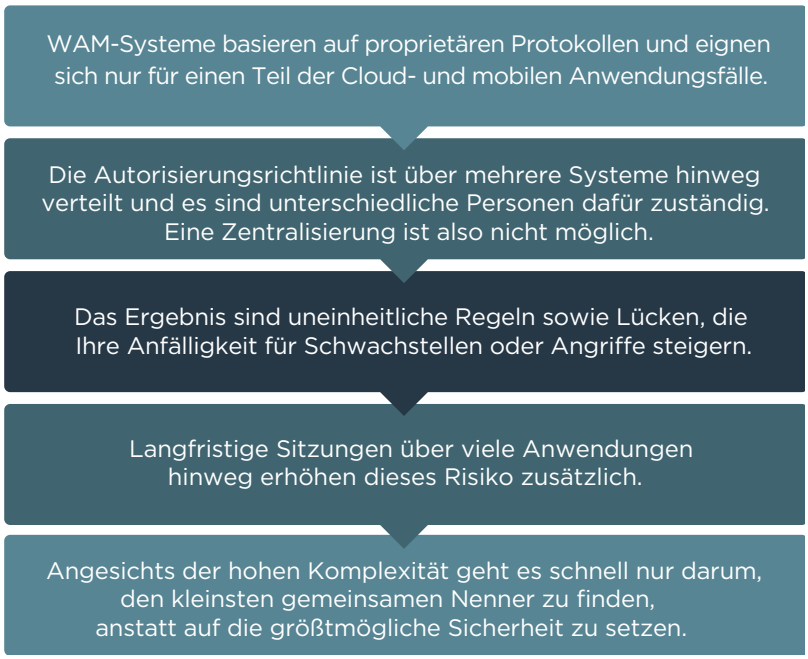
EXPERTEN-LEITFADEN: ACCESS-SECURITY

Wenn es Ihnen so geht wie vielen anderen Sicherheitsexperten, befinden Sie sich mitten in der digitalen Transformation. Jetzt, wo User und Anwendungen die Firewallgrenze zunehmend hinter sich lassen, müssen Sie Ihr digitales Unternehmen vor immer größeren Sicherheitsbedrohungen schützen – und zwar ohne die Produktivität zu beeinträchtigen oder Innovationen zu bremsen.

Vielleicht nutzen Sie ein älteres Web-Access-Management(WAM)-System, doch moderne Sicherheitsmaßnahmen können Sie damit nur mit erheblichem Aufwand ermöglichen. Im schlimmsten Fall setzen Sie Ihr Unternehmen großen Risiken aus.

WAM-Systeme eignen sich nicht für aktuelle Herausforderungen. Sie unterstützen keine Migration von Anwendungen in die Cloud und haben außerdem Schwierigkeiten mit mobilen Apps und APIs. Womöglich könnten Sie versuchen, Add-ons zu implementieren, doch das ist nicht nur ziemlich komplex, sondern erfordert auch viele Ressourcen. Zudem verursachen Sie damit einen Dominoeffekt und schaffen gefährliche Schwachstellen.

Probleme bei der Nutzung von WAM-Systemen für die moderne Sicherheit



Sie könnten natürlich alles beim Alten lassen. Aber ist das wirklich gut? Besser wäre es, eine Lösung zu finden, die speziell für die heutigen Herausforderungen konzipiert wurde. Sie sollte folgende Funktionen bieten:

- einen sicheren, zentralisierten, regelbasierten Zugriff für alle Nutzer auf alle Anwendungen – unabhängig davon, um welchen Typ von Anwendung es sich handelt oder wo sie sich befinden (Public Cloud, Private Cloud, lokal, Enterprise, Drittanbieter, mobil)
- ein Access-Management, das Benutzer-, Geräte- und Anwendungsdaten (z. B. Standort, Netzwerk und Gerätestatus) berücksichtigt und diese kontinuierlich überprüft
- eine zentralisierte Kontrolle von Identitätsdaten mit regelbasierter Data-Governance sowie Datenschutz- und Einwilligungsmanagement – und einem durchgängigen Schutz von Identitätsdaten
- eine hoch entwickelte, erweiterbare Plattform, die moderne IAM-Standards über verschiedene Anwendungsfälle mit Mitarbeitern, Partnern und Kunden hinweg umfassend unterstützt

Anders ausgedrückt: Um ein modernes Unternehmen zu schützen, brauchen Sie eine moderne Access-Security-Lösung.

01

MODERNISIERUNG MITHILFE VON IDENTITÄTEN

Wenn es darum geht, einen sicheren Zugriff über die Firewall hinaus zu gewähren, ist ein effizientes Identitätsmanagement die Lösung. Nur wenn Sie Ihre Webanwendungen und APIs mit ausgereiften Identitätsstandards – und modernen Authentifizierungs- und Autorisierungsprotokollen – schützen, können Sie den richtigen Benutzern einen sicheren und nahtlosen Zugriff auf die richtigen Ressourcen bieten.

Ein modernes Zugriffsmanagement erfordert einen dreigliedrigen Ansatz, um Usern einen sicheren Zugriff auf alle Apps und Ressourcen bereitzustellen:

1. **Single-Sign-On (SSO):** ersetzt sämtliche Passwörter mit einem einzigen Satz an Unternehmensanmeldedaten und einer durchgängigen Authentifizierungserfahrung
2. **Multifaktor-Authentifizierung (MFA):** bietet über Passwörter hinaus eine zusätzliche Sicherheitsschicht und ist ein Muss für das digitale Unternehmen
3. **Access-Security:** zentralisiert die Zugriffskontrolle mit einer regelbasierten Sicherheitsschicht für alle Webanwendungen, mobilen Apps und APIs

Moderne Access-Security-Lösungen bieten Ihnen die Möglichkeit, einen zentralen Zugriffspunkt einzurichten. Auf diese Weise behalten Sie die Kontrolle darüber, wer wie lange Zugriff auf welche Ressourcen erhält. Sie können Ihre Anwendungen lokal, in einer Private Cloud oder in der Public Cloud implementieren und dabei dasselbe Identitäts- und Access-Management-Konzept für alle drei verwenden. Das alles geht überaus schnell, sodass Sie neue Systeme innerhalb kurzer Zeit schützen und die digitale Transformation vorantreiben können.

Es ist verständlich, dass viele Unternehmen ihre alten Systeme weiterhin nutzen möchten. Doch WAM-Systeme – die aus einer Zeit stammen, in der es noch keine Cloud- und mobilen Anwendungen gab – sind eigentlich dafür ausgelegt, interne Webressourcen zu schützen, die in eigenen Datencentern gehostet sind. Die Kombination eines veralteten WAM-Systems mit API-Gateways bietet nur eine begrenzte Integration, ganz zu schweigen von der komplizierten Implementierung und Verwaltung. Das Ergebnis sind sperrige und wenig robuste Systeme, die intensive Systemintegrationsdienste für einfache Installationen und Updates erfordern und ein erhebliches Sicherheitsrisiko darstellen.

Fazit: Wenn Sie ein veraltetes System verwenden, um Aufgaben zu erledigen, für die es nicht konzipiert ist, bremsen Sie wichtige Innovationen und erhöhen zudem Ihre Kosten, Ihren Aufwand und Ihre Anfälligkeit für Angriffe.

02

EINHEITLICHE STANDARDS

Heute nutzen die meisten Organisationen eine passwortbasierte Authentifizierung und Autorisierung für APIs. Ohne standardisierte Identitätssysteme ergibt sich eine einfache, äußerst unsichere Interaktion:

USER » APP: Hallo, ich würde gerne meine Daten sehen.
APP » USER: Bitte melden Sie sich mit Benutzer-ID und Passwort an.
APP » API: Hallo, ich brauche Zugriff auf Service A, hier sind Benutzer-ID und Passwort.
API » APP: O. k., hier ist Service A.
APP » USER: Hier sind die Daten, die Sie angefordert haben.

Dieser Prozess läuft immer gleich ab, egal ob der Service, auf den zugegriffen wird, eine Social-Media-Site oder eine Cloud-App ist oder ob der Benutzer einen Desktop-PC, einen Laptop, ein Tablet oder ein Smartphone verwendet. Ein sicherer Zugriff auf APIs ist sowohl für Webanwendungen als auch für mobile Applikationen kritisch. Offensichtlich bietet diese Methode weder eine sichere Zugriffskontrolle noch flexible Optionen für den Zugriff.

Das OAuth-2.0-Protokoll löst dieses Dilemma, indem es Clients eine formale Art der Zugriffsanforderung für eine Ressource (eine API) bietet. Dazu muss der Client einfach einen Zugriffstoken vorlegen, der zuvor von einem Autorisierungsserver herausgegeben wurde. OAuth sieht drei Rollen in diesem Prozess vor:

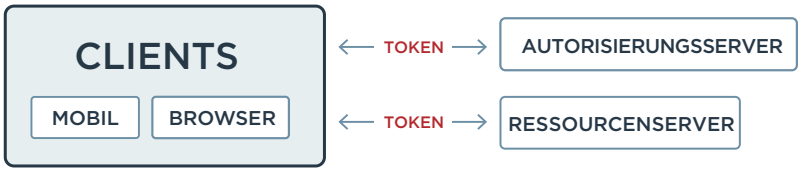


Abbildung 1: Das OAuth-2.0-Protokoll bietet eine formale Methode, wie Clients den Zugriff auf eine API anfordern können. Dazu muss der Client einfach einen Token vorlegen, der von einem Autorisierungsserver herausgegeben wurde.

CLIENT: in der Regel eine Anwendung (Web oder mobil), die auf eine bestimmte API zugreifen möchte
AUTORISIERUNGSSERVER: Server, der im Auftrag des Ressourcenservers Zugriffstoken und Refresh-Token herausgibt
RESSOURCENSERVER: Server, der Ressourcen hostet und schützt und für entsprechend authentifizierte und autorisierte Clients verfügbar macht

Wie in Abbildung 1 dargestellt, bieten moderne Access-Security-Lösungen, die OAuth unterstützen, eine sichere Methode, um einen Benutzer zu authentifizieren, die Genehmigung einzuholen und die Kontrolle über den Autorisierungsumfang zu ermöglichen – alles kritische Elemente, um einen sicheren Zugriff in modernen Unternehmen zu gewährleisten.

03

DYNAMISCHE ZUGRIFFSKONTROLLE AUF EBENE EINZELNER SEITEN

Die meisten Organisationen verwenden heute Anwendungen mit einer integrierten Autorisierungsebene. Dies kann die Verwaltung von Richtlinien schwierig, teuer und zeitaufwendig machen. Eine bessere Methode, um die Autorisierung zu verwalten, ist die Nutzung einer einzigen Kontrollebene, die die Zugriffsregelung für jede Anwendung und Anwendungsseite bestimmt.

Nehmen wir mal an, Sie haben eine Shopping-Anwendung mit einer Seite bzw. einem Bereich für Premiummitglieder. Wenn ein User klickt, um auf diese Seite zu gelangen, müssen Sie festlegen, ob diesem User der Zugriff gewährt werden sollte oder nicht. Eine moderne Zugriffssicherheitslösung schützt alle URLs mit einem Proxy/Gateway, der bzw. das die festgelegten Regeln umsetzt.
Diese Regeln sehen gewöhnlich in etwa so aus:

- prüfen, ob der Benutzer sich bereits angemeldet (authentifiziert) hat
- den Benutzer auffordern, sich zu authentifizieren, wenn er sich nicht bereits angemeldet hat
- nach der Authentifizierung die Benutzerattribute überprüfen, um zu bestimmen, ob der Benutzer durch die Regel dazu autorisiert ist, auf die Seite zuzugreifen
- bei sensiblen Seiten die Authentifizierung des Benutzers (falls autorisiert) durch die Multifaktor-Authentifizierung oder einen anderen Mechanismus hochstufen
- Seite anzeigen

Mit modernen Zugriffssicherheitslösungen können Sie die Regeln zentral auf mehrere Seiten oder Applikationen anwenden. Auf diese Weise können Sie die Zugriffsregeln für eine bestimmte Seite ändern, ohne die Anwendung zu modifizieren.

04

BESCHLEUNIGEN SIE IHRE CLOUD-MIGRATION

Mit einer modernen Access-Security-Lösung können Sie nicht nur einen sicheren Zugriff über verschiedene Anwendungen hinweg gewährleisten, sondern auch die Migration veralteter Anwendungen in Cloud-Umgebungen (wie Amazon Web Services) beschleunigen.

Durch eine schlanke, proxybasierte Architektur und zentral verwaltete Zugriffsregeln können Sie die Sicherheitsrichtlinie für Anwendungen beibehalten, die zuvor über WAM-Systeme wie CA SiteMinder oder Oracle Access Manager verwaltet wurden. Sobald die Anwendungen in das neue System migriert wurden, können Sie diese jederzeit ganz einfach in beliebige Umgebungen verschieben.

Das ist genau die responsive, flexible und schlanke Lösung, die Sie brauchen, um die aktuellen Sicherheitsherausforderungen zu meistern.

Einen sicheren Zugriff zu gewährleisten, war noch nie so schwer wie heute. Sie müssen es sich aber nicht noch schwerer machen. Ein effizientes Identitätsmanagement ist der Schlüssel, um den richtigen Usern einen sicheren und nahtlosen Zugriff auf die richtigen Ressourcen zu bieten.