



INFOBLATT

Grundlagen des Zugriffsmanagements

Was ist Cloud-Zugriffsmanagement und für wen eignet es sich?

Die Angst vor Cloud-Anwendungen

Cloud-Anwendungen sind hervorragend geeignet, um Unternehmen die besten Technologien zur Verfügung zu stellen – und zwar ohne Wartungsaufwand, mit sehr hoher Skalierbarkeit und einem schnellen Mehrwert. Die schnelle Bereitstellung und unmittelbare Produktivität von Cloud-Anwendungen sind jedoch mit Kosten verbunden. IT-Abteilungen verlieren den Überblick darüber, wer wann auf welche Anwendung mit welcher Authentifizierungsmethode zugreift. Und das gilt für IT-geprüfte Anwendungen ebenso wie für Schatten-IT-Anwendungen, die von einzelnen Abteilungen angeschafft und implementiert werden. Das Compliance-Risiko steigt, wenn Anwendungen über unterschiedliche Konsolen verwaltet werden. Außerdem hat der Helpdesk aufgrund von Passwort-Rücksetzungen alle Hände voll zu tun. Die wichtigste Person im ganzen Prozess – der Endanwender – leidet unter Passwirmüdigkeit, Ausfallzeiten und geringer Benutzerfreundlichkeit, denn die Verwaltung der zahlreichen Identitäten ist sehr aufwändig.

Grundlagen des Cloud-Zugriffsmanagements

Um Cloud-Anwendungen möglichst reibungslos implementieren zu können, gibt es Lösungen für die Zugriffsverwaltung, die die Bereitstellung und den Zugriff vereinfachen, Passwortprobleme für IT-Abteilungen und Anwender ausräumen, eine zentrale Ansicht der Zugriffsereignisse bereitstellen und dafür sorgen, dass die richtigen Zugriffskontrollen zum richtigen Zeitpunkt auf den richtigen Benutzer angewendet werden.

Einfach ausgedrückt: **Das Cloud-Zugriffsmanagement gewährleistet, dass der richtige Benutzer Zugriff auf die richtige Anwendung auf der richtigen Vertrauensstufe hat.**

Das Cloud-Zugriffsmanagement löst die Probleme, denen sich Unternehmen bei der umfassenden Einführung von Cloud-Lösungen gegenübersehen.

Vorteile des Zugriffsmanagements

Die Implementierung von Lösungen für das Cloud-Zugriffsmanagement erhöht die Zugriffssicherheit im Unternehmen, beseitigt Unklarheiten, die mit der Cloud-Sicherheit und Compliance-Risiken einhergehen, und erhöht die Benutzerzufriedenheit.

Unternehmen, die das Cloud-Zugriffsmanagement integrieren, profitieren im gesamten Unternehmen von den Vorteilen.

Höhere Benutzerfreundlichkeit

Lösungen für das Zugriffsmanagement bieten Cloud-Single-Sign-On, mit dem sich Benutzer nur einmal anmelden müssen, um Zugriff auf alle Cloud-Anwendungen zu erhalten. Sie nutzen dabei ihre vertraute Unternehmensidentität, die sie bereits jetzt verwenden. Das bedeutet, dass Benutzer nicht mehr für jede Cloud-Anwendung unterschiedliche Benutzernamen und Passwörter pflegen müssen, sondern nur noch eine Identität.

Optimierte-Cloud-Sicherheit

Mithilfe der Durchsetzung situationsbasierter Zugriffskontrollen mit detaillierten Richtlinien erhöhen Unternehmen die Sicherheit und senken das Risiko eines Datenschutzvorfalls. Durch die Berücksichtigung von Variablen wie privilegierten Benutzerkonten, der Sensibilität von bestimmten Anwendungen und kontextuellen Parametern können Administratoren die Zugriffsrichtlinien der Cloud an das jeweilige Szenario anpassen. Darüber hinaus ist der Zugriff für Anwender ganz einfach, da Richtlinien so definiert sind, dass nur bei Bedarf eine stärkere Authentifizierungsform eingefordert wird.

Einfache Verwaltung

Das Zugriffsmanagement bietet Administratoren einen zentralen Verwaltungspunkt und eine zentrale Übersicht, über die sie Zugriffsrichtlinien einmalig definieren und im gesamten Unternehmen durchsetzen können. Durch das Ersetzen mehrerer separater Cloud-Administrationskonsolen durch eine zentrale Konsole können IT-Abteilungen die Cloud-Nutzung skalieren und dabei gleichzeitig die Sicherheit und Transparenz aller Cloud-Lösungen aufrechterhalten.

Da die IT-Abteilungen nur eine Identität pro Benutzer für alle Cloud-Anwendungen verwalten müssen, sinkt der Helpdesk-Aufwand für Passwort-Rücksetzungen, der jährlich 20 % der Helpdesk-Anfragen ausmacht.

Viele Lösungen für das Zugriffsmanagement, die auf die Cloud ausgerichtet sind, vereinfachen die Integration neuer Cloud-Anwendungen, ermöglichen einen besseren Einblick in die Schatten-IT und vereinfachen die Einführung neuer Anwendungen, wenn sich die Geschäftsanforderungen weiterentwickeln.

Transparenz

Lösungen für das Zugriffsmanagement ermöglichen der IT die Beantwortung folgender Fragen: „Wer hat worauf Zugriff?“, „Wer hat wann und wie worauf zugegriffen?“ und „Wie wurde die Benutzeridentität verifiziert?“ Durch eine zentrale Sicht auf Zugriffseignisse und verwendete Authentifizierungsmethoden erhalten Unternehmen einen transparenten Einblick in die Cloud-Zugriffshistorie. Das wiederum vereinfacht Compliance-Audits und die Nachverfolgung von Aktivitäten.

Detaillierte Informationen über Anwendungszugriffe sparen Unternehmen zudem Kosten, da sie so erkennen können, welche Anwendungslizenzen unzureichend genutzt werden.

Zugriffsmanagement – das clevere Management für Cloud-Umgebungen

Lösungen für das Cloud-Zugriffsmanagement ermöglichen eine intelligente Verwaltung der Cloud-Anwendungen im gesamten Unternehmen. Durch die Bereitstellung des Single-Sign-On für Benutzer und die Nutzung granularer Zugriffsrichtlinien, die die richtige Authentifizierungsstufe zur richtigen Zeit durchsetzen, wird die Authentifizierung für alle Anwender problemlos und einfach möglich. So steigt die Benutzerfreundlichkeit. Das Zugriffsmanagement ersetzt die altmodischen binären Ja/Nein-Authentifizierungsentscheidungen und bedient die vielfältigen Herausforderungen des Sicherheitsmanagements und der Compliance im Unternehmen.

Kontakt: Eine Übersicht unserer Niederlassungen und die entsprechenden Kontaktdaten finden Sie unter safenet.gemalto.de/contact-us/.

Folgen Sie uns: blog.gemalto.com/security

 [GEMALTO.COM](https://gemalto.com)



Das Cloud-Zugriffsmanagement bietet Vorteile im gesamten Unternehmen:

- > Höhere Benutzerfreundlichkeit
- > Optimierte-Cloud-Sicherheit
- > Einfache Verwaltung
- > Transparenz

SafeNet Identity & Data Protection-Lösungen von Gemalto

Gemalto bietet Unternehmen eines der umfassendsten Portfolios für den Schutz kritischer Daten. Die Kunden profitieren vom branchenführenden Schutz ihrer Daten, digitalen Identitäten, Zahlungsvorgänge und Transaktionen. Durch die SafeNet-Lösungen für den Identitätsschutz von Gemalto können Unternehmen in zahlreichen vertikalen Märkten, z. B. Behörden und große Finanzinstitute, Lösungen für die Zugriffsverwaltung, das Management von PKI-Zugangsdaten, die leistungsstarke Authentifizierung und das Identitätsmanagement nutzen, um den Zugriff auf vertrauliche Daten sowie digitale Interaktionen zu schützen. 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.



gemalto
security to be free