gemalto
security to be free

E-BOOK

Zugriffsmanagement

Überlegungen zur Auswahl einer Lösung für das Zugriffsmanagement

Inhalt

Einführung	3
Überlegungen	4
WARUM	5
WER	7
WAS	8
WO	9
WANN	11
WIE	12
Schlussbemerkung	14

Einführung

Die unaufhaltsame Flut digitaler Technologien hat zwar die Art und Weise vereinfacht, wie wir Geschäfte machen, stellt aber für Unternehmen dennoch ein gewisses Risiko dar. Mit Daten ist Geld zu machen, und Hacking ist ein rentables Geschäft. Viele Hackerangriffe zielen nicht nur auf Finanzdaten ab, sondern auch auf Daten von Kunden und Mitarbeitern oder Konstruktionspläne. Im Grunde lässt sich jeder digitale Datensatz stehlen und zu Geld machen. Sicherheitsadministratoren stehen oft vor dem Problem, vertrauliche Unternehmensdaten zuverlässig zu schützen und zu sichern, ohne dabei deren Nutzbarkeit und den Benutzerzugriff zu beeinträchtigen. Unsere Marktanalyse zeigt, dass immer mehr Unternehmen auf Lösungen für das **Identity & Access Management** (IAM) setzen, um diesem Problem zu begegnen. Der Benutzer selbst wird zum neuen IT-Perimeter.

Gartner definiert IAM als „die Sicherheitsdisziplin, die den richtigen Personen Zugriff auf die richtigen Ressourcen zur richtigen Zeit aus den richtigen Gründen gewährt." Tatsächlich gibt es aber so einiges zu berücksichtigen, wenn es darum geht, die geeignete Lösung zu finden, die alle Unternehmensanforderungen erfüllt. Bei der Implementierung der richtigen IAM-Lösung in Ihrem Unternehmen sollten Sie zunächst alle Komponenten kennen.

Überlegungen

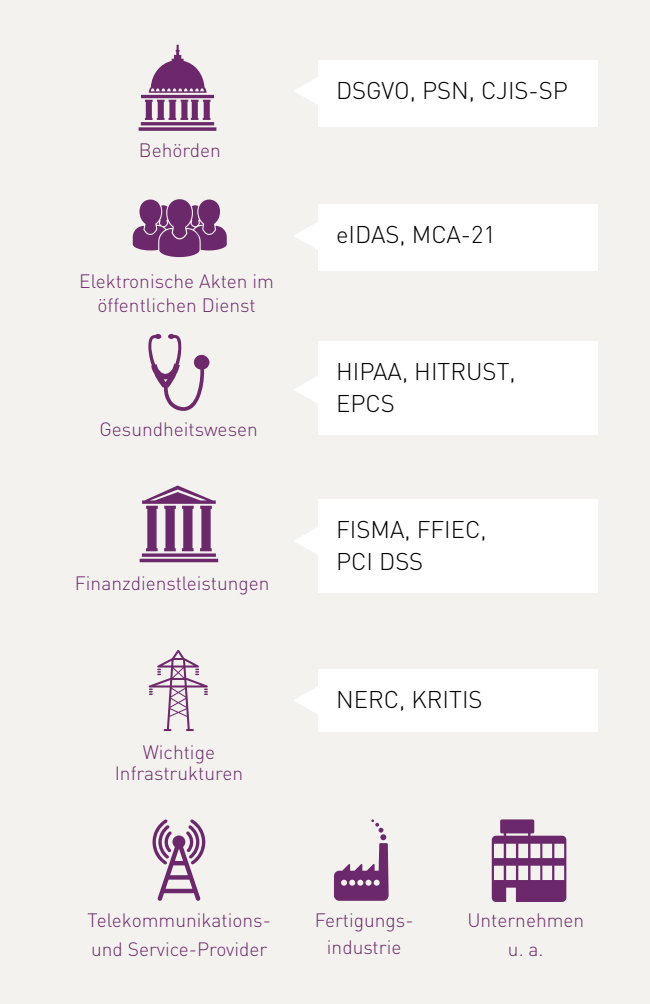
Bei komplexen Projekten dieser Größenordnung schadet es nicht, wenn man sich wieder auf gewisse Grundwerte besinnt, die wir schon in der Schule gelernt haben: die sechs Ws. Anhand dieser Methode wollen wir uns einige der wichtigsten Punkte anschauen, mit deren Hilfe Ihr Unternehmen eine Lösung implementieren kann, die sämtliche Anforderungen erfüllt.

In jedem der folgenden Abschnitte finden sich neben Informationen von Entscheidungsträgern verschiedener Unternehmen auch Fragen, die sich bei der Auswahl der geeigneten IAM-Lösung stellen. Fangen wir damit an, WARUM Ihr Unternehmen eine IAM-Lösung benötigt.

Frage	Thema
WARUM	Warum möchten Sie eine Lösung für das Zugriffsmanagement einführen?
WER	Wer benötigt eine zusätzliche Sicherheitsebene?
WAS	Welche Anwendungen und Ressourcen sollen geschützt werden?
WO	Wo befinden sich Anwendungen und Benutzer?
WANN	Wann soll die Lösung implementiert werden?
WIE	Wie möchten Sie Ihre Benutzer schützen?

WARUM

Im Folgenden klären wir, WARUM ein Unternehmen ein Zugriffsmanagement braucht: Welche aufsichtsbehördlichen Vorgaben müssen Sie für Ihre Daten einhalten? Gab es bereits einen Datenschutzvorfall oder sind Sie besonders gefährdet? Möchten Sie eine hybride Umgebung schützen? Gibt es von Seiten der Führungsebene strengere Kontrollen? Weiten Sie den Zugriff auf Personen außerhalb Ihres Unternehmens aus? Möchten Sie eine Single-Sign-On (SSO)-Lösung implementieren?

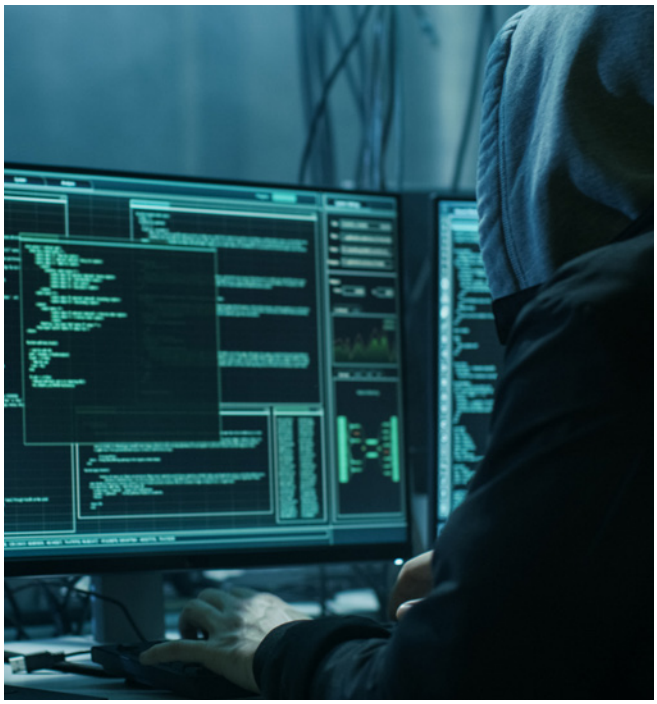


Compliance

Möglicherweise muss Ihr Unternehmen bestimmte aufsichtsbehördliche Vorschriften einhalten. Gesetzliche Vorgaben, die eine Multi-Faktor-Authentifizierung zum Schutz des Remote-Zugriffs auf Unternehmensnetzwerke vorschreiben, sind z. B. Public Services Network (PSN) im Vereinigten Königreich, PCI DSS V 3.2 für Finanzdienstleister rund um den Globus, NERC-CIPC in den USA (North American Electric Reliability Corporation Critical Infrastructure Protection Committe) sowie eIDAS bzw. IVT in der Europäischen Union, die ein Rahmenwerk für die grenzüberschreitende elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im EU-Binnenmarkt schafft. Zahlreiche dieser Vorschriften besagen, dass Unternehmen für den für den Zugriff auf vertrauliche Anwendungen und Daten Audits und Berichte benötigen. Eine leistungsstarke IAM-Lösung verfügt über geeignete Berichts- und Nachverfolgungsfunktionen und ermöglicht so eine vollständige Transparenz für die gesamte Infrastruktur mittels einer zentralen Übersicht. Viele Richtlinien verfügen zudem über strikte zeitliche Vorgaben, die im Abschnitt WANN genauer beschrieben werden.

Datenschutzverletzung

Oft werden IAM-Lösungen aufgrund des Risikos einer Datenschutzverletzung eingeführt. Dieses Risiko hat oberste Priorität. Unternehmen rund um den Globus erhöhen ihre Sicherheitsvorkehrungen, um sich vor kostspieligen Datenverlusten zu schützen. Die Kosten eines Datenlecks überschreiten die Bereitstellungskosten einer IAM-Lösung um ein Vielfaches. Einer aktuellen Cloud-Studie zufolge sagen neun von zehn befragten Entscheidungsträgern in der IT, dass die Sicherheitsrichtlinien in ihrem Unternehmen für das Zugriffsmanagement durch Datenschutzverletzungen bei Verbraucherangeboten beeinflusst wurden. Das zeigt deutlich, welche Bedeutung Datenlecks beizumessen ist.



Unser Bericht zum Breach Level Index von 2017 zeigt auf, dass 1,9 Mio. Datensätze durch Zutun der Benutzer offengelegt wurden. Benutzer gelten in jedem Unternehmen als das schwächste Glied in der Kette, wenn es um Sicherheit geht. Bei der Auswahl einer IAM-Lösung sollten Unternehmen auf ein Angebot setzen, dass das Hauptaugenmerk auf die Authentifizierung und Autorisierung von Benutzern legt. Dieser Aspekt wird in den Abschnitten WER und WIE genauer beschrieben.

Cloud auf dem Vormarsch

Unsere aktuelle globale Umfrage zur Cloud-Datensicherheit, die wir zusammen mit dem Ponemon Institute durchgeführt haben, ergab, dass Unternehmen im Schnitt 27 Cloud-Anwendungen nutzen. Diese Angebote sind zwar praktisch, stellen aber ein Sicherheitsrisiko dar, da diese Ressourcen nicht mehr intern kontrolliert werden. Darüber hinaus ist es wichtig zu wissen, WAS in Ihrer Umgebung geschützt werden soll. Die Lösung sollte verschiedene Integrationsmöglichkeiten bieten, die zudem eine Ausweitung des Schutzes auf hybride Umgebungen erlauben. Viele Cloud-Anwendungen unterstützen die SAML-Authentifizierung. Die IAM-Plattform sollte daher über eine SAML-Integration verfügen, um eine leichte Bereitstellung zu ermöglichen.

Benutzererfahrung

SSO-Lösungen sind so beliebt, weil sie sehr benutzerfreundlich sind. Da Unternehmen immer mehr Anwendungen einsetzen, wird es für Benutzer schwierig, sich jeden einzelnen Benutzernamen nebst Passwort zu merken. Bei der einfachsten Form des SSO hat der Benutzer einen Zugangsdatensatz, der ihm Zugriff auf alle benötigten Ressourcen gewährt. Das ist jedoch mit einem Risiko verbunden: Wird dieser Zugangsdatensatz ausgespäht, können sämtliche Daten offengelegt werden. Die IAM-Lösung sollte eine ähnlich einfache Benutzeranmeldung wie das SSO aufweisen, ohne allerdings die Sicherheit vertraulicher Daten zu beeinträchtigen. Sie sollten die Möglichkeit haben, Richtlinien für die Durchsetzung einer leistungsstarken Authentifizierung zu erstellen, die darauf aufsetzt, WER WANN und WO eine Zugriffsanfrage stellt.

Einfache Implementierung

Die Lösung sollte außerdem vielseitig und skalierbar sein, damit sie mit Ihrem Unternehmen mitwachsen kann und auch künftige Anforderungen im digitalen Zeitalter erfüllt. Erwägen Sie einen IAM-Anbieter, der eine Cloud-Lösung im Programm hat. Der Vorteil von IDaaS bzw. einer cloud-basierten Plattform für das Zugriffsmanagement ist, dass sie Audits gemäß ISO 27001:2013 bzw. SOC2 erfolgreich bestanden haben. Zudem sinken die Gesamtbetriebskosten (TCO) für Ihr Unternehmen. Cloud-Lösungen sind flexibel und erlauben Unternehmen den Schutz von Ressourcen unabhängig davon, WO sie sich befinden.

Entscheiden Sie sich daher für eine **Zugriffsmanagementlösung**, die sich schnell und unkompliziert bereitstellen lässt. Sie sollte darüber hinaus bei der Konsolidierung der Verwaltung von Zugriffsrichtlinien für alle Anwendungen in der Umgebung helfen. Ein leistungsstarkes System erhöht die Produktivität im gesamten Unternehmen, während gleichzeitig die Komplexität Ihrer Sicherheitslösung sinkt und sämtliche Benutzer zuverlässig geschützt werden. Die Vorteile einer flexiblen, leistungsstarken IAM-Lösung liegen auf der Hand: mehr Sicherheit, Validierung von Benutzern, Konsolidierung von Anwendungszugriffen und Einhaltung gesetzlicher Vorgaben.

WER

Sehr umfangreiche IAM-Lösungen unterstützen Unternehmen falls erforderlich bei der Anwendungsverwaltung und der Durchsetzung einer starken Authentifizierung. Dabei werden geltende Zugriffsrichtlinien natürlich eingehalten.

Wenn es um das WER geht, sollten Sie an Ihre Benutzer denken – vom CEO über den IT-Administrator bis hin zum Empfangspersonal. Sie alle nutzen Unternehmensressourcen und sind die größte Sicherheitslücke im gesamten Netzwerk.

Außerdem stellen Benutzer die anspruchsvollste und schwierigste Komponente in Ihrer Infrastruktur dar, wenn es um die Verwaltung geht. Wir möchten schnell und problemlos auf unsere Systeme und Daten zugreifen können, und zwar unabhängig davon, wo wir gerade sind. Das ist Segen und Fluch zugleich. Ihr Sicherheitsteam muss ein Gleichgewicht zwischen Benutzerfreundlichkeit und Sicherheit schaffen. Das ist keine leichte Aufgabe. Überlegen Sie also, wer Ihre Benutzer sind. Handelt es sich ausschließlich um interne Anwender? Arbeiten Sie mit externen Mitarbeitern zusammen? Haben Sie mehrere Standorte? Sind viele Mitarbeiter oft auf Reisen? Müssen Sie den Zugriff für bestimmte Benutzergruppen sperren? Verfügen Sie bereits über eine sichere SSO-Lösung?

Wenn Sie Ihre Benutzer kennen, können sie besser entscheiden, welche Zugriffskontrollen Sie benötigen. Benutzer mögen SSO, da sie so ihre Zugangsdaten nur einmal eingeben müssen, um Zugriff auf alle nötigen Ressourcen zu erhalten. Dennoch sollten Sie sich für eine Lösung entscheiden, mit der Sie Zugriffsrichtlinien für bestimmte Benutzergruppen definieren können. Bei herkömmlichen SSO-Lösungen besteht immer noch das Risiko, dass Hacker sich durch kompromittierte Zugangsdaten leicht Zugriff auf Ihre Unternehmensumgebung verschaffen können.

Die Lösung sollte es Ihnen ermöglichen, die für den Zugriff erforderliche Authentifizierung bzw. Autorisierung im Bedarfsfall verschärfen zu können. Für Benutzer im Unternehmensnetzwerk ist eine andere Authentifizierung erforderlich als für Zugriffe von außerhalb. Die verschiedenen Authentifizierungsarten werden im Abschnitt WIE genauer erläutert.

Des Weiteren sollte die implementierte Lösung über Richtlinien verfügen, die sich an Ausnahmen, Risikobewertungen, Einschränkungen und Ausschlüsse und damit die verschiedenen Anwendungsszenarien in Ihrem Unternehmen anpassen lassen. Setzen Sie auf eine Lösung, die sich schnell und einfach adaptieren lässt. So können Sie die Administrationskosten selbst in komplexen Umgebungen im Rahmen halten.

Wenn feststeht, WER auf die Ressourcen in Ihrer Umgebung zugreift, müssen Sie eruieren, auf WAS zugegriffen wird.

WAS

In vielen Unternehmen gibt es unzählige Anwendungen und Ressourcen, ohne die der Geschäftsbetrieb nicht möglich wäre. Die Verwaltung und Pflege von Sicherheitsrichtlinien und Benutzerzugangsdaten für jede einzelne Anwendung wird schnell zur Mammutaufgabe. Berücksichtigen Sie den Aufbau Ihrer Infrastruktur. Was soll geschützt werden? Was wird bereits geschützt? Nutzen Sie Cloud-Anwendungen? Nutzen Sie noch ein VPN? Verwenden Sie VDI-Lösungen? Nutzen Sie ältere, maßgeschneiderte Lösungen? Verfügen Sie über ein Webportal für Benutzer?

Früher ging es hauptsächlich darum, die Unternehmensinfrastruktur zu sperren und sämtliche Daten in einer sicheren, physikalischen Serverfarm vorzuhalten, auf die nur Personen innerhalb des Netzwerks Zugriff hatten. Mitarbeiter, die von Zuhause arbeiteten, haben über eine sichere Remote-Verbindung auf das Netzwerk zugegriffen, die in der Regel eine Multi-Faktor-Authentifizierung benötigte.

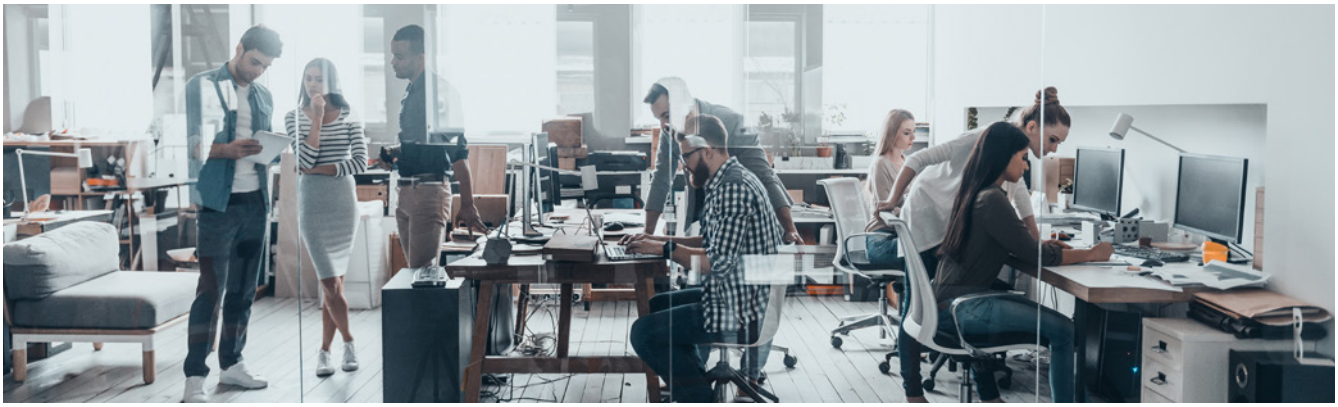
In modernen, hybriden Umgebungen gibt es sowohl Cloud- als auch Vor-Ort-Anwendungen, die geschützt werden müssen. Die eingesetzte IAM-Lösung sollte flexibel genug sein, damit Sie sämtliche Anwendungen integrieren und die Zugriffskontrolle und Authentifizierung auf Anwendungen ausweiten können, die keine native Unterstützung aufweisen. Viele Cloud-Anwendungen unterstützen die SAML-Authentifizierung. Die IAM-Plattform sollte daher über eine SAML-Integration verfügen, um eine leichte Bereitstellung zu ermöglichen.

Sie werden schnell feststellen, dass die Kombination aus einer leistungsstarken IAM-Lösung mit einer modernen Firewall oder Appliance zur Anwendungskontrolle den besten Schutz bietet. Die Lösung sollte die bestehende Umgebung ergänzen, damit möglichst wenig Veränderungen vorgenommen werden müssen.

Die IAM-Lösung sollte es Ihnen ermöglichen, alle Anwendungen in eine zentrale Verwaltungsplattform zu integrieren und Richtlinien auf der Basis Ihrer Geschäftsanforderungen durchzusetzen. Mit einer ausreichend flexiblen Lösung können Sie Zugriffsrichtlinien nur für bestimmte Anwendungen oder gleich die gesamte Umgebung festlegen. Darüber hinaus sollte die Lösung konsolidierte Berichte für Compliance-Audits erstellen, die besagen, WER auf WAS zugegriffen hat. Durch die zentrale Verwaltung sinken die Gesamtbetriebskosten für die Lösungsimplementierung. Außerdem lassen sich Änderungen in der gesamten Infrastruktur schnell und einfach vornehmen.

Es ist aber nicht nur wichtig, WER und WAS geschützt wird; auch WO und WANN Zugriffe erfolgen, ist von Bedeutung.

WO



In der modernen Geschäftswelt findet man nur selten Unternehmensumgebungen, die isoliert sind, sich auf einen einzigen Standort beschränken oder zentral agieren. Wenn Sie ein zentrales Unternehmen verwalten, gibt es immer noch externe Faktoren, die bei einer IAM-Implementierung in Betracht gezogen werden müssen. Oft ist es nämlich so, dass die kleinsten Umgebungen die größte Komplexität aufweisen.

Die implementierte Lösung sollte nicht nur berücksichtigen, WER und WAS geschützt werden muss, sondern darüber hinaus Zugriffskontrollen dafür ermöglichen, von WO die Zugriffe erfolgen.

Ganz gleich, ob Sie in einem internationalen Konzern oder in einem kleinen regionalen Unternehmen tätig sind, ist Ihr Budget sicherlich begrenzt, und die IT arbeitet an mehreren Projekten gleichzeitig. Mitarbeiter müssen mit weniger Budget mehr leisten – und das, obwohl Studien zeigen, dass viele Unternehmen für Zugriffsmanagementlösungen höhere Budgets veranschlagen.

Unserem Identity & Access Management Index 2018 zufolge sind die Ausgaben für das Zugriffsmanagement um 45 % gestiegen. Mitarbeiter sind noch immer mit strengen Projektzeitplänen konfrontiert. Gerade deshalb sollte eine IAM-Lösung leicht zu implementieren und zu verwalten sein. Beachten Sie dies, wenn Sie darüber nachdenken, WANN die Lösung und das Budget bereitgestellt werden sollen.

In Bezug auf das WO gibt es auch einige Punkte, die in Betracht gezogen werden müssen. Wo befinden sich Ihre Anwendungen? Wo sind Ihre Benutzer? Haben Sie mehrere Standorte? Nutzen Ihre Mitarbeiter einen Remote-Zugriff? Arbeiten Ihre Mitarbeiter mobil? Sind Sie in bestimmten Ländern tätig? Erlauben Sie den mobilen Zugriff auf Daten? Wie sorgen Sie für Überwachung und Schutz von Traffic aus Ländern, in denen Sie gar keine Mitarbeiter haben?

Mitarbeiter sind heute deutlich flexibler und mobiler als je zuvor und benötigen einen standortunabhängigen Zugriff auf Unternehmensressourcen. Viele Benutzer sind nur selten im Büro und haben nicht immer die Zeit, das Notebook einzuschalten, eine VPN-Verbindung herzustellen und sich am Unternehmensnetzwerk anzumelden, um auf die benötigten Dokumente zuzugreifen. Angesichts dieser Tatsache sollte die IAM-Lösung einen einfachen Zugriff ermöglichen, ohne dabei die Sicherheit zu gefährden.

Mobile Mitarbeiter und solche, die eine Remote-Verbindung nutzen, sollten über ein benutzerfreundliches Portal auf alle Anwendungen zugreifen können. Für sensible Daten kann hier eine leistungsstarke Authentifizierung eingerichtet werden. Die flexible Authentifizierung ist ein zentraler Aspekt, auf den zu einem späteren Zeitpunkt eingegangen wird, wenn wir besprechen, WIE die IAM-Lösung implementiert und umgesetzt wird.

...der Benutzer in den befragten Unternehmen benötigen im Schnitt Remote-Zugriff auf Unternehmensanwendungen.

43 %

Dem Identity & Access Management Index 2018 zufolge schützen nur 43 % der Befragten externe Benutzer durch leistungsstarke Authentifizierung. Rund neun von zehn Befragten gaben an, dass ihr Unternehmen den Zugriff auf Daten über Mobilgeräte zu einem gewissen Grad einschränkt. Bedenklicherweise sagen nur 35 %, dass es diesbezüglich umfassende Einschränkungen gibt.

Die Lösung sollte Ihnen die Möglichkeit bieten, spezielle Richtlinien für verschiedene Benutzer festzulegen – je nachdem, ob diese intern im Büro, extern oder über ein Mobilgerät zugreifen. Für Zugriffsanfragen von außen sollten striktere Kontrollen gelten, damit Identität und Herkunft der Anfrage validiert werden können.

Wenn externe Benutzer in bestimmten Ländern tätig sind, sollte der Zugriff für Benutzer an diesen Standorten eingeschränkt werden. Entsprechend gilt es, Zugriffsanfragen von unerwünschten Standorten einzuschränken oder abzulehnen.

Die Lösung sollte Ihnen transparent vermitteln, woher Zugriffsanfragen kommen, und über entsprechende Richtlinien verfügen, die das Risiko für bestimmte Zugriffe bewerten können. Durch verschiedene Zugriffsrichtlinien und Authentifizierungsanforderungen von vertrauenswürdigen bzw. nicht vertrauenswürdigen Personen und Standorten wird ein Gleichgewicht zwischen Nutzbarkeit und Sicherheit hergestellt. Durch die Möglichkeit, Anfragen von Mobilgeräten oder aus unerwünschten Ländern abzuweisen, können Sie vorhandene Netzwerkkontrollen stärken. Die IAM-Lösung sollte ebenso vielseitig sein wie Ihr Unternehmen.

WANN

Bei der Implementierung neuer Sicherheitsrichtlinien bzw. -regeln stellen Projektzeitpläne in der Regel das größte Hindernis dar. Überlegen Sie daher, ob es bestimmte Fristen gibt, die Sie aus Compliance-Gründen einhalten müssen. Wie lauten Ihre internen Ziele für die implementierte Lösung? Welche anderen laufenden Projekte müssen berücksichtigt werden? Steht ein Sicherheits-Audit bevor? Gibt es eine Frist für das verfügbare Budget?

Da immer mehr Unternehmen Cloud-Anwendungen nutzen, ist es nur folgerichtig, über eine cloud-basierte IAM-Lösung von einem Anbieter nachzudenken, der IDaaS im Portfolio hat. Bei cloud-basierten Lösungen sind die Infrastrukturinvestitionen niedriger und sie lassen sich in der Regel in allen Unternehmen unabhängig von deren Größe schnell implementieren. Eine leistungsstarke Sicherheitslösung, die eine Automatisierung und umfangreiche Zugriffsrichtlinien unterstützt, ist optimal und lässt sich mit nur wenigen IT-Mitarbeitern implementieren. Wenn Sie die zeitlichen Vorgaben für Budget und Implementierung kennen, können Sie den Umfang der zu erwägenden Lösungen weiter eingrenzen.

Jede Infrastruktur beinhaltet zahlreiche Komponenten und Anwendungen. Setzen Sie daher auf eine Lösung, die vorlagenbasierte Integrationsmöglichkeiten bietet, um eine schnelle und reibungslose Bereitstellung zu ermöglichen. Ihre IAM-Lösung sollte darüber hinaus die Möglichkeit einer Integration mit SAML 2.0, RADIUS oder APIs haben, damit alle Technologien in Ihrer Umgebung geschützt werden können.

Die Implementierung einer Lösung, die sich leicht in vorhandene Authentifizierungsverfahren integrieren lässt, z. B. zertifikatbasierte Authentifizierung oder PKI, senkt den Zeitaufwand für die Bereitstellung der Authentifizierungsverfahren für Benutzer und sorgt für eine höhere Akzeptanz.

Bei der Bereitstellung einer IAM-Lösung ist es besonders wichtig zu überlegen, WIE die Lösung implementiert wird und WIE Sie Ihre Benutzer schützen.

WIE

Es gibt zahlreiche Lösungen, die Single-Sign-On (SSO) und föderierte Identitäten unterstützen. Das können IDaaS-Lösungen, kostenlose Angebote oder Systeme sein, bei denen vor Ort in Zeit und Ressourcen investiert werden muss. Überlegen Sie, welche Vorteile jede einzelne Lösung für Ihr Unternehmen bietet. Fragen Sie sich auch, WIE diese Lösungen implementiert werden und WIE Sie den Schutz in Ihrem Unternehmen verbessern.

SSO-Lösungen galten einst als Utopie in der Geschäftswelt. Mittlerweile gelten sie als leicht zu verwalten und benutzerfreundlich und bieten Vorteile für alle Beteiligten. Bedenken Sie aber, dass viele SSO-Lösungen von Haus aus nur statische Passwörter unterstützen. Hier ist eine zusätzliche Investition zur Implementierung einer starken Zwei-Faktor-Authentifizierung erforderlich (die von vielen aufsichtsbehördlichen Vorgaben verlangt wird). Tatsächlich haben sich Passwörter unabhängig von ihrer Komplexität und strengen Passwortrichtlinien als wenig sicher erwiesen.

Laut dem Data Breach Investigations Report von Verizon waren 81 % der Datenschutzverletzungen 2017 auf gestohlene oder schwache Passwörter zurückzuführen[1]. 2016 waren es nur 63 %. Einige Lösungen mit Multi-Faktor-Authentifizierung sind eingeschränkt oder nutzen Authentifizierungsverfahren von Drittanbietern.

Wählen Sie eine Lösung, die alle Authentifizierungsverfahren unterstützt und die nachweislich Erfolge im Bereich der starken Authentifizierung vorzuweisen hat. Darüber hinaus sollten Sie die gewünschte Authentifizierungsmethode selbst auswählen können. Als Basis gelten hier das WER, WAS und WO für Zugriffsanfragen. Kommen wir nun dazu, WIE Sie Ihre Zugriffsmanagementlösung schützen.

Hier sollten Sie unbedingt erwägen, wie die Benutzerauthentifizierung für Anwendungen und Ressourcen erfolgt. Nutzen Sie immer noch Passwörter? Verfügen Sie über strikte Passwortrichtlinien? Verwenden Sie bereits Hardware- oder Software-Token für die starke Authentifizierung? Welche Art der Authentifizierung möchten Sie nutzen? Unterstützen Ihre Software-Token die Out-of-Band-Authentifizierung?

Benutzer sollten leicht auf Systeme zugreifen können. Ist das nicht der Fall, führt das zu großer Frustration auf Anwenderseite. Benutzer werden sich beschweren und gegen andere Verfahren als das herkömmliche Passwort wehren.

Das wiederum ist interessant, wenn man bedenkt, dass 20 % aller Helpdesk-Anfragen auf das Rücksetzen verloren gegangener oder vergessener Passwörter zurückzuführen sind.

Keine Umgebung ist homogen. Es ist sehr wahrscheinlich, dass Sie verschiedene Authentifizierungsmöglichkeiten für Ihre Benutzer anbieten müssen. Eine weitere Frage, die sich stellt: Wie verwalten und pflegen Sie den Lebenszyklus

von Token möglichst effizient? Die Lösung sollte den Token-Lebenszyklus automatisch verwalten und zudem bewährte Verzeichnispasswörter und Zertifikate unterstützen. Die IAM-Lösung sollte Sicherheitskontrollen vereinfachen und den Aufwand für Ihre IT senken. Lösungen mit Automatisierung und einer Self-Service-Verwaltung für Token werden von Benutzern eher akzeptiert.

Bei der Multi-Faktor-Authentifizierung erfreut sich der Software-Token der größten Beliebtheit. Es handelt sich hier um eine auf einem Gerät installierte Anwendung, mit deren Hilfe der Benutzer einen einmalig gültigen Passcode (OTP) generiert, der für Authentifizierungsanfragen genutzt wird.

1 https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

Für diese Art Token unterstützen mobile Anwendungen Push-Benachrichtigungen und Out-of-Band (OOB)-Authentifikatoren. So müssen Benutzer kein Passwort mehr eingeben, sondern lediglich noch in der Anwendung auf „Erlauben" klicken. Das erhöht die Benutzerfreundlichkeit enorm und sorgt gleichzeitig für eine äußerst hohe Sicherheit. Möglich wird dies durch Token, die verschlüsselte kryptografische Bibliotheken verwenden, die über eine sichere Verbindung mit der IAM-Plattform kommunizieren und den Benutzer authentifizieren bzw. die Identität validieren.

Durch dieses Authentifizierungsverfahren wird bei der Anfrage übermittelt, von welcher Anwendung sie stammt. Außerdem gibt es einen Audit-Trail in der Management-Plattform. Auf diese Weise können Benutzer leichter erkennen, ob ihre Zugangsdaten einem Hackerangriff zum Opfer gefallen sind. Des Weitern können IT-Administratoren die Benutzerauthentifizierung und Zugriffsaktivitäten nachverfolgen und somit auch verdächtige Vorgänge überwachen.

Vielleicht nutzt Ihr Unternehmen bereits eine zertifikatbasierte Authentifizierung oder eine PKI-Lösung. Durch eine Lösung, die sich in solche vorhandenen Authentifizierungsverfahren integrieren lässt, erhöht sich die Akzeptanz seitens der Benutzer, da diese selbst für hybride Anwendungen eine vertraute Authentifizierungsmethode nutzen können.

Sie können die Akzeptanz durch ein benutzerfreundliches Portal weiter erhöhen, in dem alle Unternehmensressourcen zentral hinterlegt sind. Der Schutz erfolgt über eine Anmeldung mit starker Authentifizierung. Durch die Möglichkeit, Anwendungen bestimmten Benutzergruppen zuzuordnen, wird sichergestellt, dass Benutzer nur auf die Ressourcen zugreifen, für die sie entsprechende Rechte besitzen. So steigt die Benutzerzufriedenheit. Außerdem müssen keine Lesezeichen im Browser mehr angelegt werden, da alle benötigten Anwendungen zentral zugänglich sind. Ganz nebenbei steigt auch noch die Produktivität.

Das Single-Sign-On für kann über ein Benutzerportal erfolgen. Idealerweise sollten Sie Ihre Sicherheitsrichtlinien so festlegen, dass für bestimmte Szenarien, Benutzergruppen oder sensible Anwendungen im Portal eine stärkere Authentifizierung erforderlich ist. Dabei sollte die Benutzererfahrung jedoch nicht beeinträchtigt werden. Ebenfalls sollten Sie überlegen, ob Kontrollen für bestimmte Authentifizierungsverfahren und ggf. eine kombinierte Authentifizierung eingerichtet werden sollen, je nachdem, von wo aus der Benutzer auf das Portal zugreift.

Durch eine flexible IAM-Plattform, die verschiedene Authentifizierungsverfahren unterstützt, können Sie Benutzer durch eine sichere Authentifizierung validieren. Diese kann mehrere Stufen aufweisen, ermöglicht aber dennoch den einfachen Zugriff auf Ihre Umgebung. Ihr Unternehmen ist nicht statisch; Ihre Anforderungen werden sich mit der Zeit ändern. Daher sollte die Lösung möglichst flexibel sein und es Ihnen ermöglichen, Richtlinien und Anforderungen nach Bedarf anzupassen.

Das Hinzufügen neuer Anwendungen und Benutzer, das Ändern von Authentifizierungsverfahren und die Verwaltung von Token-Lebenszyklen sollte IT-Mitarbeiter nicht zusätzlich belasten. Sie benötigen also eine Lösung, die sich einfach verwalten, pflegen und implementieren lässt.

Schlussbemerkung

Die Implementierung einer Lösung für das Zugriffsmanagement muss keine Mammutaufgabe sein. Dennoch sollte Ihr Unternehmen die eigenen Anforderungen genau kennen und sicherstellen, dass die Lösung für die jeweiligen Anwendungsfälle und die Geschäftsanforderungen Ihrer Infrastruktur geeignet ist.

Wenn Sie Ihr Unternehmen und Ihre Anforderungen vor der Implementierung einer IAM-Lösung genau kennen, steigt die Sicherheit in Ihrer gesamten Umgebung. Zudem können Sie die Lösung implementieren, ohne die Benutzer zu beeinträchtigen, wodurch wiederum die Akzeptanz der neuen Lösung steigt.

Setzen Sie auf eine Lösung, die verschiedene starke Authentifizierungsverfahren unterstützt und über eine zentrale Management-Konsole mit umfangreichen und leicht konfigurierbaren Richtlinien für die Zugriffskontrolle verfügt. Die ideale Lösung ist benutzerfreundlich und beeinträchtigt die Sicherheit nicht. Sie hilft Ihrem Unternehmen dabei, aufsichtsbehördliche Vorgaben einzuhalten und verschiedene Sicherheitsstufen zu bedienen.

Die Gemalto-Lösungen für das Zugriffsmanagement helfen Ihnen bei der Einhaltung aufsichtsbehördlicher Vorgaben. Unsere gehostete Lösung SafeNet Trusted Access für das Zugriffsmanagement sorgt schnell und einfach für den Schutz Ihrer Umgebung.

Verwaltung und Schutz des Zugriffs auf alle Anwendungen
Risikoverwaltung durch Unternehmensrichtlinien und zentraler Einblick in alle Zugriffsereignisse

Verwaltung des App-Zugriffs über einen zentralen Cloud-Service
Implementierung konsistenter Zugriffskontrollrichtlinien für alle Cloud-Anwendungen über einen zentral verwalteten Service

Effiziente Risikoverwaltung
Schutz wichtiger Ressourcen, Erhöhung der Benutzerfreundlichkeit ohne Beeinträchtigung der Sicherheit

Verwendung eines beliebigen Authentifizierungsverfahrens
Bedienung verschiedener Sicherheitsstufen durch Nutzung vorhandener Authentifizierungsverfahren und deren Ausweitung auf die Cloud

Einhaltung gesetzlicher Vorgaben und Bedienung von Sicherheitsstufen
Einhaltung von Datenschutzvorgaben aller Branchen

Vereinfachte Anmeldung
Einfache Benutzeranmeldung an mehreren Apps per Cloud-SSO, im Bedarfsfall mit strengerer Authentifizierung

SAFENET-LÖSUNGEN FÜR IDENTITY &ACCESS MANAGEMENT VON GEMALTO

Mithilfe der branchenführenden Gemalto-Lösungen für das Identity & Access Management können Unternehmen den Zugriff auf die Unternehmens-IT sowie web- und cloud-basierte Anwendungen zentral verwalten und schützen. Die Nutzung von richtlinienbasiertem Single-Sign-On und universellen Authentifizierungsverfahren ermöglicht Unternehmen ein effizientes Risiko-Management sowie die Einhaltung aufsichtsbehördlicher Vorgaben und erlaubt einen transparenten Einblick in alle Zugriffsaktivitäten, während der Anmeldevorgang für Benutzer vereinfacht wird.

Kontakt: Die Übersicht unserer Geschäftsstellen finden Sie auf safenet.gemalto.de

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) - 14Sep2018 – Design: RM