thalesgroup.com

THALES

Vier Schritte für das Cloud-Zugriffsmanagement

Eine praktische Schritt-für-Schritt-Anleitung zur Verwaltung des Cloud-Zugriffs in Unternehmen

Probleme beim Cloud-Zugriff in Unternehmen

Die Nutzung von Cloud-Anwendungen in Unternehmen ist heute gang und gäbe. 93 % aller Unternehmen greifen auf cloud-basierte IT-Services zurück[1]. Das ist allerdings mit einigen Problemen verbunden. Wenn Unternehmen Cloud-Anwendungen und moderne Technologien nutzen, um einen schnellen Mehrwert zu erzielen, steigen der Verwaltungsaufwand und die Komplexität für Benutzer.

Passwortmüdigkeit

Benutzern fällt es schwer, sich unzählige Benutzernamen und Passwörter zu merken. Sie müssen sich täglich mehrmals an jeder Anwendung authentifizieren, die sie öffnen. Das führt zur sogenannten Passwortmüdigkeit – die Unzufriedenheit, die durch das tägliche Erstellen, Aktualisieren und Rücksetzen von Passwörtern für verschiedene Anwendungen entsteht.

Unzureichende Sicherheit

Cloud-Anwendungen sind standardmäßig nur durch schwache statische Passwörter geschützt. Das stellt eine Gefahr für vertrauliche Daten dar und erhöht das Risiko von Datenschutzverletzungen. Der Großteil der Datenschutzvorfälle in aller Welt ließe sich mit einer leistungsstarken Zwei-Faktor-Authentifizierung vermeiden[2].

Komplexe Verwaltung

Jede neue Cloud-Anwendung im Unternehmen muss über eine eigene Konsole oder ein Admin-Portal verwaltet und Fehler behoben werden. Die Skalierbarkeit der Administration leidet, wenn ein Dutzend oder mehr Anwendungen im gesamten Unternehmen genutzt werden.

Compliance-Risiko

Um gesetzliche Vorgaben einhalten zu können, ist ein Einblick in Zugriffsaktivitäten erforderlich. IT-Abteilungen müssen wissen, welche Benutzer wann auf welche Anwendungen zugreifen. Da auch vertrauliche Daten in der Cloud vorgehalten werden, müssen Administratoren wissen, wie die Identitäten von Benutzern verifiziert werden.

Hohe Help-Desk-Kosten

Die steigende Anzahl der Cloud-Identitäten und Zugangsdaten führt zu häufigen Anfragen zum Rücksetzen von Passwörtern, die 20 % der Help-Desk-Kosten von Unternehmen ausmachen[3].

1 Quelle: Spiceworks, Umfrage: 93 Percent of Organizations Use Cloud-Based IT Services

2 Quelle: 2016 Data Breach Investigations Report

3 Quelle: Statisnet, Forgotten user passwords – Eliminate the Problem Dramatically Reduce the Cost

Vier einfache Schritte zur vollen Cloud-Zugangskontrolle

Schritt 1 – Single-Sign-On für die Cloud

Um die benutzerseitige Passwortmüdigkeit zu eliminieren und IT-Mitarbeitern zahlreiche Anfragen für das Rücksetzen von Passwörtern zu ersparen, kann Single-Sign-On für alle im Unternehmen genutzten Cloud-Anwendungen eingesetzt werden.

Was ist Single-Sign-On?
Mit Single-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.

So müssen sich Benutzer nur einmal authentifizieren, um zeitgleich Zugang zu sämtlichen Cloud-Anwendungen zu erhalten. Die Anmeldung erfolgt mit der aktuellen Unternehmensidentität. Dies ist dieselbe Identität, mit der sich Benutzer morgens am Unternehmensnetzwerk und abends am VPN anmelden.

Rollenbasiertes SSO
Unterschiedliche Benutzer und Benutzergruppen benötigen Zugriff auf verschiedene Cloud-Anwendungen. Single-Sign-On lässt sich für beliebig viele Cloud-Umgebungen nutzen und an die diversen Teams, Rollen, Abteilungen und Einzelanwender anpassen. Die F&E-Abteilung beispielsweise benötigt neben dem Zugriff auf unternehmensweite Anwendungen auch Zugang zu Anwendungen wie Jira, Confluence oder AWS. Das Marketing muss sowohl auf Salesforce, Office 365 als auch auf WordPress zugreifen können. Geschäftspartner, z. B. Subunternehmer oder Händler, benötigen vielleicht Zugang zu Cloud-Anwendungen wie Partner-Portalen oder Produktivitätslösungen.

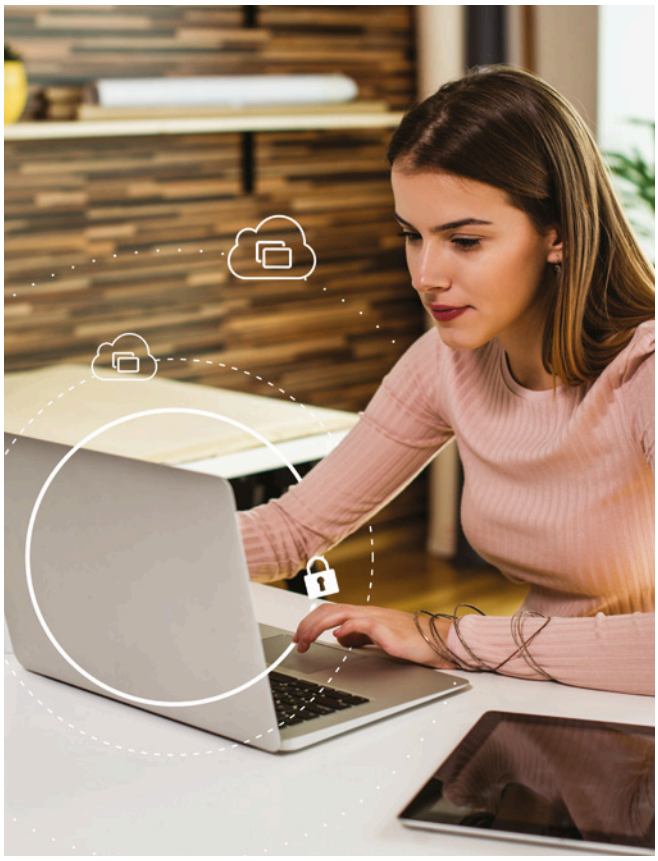
Um die Konfiguration gruppenbasierter Zugriffsrichtlinien zu vereinfachen, können rollenbasierte Benutzergruppen innerhalb des Unternehmens erstellt werden, z. B. für Active Directory, MySQL oder andere Datenspeicher.

Mit rollenbasierten Gruppen können Zugriffsberechtigungen auch einfach bereitgestellt, aktualisiert und entzogen werden, wenn Mitarbeiter eingestellt werden, das Unternehmen verlassen oder in eine andere Position wechseln.

Vorteile von SSO: Benutzerfreundlich, einfach zu verwalten und richtlinienkonform
SSO bietet nicht nur bequemen und problemlosen Zugriff für Benutzer, sondern vereinfacht auch IT-Administratoren das Leben, da diese nur eine Identität (einen Benutzernamen und ein Passwort) pro Anwender für alle Cloud-Ressourcen verwalten müssen. Damit entfallen der Aufwand für das Rücksetzen von Passwörtern und die Problembehebung über mehrere Verwaltungskonsolen.

Mit einer zentralen Übersicht für alle Zugriffsaktivitäten erhält die IT einen Einblick, wer wann worauf mit welcher Authentifizierungsmethode zugreift. Damit werden Sicherheits-Audits und die Einhaltung aufsichtsbehördlicher Vorgaben zum Kinderspiel. Durch den einheitlichen Blick auf Cloud-Zugriffe lassen sich zudem unzureichend genutzte Lizenzen für Cloud-Anwendungen identifizieren.

Single-Sign-On wird schon seit Langem für Vor-Ort-Anwendungen, Portale und Netzwerke (z. B. mit Kerberos-Protokoll) genutzt. Durch die Weiterentwicklung von Protokollen für föderierte Identitäten (wie SAML 2.0), die Unternehmensidentitäten auf die Cloud ausweiten, können Unternehmen diese Funktionalität nun auch für cloud-basierte Ressourcen nutzen.



Schritt 2 – Schutz von Identitäten mit detaillierten Zugriffsrichtlinien

SSO ist äußerst benutzerfreundlich und reduziert den IT-Aufwand. Dennoch reicht es allein für das Cloud- Zugriffsmanagement nicht aus. Dank SSO benötigt jeder Benutzer nur eine Identität für alle Cloud-Anwendungen. Was aber passiert, wenn diese Identität kompromittiert wird? Hier kommen situationsbasierte Zugriffskontrollen ins Spiel, mit deren Hilfe sich die geeignete Authentifizierung für den richtigen Benutzer zum richtigen Zeitpunkt festlegen lässt.

Situationsbasierte Zugriffsrichtlinien
Wir alle kennen die Zwei-Faktor-Authentifizierung (2FA). Für Anwendungen mit geringem Risiko, über die auf das Unternehmensnetzwerk zugegriffen wird (und ähnliche Anwendungsfälle), scheint 2FA etwas übertrieben zu sein. Um also diese eine Identität mit der geeigneten Authentifizierung zu schützen, können detaillierte Zugriffsrichtlinien angewendet werden, die zur Authentifizierung und zum jeweiligen Anwendungsfall passen. Zeiterfassungsanwendungen erfordern z. B. geringere Zugriffskontrollen als die Anmeldung an sensiblen Unternehmensressourcen wie beispielsweise ein VPN. Für die Anmeldung am Konto von IT-Administratoren oder CEOs wiederum ist eine höhere Sicherheit angebracht.

Da nicht alle Anwendungen dieselbe Sicherheit benötigen und nicht alle Benutzer die gleichen Berechtigungen haben, können situationsbasierte Zugriffsrichtlinien definiert werden, die die Vertraulichkeit und das Risiko cloud-basierter Anwendungen sowie die Rechte von Benutzergruppen (z. B. C-Level-Führungskräfte oder IT-Administratoren) berücksichtigen.

Ist die Vertrauenswürdigkeit niedrig, z. B. bei der Anmeldung über ein unbekanntes Netzwerk, lässt sich die Sicherheit durch eine zusätzliche Authentifizierungskomponente aufstocken. Das kann beispielsweise die Zwei-Faktor-Authentifizierung oder eine Out-of-Band-Push-Authentifizierung sein. Ist die Vertrauenswürdigkeit hoch, z. B. bei der Anmeldung über das Büronetzwerk und ein bekanntes Gerät, erhält der Benutzer unmittelbar Zugriff.

Kontextbasierte, kontinuierliche Authentifizierung
Mithilfe von Kontextinformationen, beispielsweise die Anmeldung über ein vertrauenswürdiges Netzwerk oder ein bekanntes Gerät, sorgen Lösungen für die Zugriffsverwaltung für eine hohe Benutzerfreundlichkeit. Zusätzliche Authentifizierungskomponenten sind nur in Situationen erforderlich, die mit einem hohen Risiko verbunden sind. Wenn Anwender vormittags ihr Notebook, mittags ihr Tablet und abends wieder ihr Notebook verwenden, wird je nach Anwendung, an der die Anmeldung erfolgt, Teamzugehörigkeit und verhaltensbasierten Kontextinformation die geeignete Zugriffsrichtlinie angewendet. So wird den ganzen Tag über eine kontinuierliche Authentifizierung möglich, die auf der jeweiligen Vertrauenswürdigkeit beruht.

Wird also Single-Sign-On für alle Cloud-Anwendungen der verschiedenen Benutzergruppen genutzt, z. B. C-Level- Mitarbeiter, F&E und Vertrieb, können situationsbasierte Zugriffsrichtlinien eingesetzt werden, die die Authentifizierungsmethode auf das vorliegende Szenario abstimmen. So wird jede Anmeldung vertrauenswürdig, während der Zugriff jederzeit problemlos möglich ist.

Erst global, dann detailliert
Um die Einrichtung von Zugriffsrichtlinien zu vereinfachen, sollte mit einer einzigen zentralen Richtlinie begonnen werden, der dann ggf. Ausnahmen hinzugefügt werden.

Diese globale Richtlinie gilt als Standard für alle Cloud-Anwendungen und -Benutzer und schreibt Mitarbeitern beispielsweise vor, sich einmalig per SSO und einem einmalig gültigen Passwort (OTP) an jeder Sitzung anzumelden und Cloud- und Web-Anwendungen ohne zusätzliche Authentifizierung zu nutzen.

Sobald die globale Richtlinie steht, können Ausnahmen hinzugefügt werden, für die bei höherem Risiko eine striktere Authentifizierung erforderlich ist, z. B. beim Zugriff auf vertrauliche Anwendungen von außerhalb des Unternehmensnetzwerks. Für alle übrigen Anwendungen gelten nach wie vor nur die zuvor in der globalen Richtlinie definierten Standard-Zugriffskontrollen.

Schritt 3 – Optimierung von Zugriffsrichtlinien durch datenorientierte Einblicke

Wie können Sie herausfinden, ob Zugriffsrichtlinien zu lax, zu strikt oder genau richtig sind? Ganz einfach: durch datenorientierte Einblicke. Wenn Sie wissen, welche Benutzer mit welchen Zugriffsrichtlinien auf welche Anwendungen zugreifen, kann die IT-Abteilung im Laufe der Zeit detaillierte, situationsbasierte Zugriffsrichtlinien entwickeln.

Greifen Benutzer beispielsweise oft über ein unbekanntes Netzwerk oder von einem Hochrisikostandort aus auf sensible Anwendungen zu, was durch die Häufigkeit des Richtlinieneinsatzes deutlich wird, lässt sich die für den Zugriff auf eine bestimmte Anwendung erforderliche Vertrauenswürdigkeit in dieser Richtlinie heraufsetzen. Schrieb die Richtlinie bisher nur ein Passwort oder eine PINNummer vor, kann diese Vorgabe in einen einmalig gültigen Passcode geändert werden.

Schreibt eine Zugriffsrichtlinie andersherum ein Passwort und ein OTP vor und wird häufig für alle Benutzer verwendet, kann der Anmeldevorgang durch Benutzername und OTP vereinfacht werden. Kontextbasierte Informationen werden dann als zusätzliche Authentifizierungskomponenten genutzt (z. B. ob der Zugriff über ein bekanntes oder ein unbekanntes Gerät erfolgt).

Werden statistische Daten in Zugriffsrichtlinien integriert, können Unternehmen ein effizientes Risikomanagement umsetzen und ein Gleichgewicht zwischen Sicherheitsanforderungen und Erwartungen an die Benutzerfreundlichkeit schaffen.

Schritt 4 – Skalierbarkeit der Cloud-Umgebung

Wie viele Cloud-Anwendungen möchte Ihr Unternehmen im kommenden Jahr hinzufügen? Stehen Fusionen oder Übernahmen bevor? Bevor Sie sich für eine Lösung zur Cloud-Zugriffsverwaltung entscheiden, sollten Sie sicherstellen, dass sich die Lösung skalieren lässt und mit Ihren Anforderungen wächst. So sollten sich z. B. Benutzergruppen und cloudbasierte Anwendungen bedarfsorientiert hinzufügen lassen.

Die meisten Cloud-Services unterstützen Branchenstandards wie SAML 2.0, mit denen sich das Cloud-Zugriffsmanagement im Zuge des Hinzufügens weiterer Anwendungen skalieren lässt. Im Lieferumfang enthaltene Integrationen vereinfachen darüber hinaus die Bereitstellung neuer Integrationen.

SafeNet Trusted Access – die clevere Zugriffsverwaltung fü¨r Clouds

SafeNet Trusted Access für die Zugriffsverwaltung vereint das bequeme Single-Sign-On und die detaillierte Zugriffssicherheit. Durch die Validierung von Identitäten, das Durchsetzen von Zugriffskontrollen und intelligentes Single-Sign-On sorgen Unternehmen für einen sicheren und problemlosen Zugriff auf zahlreiche Cloud-Anwendungen. Gleichzeitig sinkt der Verwaltungsaufwand, da die Zugriffskontrollen zentral über eine einfach zu bedienende Konsole definiert und angewendet wird.

SafeNet Trusted Access lässt sich schnell und einfach einrichten und erlaubt die einfache Umsetzung von Cloud-Lösungen. Ganz nebenbei werden Transparenz und Compliance verbessert. Vereinfachte Cloud-Workflows sorgen zudem für eine höhere Skalierbarkeit.

Durch flexible, individuelle Authentifizierung und Zugriffskontrollen reduziert SafeNet Trusted Access die Komplexität und Unzufriedenheit auf der Seite der Benutzer, die sich mit einer einzigen Unternehmensidentität an allen Cloud- Anwendungen anmelden können.

SafeNet Access Management- und Authentifizierungslösungen von Thales

Mit den branchenführenden Access Management- und Authentifizierungslösungen von Thales können Unternehmen den Zugriff auf Unternehmens-IT, Web- sowie auf Cloud-basierte Anwendungen zentral verwalten und sichern. Mit richtlinienbasierten SSO- und universellen Authentifizierungsmethoden können Unternehmen Verstöße effektiv verhindern, sicher in die Cloud migrieren und die Einhaltung gesetzlicher Bestimmungen vereinfachen.

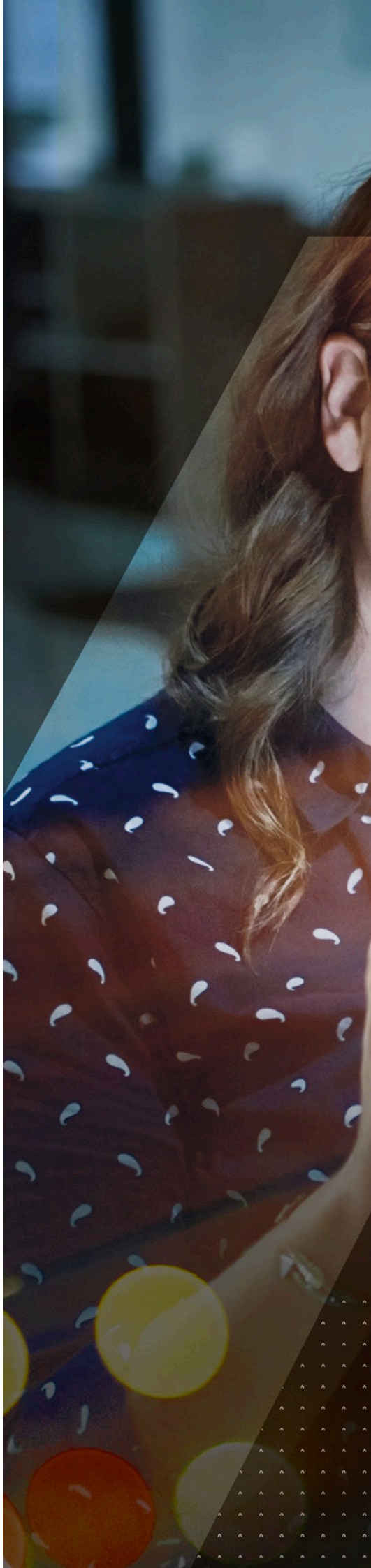
Mehr Informationen zu den Thales Access Management Lösungen finden Sie unter: thalesesecurity.com/thales-gemalto

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: asia.sales@thales-esecurity.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalesgroup.com <

© Thales - January 2020 • RMv3