form von Anwendungen, die SSO nicht unterstützen. Anwender müssten von ihren App-Anbietern fordern, echte SSO-Funktionalitäten über SAML oder Kerberos anzubieten und nicht einfach noch einen Benutzernamen und ein weiteres Passwort, um das sie sich kümmern müssten. Zudem sollten MFA und SSO gemeinsam und parallel eingesetzt werden.

Trotz aller Herausforderungen ist sich Scott jedoch sicher, dass SSO eine glänzende Zukunft hat. Durch den Einsatz eines ‚Zero Trust'-Modells bezüglich der Sicherheit werde SSO großflächiger Anwendung finden, damit Anwender stets auf die gleiche Art und Weise arbeiten könnten, egal wo sie sind und welches Gerät sie verwenden. Immer mehr Anbieter würden SSO in Ihre Anwendungen mit einbeziehen und MFA werde größere Akzeptanz finden aufgrund der potentiellen Gefahr nur eines einzigen Satzes an Zugangsdaten.

Jens Dose

Jens Dose ist Redakteur des CIO Magazins. Neben den Kernthemen rund um CIOs und ihre Projekte beschäftigt er sich auch mit der Rolle des CISO und dessen Aufgabengebiet.