gemalto
security to be free

Handbuch für das Zugriffs-management

Inhalt

Einführung 3

Glossar für das Zugriffsmanagement 4

Identity & Access Management (IAM) 4

Zugriffsmanagement 5

IDaaS 6

Identity Governance & Administration (IGA) 6

Föderierte Identitäten 7

Föderierte Anmeldung 7

Identity Provider 8

SAML 9

WS-Fed 11

Open ID Connect 13

Single-Sign-On (SSO) 15

Passwort-Speicher 16

Autorisierung 17

Authentifizierung 17

Kontextbasierte Authentifizierung 18

Kontinuierliche Authentifizierung 19

Einführung

Im Laufe der Jahre haben Sie vielleicht schon so einiges über das Zugriffsmanagement gehört. Tatsächlich werden die Begriffe „Authentifizierung“ und „Zugriffsmanagement“ oft synonym verwendet. Es gibt allerdings durchaus einen Bedeutungsunterschied. Bei der Authentifizierung wird die Identität eines Benutzers validiert, während das Zugriffsmanagement ermittelt, ob ein Benutzer die Erlaubnis hat, auf eine bestimmte Ressource zuzugreifen, und die für die jeweilige Ressource festgelegte Zugriffsrichtlinie durchsetzt.

Das Zugriffsmanagement ist sehr wichtig, wenn es darum geht, den Zugriff auf Cloud-Ressourcen zu verwalten. Heutzutage greifen Benutzer in der Regel täglich auf mehrere Cloud-Anwendungen zu. Das ist sowohl für die Benutzer selbst als auch für die IT lästig: Die Benutzer müssen sich zahlreiche Passwörter merken, und die IT muss unzählige vergessene Passwörter zurücksetzen. Die Lösung: Single-Sign-On: Benutzer erhalten Zugangsdaten, die für alle Cloud-Anwendungen genutzt werden können. So wird die Anmeldung an mehreren Anwendungen vereinfacht, und die IT spart viel Zeit für das Zurücksetzen von Passwörtern.

Doch diese zentralen Zugangsdaten sind nur so sicher wie die zur Verifizierung verwendete Authentifizierungsmethode. Sie ist enorm wichtig, um die Zugriffssicherheit für die Cloud zu gewährleisten. Lösungen für das Zugriffsmanagement und Single-Sign-On ermöglichen eine granulare Kontrolle der für jede Anwendung festgelegten Zugriffsrichtlinien. Wenn ein hohes Risiko erkannt wird, kommt ein zusätzlicher Authentifizierungsfaktor zum Einsatz. Auch hier leidet die Benutzerfreundlichkeit nicht.

Glossar für das Zugriffsmanagement

Identity & Access Management (IAM)

Lösungen für das Identity & Access Management (IAM) bestehen aus den Komponenten Identity Governance & Administration (IGA) und Access Management (AM). IAM-Lösungen bieten ein methodisches Framework für das Erlauben (und Anfordern) von Zugriffen auf Anwendungen (IGA) sowie das Durchsetzen von Zugriffskontrollen (AM) und sorgen für transparente Einblicke in Zugriffsereignisse (AM). Da die meisten Unternehmen die IGA- und AM-Komponenten getrennt voneinander einsetzen, werden diese zunehmend als eigenständige Standalone-Lösungen und nicht mehr als kombinierte Funktionalität einer IAM-Suite eingestuft.

Zugriffsmanagement

Mit dem Zugriffsmanagement kann festgestellt werden, ob ein Benutzer die Erlaubnis hat, auf eine bestimmte Ressource zuzugreifen. Hier wird die für die jeweilige Ressource festgelegte Zugriffsrichtlinie durchgesetzt.

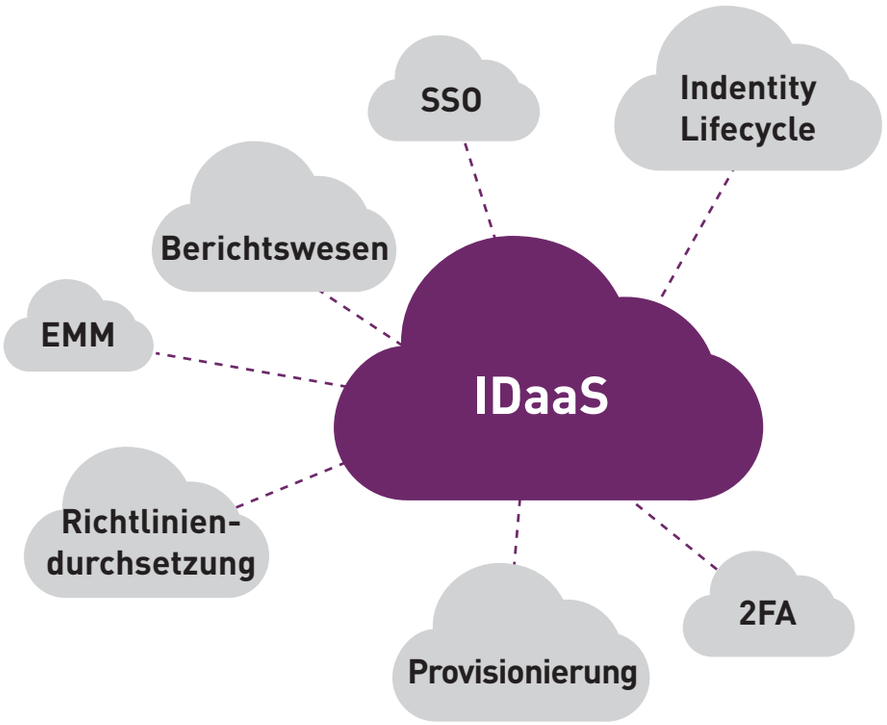
Das Zugriffsmanagement basiert auf Zugriffsrichtlinien, die von IT-Administratoren definiert werden und Informationen darüber enthalten, welche Benutzergruppen (z. B. Vertrieb, F&E, Personalabteilung) auf welche Cloud-Anwendungen (z. B. Salesforce, Office 365, Jira, Taleo) zugreifen dürfen. Außerdem sind Informationen über die für den Zugriff auf jede Anwendung erforderlichen Benutzerattribute (z. B. vertrauenswürdiges Netzwerk, Passwort, einmalig gültiges Passwort) enthalten.

Die Zugriffsrichtlinie kann je nach Sensibilität einer Cloud-Anwendung mehr oder weniger Benutzerattribute erfordern. Diese Attribute werden mittels risikobasierter oder kontextbasierter Authentifizierung bewertet, die für die Durchsetzung der für jede Cloud-Anwendung definierten unterschiedlichen Zugriffsrichtlinien von zentraler Bedeutung ist. (Weitere Informationen finden Sie unter „Kontextbasierte Authentifizierung“.)

Von großer Bedeutung für das Cloud-Zugriffsmanagement ist auch das Single-Sign-On, das es ermöglicht, sich an allen Cloud-Anwendungen mit einem einzigen Benutzernamen und Passwort bzw. einer zentralen „Identität“ anzumelden. (Weitere Informationen finden Sie unter „Single-Sign-On“.)

IDaaS

IDaaS steht für IAM-as-a-Service bzw. Identity-as-a-Service und beschreibt Lösungen für das Identity & Access Management (IAM), die ein cloud-basiertes Service-Modell für das Identitäts- und Zugriffsmanagement bieten. Obwohl IDaaS in den letzten Jahren als eigenständiger Markt betrachtet wurde, wird es aufgrund aktueller Trends künftig in zwei getrennte Bereiche unterteilt: Zugriffsmanagement und IGA. Die Bereitstellung erfolgt als Installation vor Ort, als Software oder als cloud-basierte Plattform.



Identity Governance & Administration (IGA)

Lösungen für Identity Governance & Administration (IGA) helfen bei der Beantwortung folgender Fragen: „Wer soll Zugriff auf welche Anwendungen erhalten bzw. wer ist für welche Anwendungen zugriffsberechtigt?“ und „Wer hat von wem und wann Zugriff auf welche Anwendungen erhalten?“ Eine IGA-Lösung ermittelt beispielsweise, ob F&E-Mitarbeiter dazu berechtigt sind, auf bestimmte Entwicklungsanwendungen wie GitHub, Jira und Confluence zuzugreifen. Sie kann den Zugriff auf diese Anwendungen auf der Basis der aktuellen Gruppenzugehörigkeiten der F&E-Mitarbeiter automatisch einrichten. F&E-Mitarbeiter können auch Zugriffsrechte auf andere Anwendungen anfordern. Diese Anfrage wird dann durch einen Management-Genehmigungsprozess geleitet, den einige IGA-Lösungen unterstützen.

Föderierte Identitäten

Bei föderierten Identitäten regelt ein zentrales System – der sogenannte Trusted Identity Provider (IdP) – die Authentifizierung von Benutzern. Die Cloud-Anwendungen leiten den Authentifizierungsprozess jedes Mal an den IdP weiter, wenn ein Benutzer versucht, auf sie zuzugreifen. Zudem lösen föderierte Identitäten die Herausforderungen und Komplexität bei der Verwaltung von separaten Zugangsdaten für zahlreiche Webanwendungen – und zwar unabhängig davon, ob es sich um interne oder externe Anwendungen handelt. Sie setzen auf Protokolle wie SAML und Open ID Connect sowie auf proprietäre Protokolle wie WS-Federation von Microsoft.

Föderierte Anmeldung

Die föderierte Anmeldung ist eine Funktion von Protokollen wie SAML, Open ID Connect u. a., die ein Identity-Provider-Modell für die Benutzerauthentifizierung verwenden und die Authentifizierungsinformationen in Form einer „Assertion“ an das Zielsystem weitergeben. Die Assertion gibt die Antwort „Akzeptieren“ oder „Ablehnen“ zurück und führt dazu, dass dem Benutzer der Zugriff gewährt oder verweigert wird.

So müssen sich Benutzer nur einmal authentifizieren, um auf sämtliche Cloud-Anwendungen zuzugreifen. Anstatt sich mit verschiedenen Benutzernamen und Passwörtern bzw. „Identitäten“ an diversen Cloud-Anwendungen anzumelden, können Benutzer die gleiche Identität für das Login bei Office 365, Salesforce, AWS usw. verwenden, mit der sie sich morgens am Unternehmensnetzwerk oder abends am VPN anmelden.

Bei föderierten Identitäten regelt ein zentrales System – der sogenannte Trusted Identity Provider – die Authentifizierung von Benutzern. Die Cloud-Anwendungen leiten den Authentifizierungsprozess jedes Mal an den IdP weiter, wenn ein Benutzer versucht, auf sie zuzugreifen.

Identity Provider

SAML und andere Protokolle für föderierte Identitäten, die den sicheren Austausch von Identitätsdaten zwischen unabhängigen Websites ermöglichen, basieren auf einem Identity-Provider (IdP)- und Service-Provider-Modell. Wenn ein Benutzer auf einen Service-Provider zugreift (cloud-basierter Service), wird er zur Authentifizierung bzw. Autorisierung an den vertrauenswürdigen Identity Provider weitergeleitet. Der Identity Provider überprüft die Authentifizierungsdaten des Benutzers (z. B. Cookie, Gerät, Netzwerk, einmalig gültiges Passwort) und gibt die Antwort „Akzeptieren“ oder „Ablehnen“ zurück, die dann an den Service-Provider weitergeleitet wird. Zu den Autorisierungsdaten kann die Erlaubnis gehören, auf Informationen wie E-Mail-Adressen von einem Webmail-Konto oder Namen von Freunden eines Social-Network-Kontos zuzugreifen.

Beispielsweise fungiert der SafeNet Authentication Service als Identity Provider, wenn Benutzer wie oben beschrieben auf Cloud-Anwendungen zugreifen.

Security Token Services

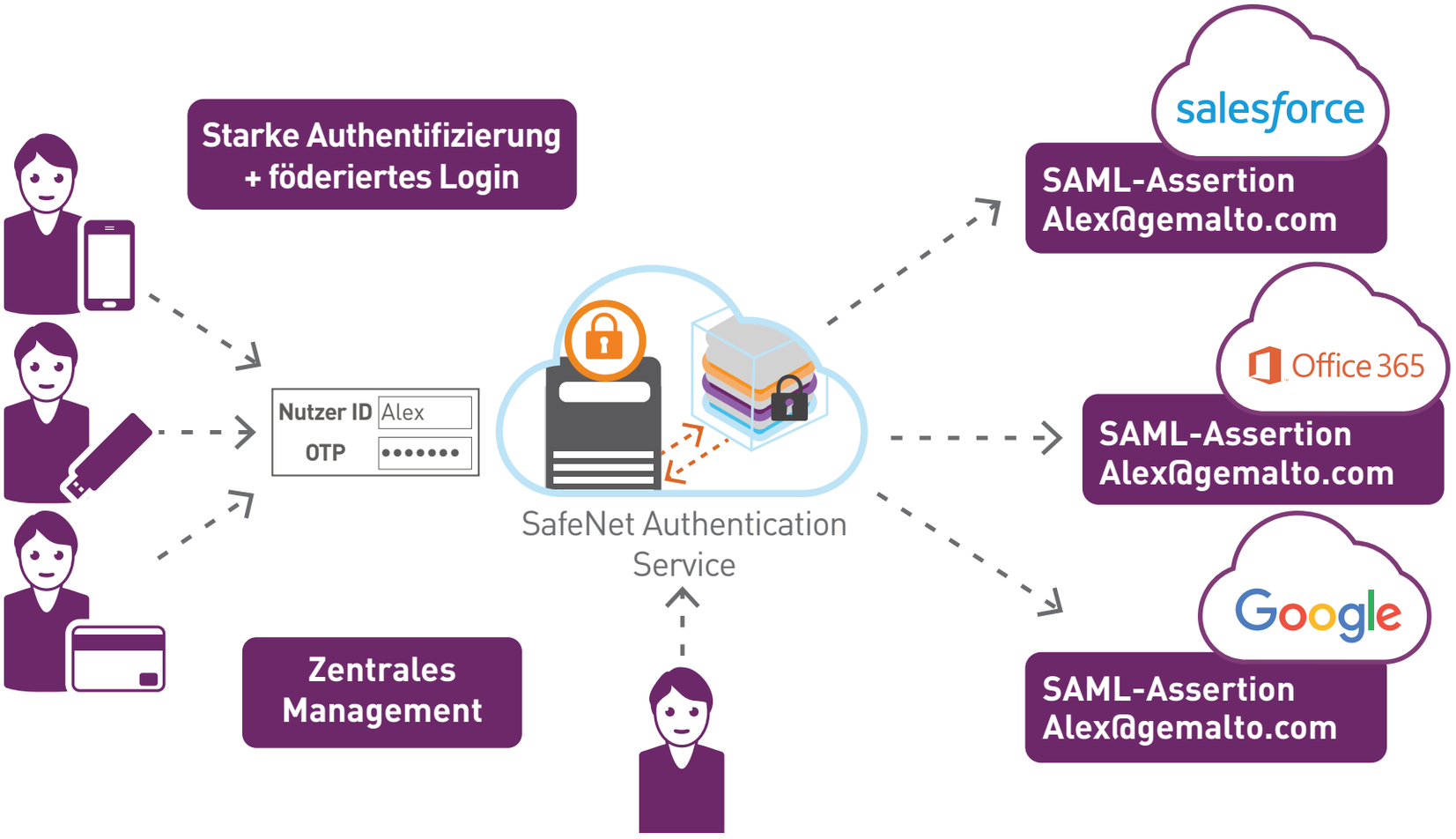
Identity-Provider-Modelle werden auch als token-basierte Authentifizierung oder Security Token Services (STS) bezeichnet. Ein STS entspricht einem Identity Provider, während die Relying Party (RP) dem Service-Provider entspricht. Statt SAML-Assertions werden hier Sicherheits-Token ausgetauscht. Unterschiedliche Namen, gleiches Prinzip.

SAML

SAML, gesprochen „Sammel“, steht für „Security Assertion Markup Language“. Es handelt sich um einen XML-basierten offenen Standard für den Austausch von Authentifizierungsdaten zwischen unabhängigen Websites. Diese Funktionalität wird auch als föderierte Identität oder föderierte Authentifizierung bezeichnet. Bei föderierten Identitäten lassen sich die aktuellen Benutzeridentitäten im Unternehmen auf die Cloud ausweiten. So ist eine Anmeldung an Cloud-Anwendungen mit der Unternehmensidentität möglich. Die föderierte Authentifizierung an Cloud-Anwendungen mit SAML ermöglicht es Benutzern, sich mit der aktuellen Unternehmensidentität an allen Cloud-Anwendungen anzumelden. So müssen sie sich nur einen Benutzernamen und ein Passwort merken.

So funktioniert SAML

Wenn ein Benutzer versucht, sich an einer cloud-basierten Anwendung anzumelden, wird er zur Authentifizierung an einen vertrauenswürdigen Identity Provider weitergeleitet. Der Identity Provider erfasst die Anmeldeinformationen des Benutzers, z. B. seinen Benutzernamen und sein einmalig gültiges Passwort, und gibt eine Antwort für den Zugriff auf die Cloud-Anwendung zurück. Diese auch SAML-Assertion genannte Antwort kann „Akzeptieren“ oder „Ablehnen“ lauten. Auf der Basis dieser Antwort blockiert oder erlaubt der Service-Provider, z. B. Salesforce, Office 365 oder Dropbox, den Zugriff auf die Anwendung.



WS-Fed

WS-Federation Services, kurz WS-Fed, ist das Microsoft-Protokoll für föderierte Identitäten. WS-Fed funktioniert mit den Active Directory Federation Services (ADFS) von Microsoft. Hier werden in Active Directory hinterlegte Identitäten auf cloud-basierte Microsoft-Anwendungen wie Office 365 oder Azure ausgeweitet. Wie SAML verwendet auch WS-Fed ein Identity-Provider-Modell. Beim Zugriff auf eine Microsoft-Cloud-Anwendung wird der Benutzer zur Authentifizierung an ADFS weitergeleitet. Auf der Basis der ADFS-Antwort gewährt oder verweigert die Cloud-Anwendung dem Benutzer den Zugriff.

OAuth

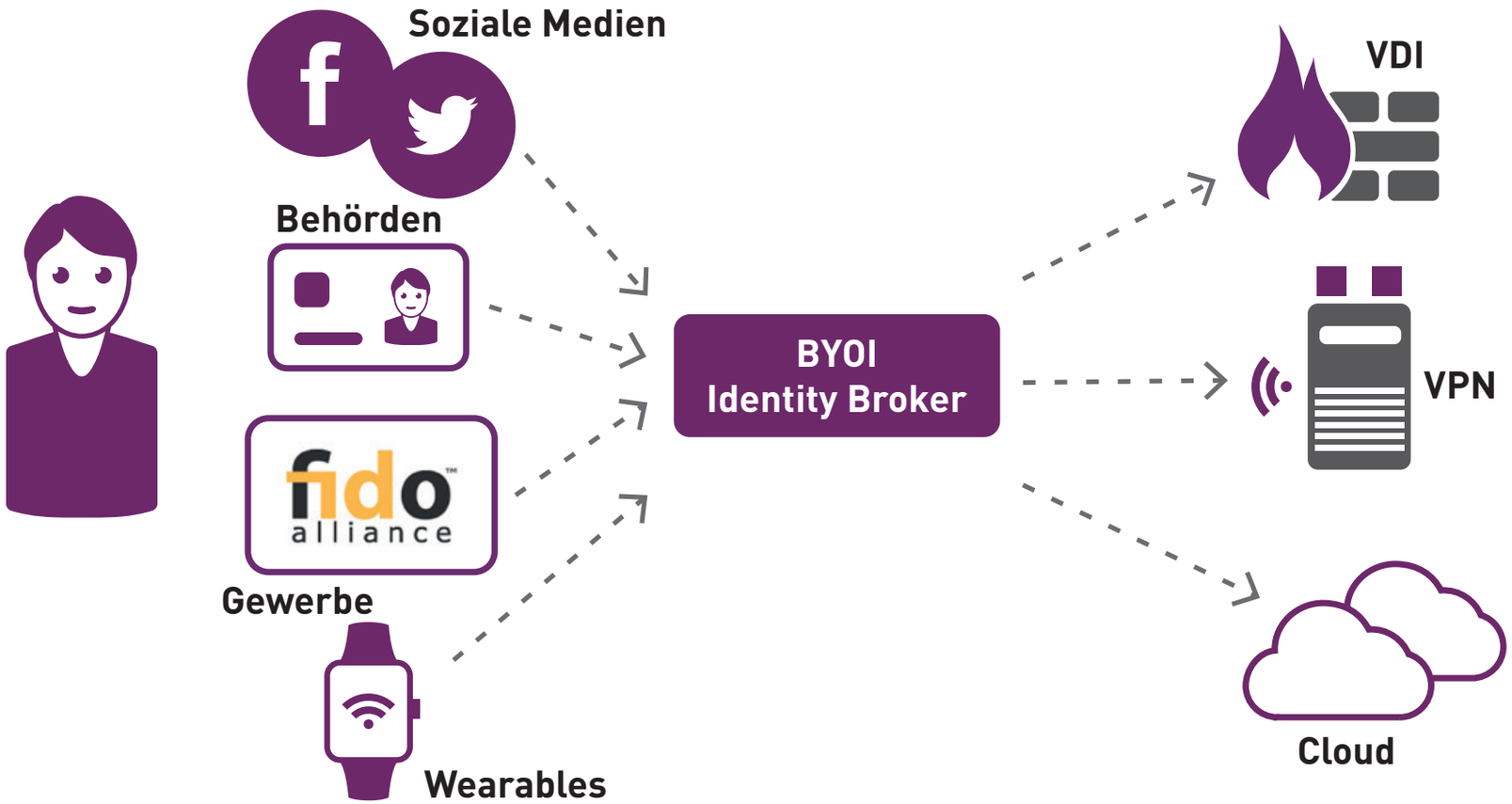
OAuth, gesprochen „Oh-Auth“, steht für Open Authorization bzw. offene Autorisierung. Es handelt sich um einen offenen Standard für die föderierte bzw. token-basierte Authentifizierung und die Autorisierung zwischen unabhängigen Websites. Wie bei anderen Protokollen für föderierte Identitäten, z. B. SAML, Open ID Connect und WS-Fed, ermöglicht OAuth das Login an einer Anwendung mit einer Identität, die von einem vertrauenswürdigen Identity Provider überprüft wird. OAuth geht über die föderierte Authentifizierung hinaus und erlaubt es Benutzern, vertrauenswürdige Websites für den Zugriff auf bestimmte Kontoinformationen wie Kontaktnamen und E-Mail-Adressen zu autorisieren. Das OAuth-Protokoll wird beispielsweise von sozialen Netzwerken verwendet, um auf Webmail-Kontakte zuzugreifen und zu fragen, ob diese Kontakte zu sozialen Netzwerken eingeladen werden sollen.

Open ID Connect

Wie auch SAML ist OpenID Connect ein offenes Protokoll für föderierte Identitäten, das ein Identity-Provider-Modell verwendet. Im Gegensatz zu SAML, das mit einem Cookie arbeitet und daher nur mit Anwendungen funktioniert, die sich in einem Browser öffnen lassen („browser-basierte Anwendungen"), bietet OpenID Connect ein Single-Sign-On-Framework, das die Implementierung von SSO für browser-basierte Anwendungen, native mobile Anwendungen und Desktop-Clients (wie Rich-Clients und einige VPNs) ermöglicht. Die meisten Single-Sign-On-Implementierungen unterstützen heute nur cloud- und browser-basierte Anwendungen. Da immer mehr Identity Provider auf OpenID Connect setzen, ist nur eine einmalige Authentifizierung erforderlich, um gleichzeitig Zugriff auf alle Ressourcen zu erhalten, darunter Desktop-Clients, browser-basierte Anwendungen und native mobile Anwendungen.

Bring Your Own Identity (BYOI)

Im Bereich Identitätsmanagement suchen Anbieter und Unternehmen nach Möglichkeiten, Mitarbeitern und Partnern den Zugriff auf Unternehmensressourcen über ihre eigene Identität zu ermöglichen. Diese Identität könnte theoretisch jede Identität sein, die ein ausreichendes Maß an Identitätssicherheit bietet, z. B. Personalausweise, Krankenkassenkarten oder Online-Identitäten wie Identitäten für soziale Netzwerke, Berufsnetzwerke und kommerziell verfügbare Identitäten wie FIDO. Die Unternehmens- und Konsumentenwelt nähern sich einander immer mehr an. Sicherheitsteams in Unternehmen stehen zunehmend unter dem Druck, die gleichen Authentifizierungsmethoden zu implementieren, wie sie typischerweise in Consumer Services zu finden sind.



Single-Sign-On (SSO)

Mit Single-Sign-On (SSO) ist nur eine einmalige Authentifizierung erforderlich. Beim Zugriff auf weitere Ressourcen erfolgt die Authentifizierung dann automatisch. Damit entfällt die separate Anmeldung und Authentifizierung für einzelne Anwendungen und Systeme. SSO fungiert quasi als Mittler zwischen Benutzer und den gewünschten Anwendungen. Hinter den Kulissen behalten Zielanwendungen und -systeme immer noch ihre eigenen Speicher für Zugangsdaten und präsentieren im Benutzersystem entsprechende Anmeldeaufforderungen. Das SSO reagiert auf diese Aufforderungen und ordnet die Zugangsdaten zu einem Zugangsdatensatz (Benutzername und Passwort) zu. (Quelle: Gartner)

Das SSO kann in einer Standalone-Lösung oder einer breit aufgestellten Zugriffsmanagementlösung durch eine Reihe von Protokollen für föderierte Identitäten umgesetzt werden. Dazu zählen Open-Source-Protokolle wie SAML 2.0 und Open ID Connect, proprietäre Protokolle wie WS-Federation von Microsoft und andere Technologien wie Passwort-Speicher und Reverse-Proxies.

Passwort-Speicher

Passwort-Speicher, auch Passwort-Manager genannt, sind eine einfache Möglichkeit für das Single-Sign-On (SSO), wenn eine Zielanwendung keine Protokolle für föderierte Identitäten unterstützt, z. B. eine Legacy- oder benutzerdefinierte Anwendung. Passwort-Speicher sind Systeme, die die Passwörter verschiedener Websites speichern und verschlüsseln. Anstatt sich bei jeder Anwendung mit einem dedizierten Passwort anzumelden, kann sich der Benutzer einfach mit einem Master-Passwort authentifizieren (das wiederum den Passwort-Speicher entschlüsselt). Dadurch entfällt die Notwendigkeit, mehrere Passwörter zu pflegen.

Autorisierung

Die Autorisierung ist ein Prozess, der sicherstellt, dass ordnungsgemäß authentifizierte Benutzer nur auf die Ressourcen zugreifen können, für die der Eigentümer oder Administrator dieser Ressource den Zugriff festgelegt und gestattet hat. In der Konsumwelt kann sich die Autorisierung auch auf den Prozess beziehen, bei dem ein Benutzer sicherstellt, dass eine cloud-basierte Anwendung (z. B. ein soziales Netzwerk) nur auf bestimmte Informationen von einer unabhängigen Website (z. B. auf das Webmail-Konto des Benutzers) zugreift.

Authentifizierung

Die Authentifizierung ist ein Prozess, bei dem die Identität eines Benutzers anhand der Anmeldeinformationen validiert oder verifiziert wird, die der Benutzer beim Login an einer Anwendung, einem Dienst, einem Computer oder einer digitalen Umgebung angibt. Die meisten Authentifizierungsdaten bestehen aus etwas, das der Anwender besitzt, z. B. der Benutzername, und etwas, das der Anwender kennt, z. B. ein Passwort. Wenn die vom Benutzer eingegebenen Anmeldeinformationen mit denen der zugrunde liegenden Anwendung oder dem Identity Provider übereinstimmen, wird er erfolgreich authentifiziert und der Zugriff gewährt.

Kontextbasierte Authentifizierung

Die kontextbasierte Authentifizierung verifiziert die Identität der Benutzer, indem sie eine Reihe von zusätzlichen Informationen beim Login an einer Anwendung bewertet. Zu den häufigsten Kontextinformationen gehören der Standort des Benutzers, die Uhrzeit, die IP-Adresse, der Gerätetyp, die URL und die Vertrauenswürdigkeit der Anwendung. Die kontextbasierte Authentifizierung, auch risikobasierte oder adaptive Authentifizierung genannt, ist in der Welt des SSO und Zugriffsmanagements von zentraler Bedeutung, um die Authentifizierung so transparent und problemlos wie möglich zu gestalten.

Durch die Bewertung der Login-Attribute eines Benutzers – sei es kontextbezogen (Gerät, Rolle, Standort) oder verhaltensbasiert (z. B. Tippgeschwindigkeit, Seitenansichtsreihenfolge) – können Lösungen für das Single-Sign-On und Zugriffsmanagement kontinuierlich die vom Benutzer geforderte Authentifizierungsstufe mit der für jede Anwendung definierten Zugriffsrichtlinie abgleichen. Auf diese Weise wird die Authentifizierung granular und möglichst reibungslos für jede Zugriffsrichtlinie einer Anwendung und nicht als pauschale, einheitliche Regel für alle Unternehmensressourcen angewendet.

Kontinuierliche Authentifizierung

Ganz gleich ob mit einem Token, einem Passwort oder einem Fingerabdruck – die Authentifizierung ist grundsätzlich eine Ja/Nein-Entscheidung: Das System überprüft die Identität eines Benutzers und erlaubt oder verweigert den Zugriff auf eine Anwendung.

Dank moderner Technologien wie der kontextbasierten Authentifizierung oder der Verhaltensbiometrie (z. B. Tippmuster und andere physikalische Merkmale) kann die Authentifizierung zu einem kontinuierlicheren Prozess werden. Durch die Bewertung zahlreicher Attribute wie IP-Adresse, mobile Parameter, bekanntes Gerät, Betriebssystem usw. kann die kontextuelle oder risikobasierte Authentifizierung die Identität einer Person bei jeder Anmeldung an einer Anwendung kontinuierlich überprüfen. Der Benutzer bekommt davon nichts mit.

Die kontextuelle Authentifizierung bietet viele Möglichkeiten zur Überprüfung der Identität einer Person. Und genau so lässt sich ein Gleichgewicht zwischen Benutzerfreundlichkeit und granularer Zugriffskontrolle für zahlreiche Cloud-Anwendungen schaffen. Aus diesem Grund ist die kontinuierliche Authentifizierung, die auf kontextbasierter Authentifizierung basiert, eine wichtige Grundlage des Cloud-Zugriffsmanagements.

Gemaltos Angebot von SafeNet-Lösungen für Identitäts- und Datenschutz ermöglicht Behörden und Unternehmen die Umsetzung eines datenzentrischen Security-Ansatzes. Mit innovativen Verschlüsselungsmethoden, branchenführender Krypto-Management-Technologie, Authentifizierungs- und Identitätsmanagementlösungen können sie sensible Daten schützen – unabhängig davon, wo sich diese befinden. Gemalto hilft damit auch Institutionen mit strengsten Datenschutzregeln die Compliance-Anforderungen zu erfüllen. Sensible Informationen, Kundendaten und digitale Transaktionen sind so sicher vor Diebstahl und Manipulation – für mehr Vertrauen in einer zunehmend digitalen Welt.

Kontakt: Eine Übersicht unserer Niederlassungen und die entsprechenden Kontaktdaten finden Sie unter safenet.gemalto.com.

Folgen Sie uns: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free

©Gemalto 2018. Alle Rechte vorbehalten. Gemalto und das Gemalto-Logo sind Marken bzw. Dienstleistungsmarken von Gemalto und in bestimmten Ländern eingetragen. eB (DE) - 29Aug2018 – Design: RM