okta

Die acht größten Herausforderungen beim Identitäts- und Zugriffsmanagement (Identity & Access Management) für SaaS-Anwendungen

Okta Deutschland
Oskar-von-Miller-Ring 20
80333 München

info_germany@okta.com
+49 (89) 26203329

Inhaltsverzeichnis

Die Bedeutung der Benutzeridentität für SaaS-Anwendungen

Die Enterprise Cloud revolutioniert die IT-Welt. IT-Abteilungen überall, von kleinen und mittleren Unternehmen bis hin zu den größten börsennotierten Konzernen, stellen lokale Anwendungssoftware schrittweise auf On-Demand-Services in der Cloud um. Mit diesem Übergang zu einem hybriden On-Demand-/On-Premise-Modell wird es immer wichtiger zu kontrollieren, wem Zugriff auf welche Anwendungen und Daten gewährt wird. Dies stellt CIOs und ihre IT-Abteilungen vor ganz neue Herausforderungen beim Identitätsmanagement. Für Endbenutzer wird es immer schwieriger, den Überblick über diverse URLs, Benutzernamen und Passwörter zu behalten, die sie für ihre Anwendungen benötigen. Zudem ändert sich die Rolle der IT: Als Verwalter der neuen Services muss die IT-Abteilung auch als Berater für Software-as-a-Service-Anwendungen (SaaS) fungieren, damit das Unternehmen optimal von seinen Investitionen profitiert.

Dieses Whitepaper stellt die acht größten Herausforderungen für das Identity and Access Management (IAM) im Zusammenhang mit der Einführung und Bereitstellung von Cloud-

und SaaS-Anwendungen vor. Zudem werden Best Practices für jede einzelne dieser Herausforderungen beschrieben.

Endbenutzer sind Passwörter leid

Das SaaS-Modell erleichtert Benutzern den ersten Zugriff auf ihre Anwendungen, aber

die Komplexität nimmt mit der Anzahl der verwendeten Anwendungen schnell zu. Jede Anwendung hat unterschiedliche Passwortanforderungen und auch die Ablaufzeiten der Passwörter variieren. Multipliziert man die Vielfalt der Anforderungen mit der Vielfalt der Ablaufzyklen, führt dies zu Produktivitätseinbußen und verärgerten Benutzern, die sich mit ständig wechselnden Passwörtern und URLs für diverse Anwendungen auseinandersetzen müssen.

Noch bedenklicher sind die Sicherheitsrisiken, die von den passwortmüden Benutzern verursacht werden, indem sie auf leicht durchschaubare oder wiederverwendete Passwörter zurückgreifen, sie auf Haftzetteln notieren oder in unverschlüsselten Dateien auf Laptops speichern.

IAM-Dienste in der Cloud können diese Bedenken ausräumen, indem sie Single Sign-On

für alle Anwendungen ermöglichen und Endbenutzern einen zentralen Ort für den Zugriff auf alle Systeme mit einem Benutzernamen und Passwort bieten. Mehr noch, ein Cloud-Identitätsmanagementsystem gibt Ihrer IT-Abteilung die Möglichkeit, Identitäten sowohl über On-Demand- als auch über lokal gehostete Anwendungen zu verwalten. In den meisten Unternehmen ist Microsoft Active Directory (AD) das maßgebliche Benutzerverzeichnis, das den Zugriff auf grundlegende IT-Services wie E-Mail und Dateifreigaben regelt. Häufig wird AD auch verwendet, um den Zugriff auf weitere Geschäftsanwendungen und IT-Systeme zu steuern.

Manuelles Erteilen und Entziehen von Zugriffsberechtigungen ist fehleranfällig

Wenn ein neuer Mitarbeiter im Unternehmen beginnt, stellt ihm die IT meist Zugriff auf das Firmennetzwerk, Dateiserver, E-Mail-Konten und Drucker zur Verfügung. Da viele SaaS-Anwendungen auf Abteilungsebene verwaltet werden (die Vertriebsabteilung verwaltet Salesforce.com, die Buchhaltung QuickBooks, das Marketing Marketo), wird der Zugriff auf diese Anwendungen oft einmalig vom Administrator der jeweiligen Anwendung gewährt, nicht von der zentralen IT.

Warum sollten SaaS-Anwendungen nicht so einfach zentral bereitzustellen sein wie Ihre Kernnetzwerkdienste? Ein robustes Identity and Access Management in der Cloud muss in der Lage sein, die Bereitstellung neuer SaaS-Anwendungen zu automatisieren – als natürliche Erweiterung Ihres aktuellen On-Boarding-Prozesses. Wenn ein Benutzer dem Hauptverzeichnisdienst (z. B. Active Directory) hinzugefügt wird, sollte seine Mitgliedschaft in bestimmten Sicherheitsgruppen sicherstellen, dass er automatisch mit den entsprechenden Anwendungen versorgt wird und die Zugriffsberechtigungen erhält, die er für seine Arbeit benötigt. So einfach sollte es sein.

Das Ausscheiden von Mitarbeitern bereitet Unternehmen noch größere Kopfschmerzen: Die IT-Abteilung kann den Zugriff auf E-Mail- und Unternehmensnetzwerke zentral widerrufen, muss sich aber auf externe Anwendungsadministratoren verlassen, um dem ausscheidenden Mitarbeiter den Zugriff auf SaaS-Anwendungen zu entziehen. Das Unternehmen wird dadurch anfällig, da kritische Geschäftsanwendungen und Daten in die Hände von vielleicht nachtragenden ehemaligen Mitarbeitern geraten können. Prüfer schauen bei Audits als erstes auf Lücken beim Entzug von Berechtigungen.

Ein IAM-Dienst in der Cloud sollte der IT-Abteilung nicht nur die automatische Bereitstellung neuer Anwendungen ermöglichen, sondern auch folgende Funktionen bieten:

- **Automatisierter Entzug von Berechtigungen für alle lokalen und On-Demand-Anwendungen**
- **Umfassende Integration mit Active Directory**
- **Klare Audit-Trails**

Der IAM-Dienst soll die Gewissheit bringen, dass Mitarbeiter beim Ausscheiden aus dem Unternehmen keine Daten mitnehmen können.

Transparente Compliance: Wer hat Zugriff auf was?

Unternehmen müssen immer einen klaren Überblick darüber haben, welche Personen Zugriff auf Anwendungen und Daten haben, wie sie darauf zugreifen und was sie damit tun. Bei Cloud-Diensten ist dies umso wichtiger. Leider bieten nur die fortschrittlichsten Angebote wie Salesforce.com überhaupt ein geeignetes Reporting, das dann aber auf diese eine Anwendung beschränkt ist.

Wenn bei einem Audit die Frage aufkommt, wer Zugriff auf Anwendungen und Daten hat, ist ein transparenter Überblick mit Kontrolle über alle Systeme erforderlich. Ihr IAM-Dienst sollte es Ihnen ermöglichen, Zugriffsrechte für alle Dienste festzulegen und zentralisierte Audit-Berichte über Zugriffsrechte, Bereitstellung und Entzug sowie Endbenutzer- und Administratoraktivitäten zu liefern.

Isolierte Benutzerverzeichnisse für jede Anwendung

Wie die meisten Unternehmen werden Sie beträchtliche Investitionen in ein Firmenverzeichnis (wie Microsoft Active Directory) getätigt haben, um den Zugriff auf lokale Netzwerkressourcen zu verwalten. Wenn Sie Cloud-Dienste einführen, sollten Sie diese Investition nutzen und auf die Cloud ausdehnen, statt eine parallele Verzeichnis- und Zugriffsverwaltungsinfrastruktur nur für die neuen SaaS-Anwendungen aufzubauen.

Eine Cloud-IAM-Lösung sollte sowohl

Endanwendern als auch IT-Administratoren den Zugriff überall, jederzeit und mit jedem Gerät erleichtern. Eine gute Lösung sollte dabei nicht nur browserbasiertes Single Sign-On für Endbenutzer für alle Anwendungen ermöglichen, sondern auch einen einfachen Zugriff auf dieselben Dienste mit Mobilgeräten.

Anwendungsintegrationen auf dem neuesten Stand halten

Die echte Zentralisierung von Single Sign-On und Benutzerverwaltung erfordert die Integration von zahlreichen Anwendungen und die Überwachung der Wartungsanforderungen fürneue Versionen jeder Anwendung. Für die überwiegende Mehrheit der Unternehmen ist es unrealistisch und ineffizient, dass ihre IT-Abteilung eigene Konnektoren für diese dynamische Anwendungslandschaft pflegt.

Die heutigen Enterprise-Cloud-Anwendungen werden mit modernsten, internetoptimierten Architekturen erstellt. Die modernen Webtechnologien, die diesen Anwendungen zugrunde liegen, bieten Anbietern hervorragende Möglichkeiten, ihre Dienste und die damit verbundenen Schnittstellen zu entwickeln. Für IT-Profis bedeutet das leider auch, dass oft jeder neue Anbieter einen neuen Ansatz bei der Integration verlangt, insbesondere in Bezug auf Benutzerauthentifizierung und -verwaltung.

Darüber hinaus ändern sich SaaS-Apps wie lokale Anwendungen ebenfalls im Laufe der Zeit. Eine gute Cloud-IAM-Lösung muss mit den unterschiedlichsten Änderungen Schritt halten und sicherstellen, dass die Anwendungsintegration und damit der Zugriff immer auf dem neuesten Stand und funktionsfähig sind. Ihr IAM-Service sollte diese verschiedenen Integrationstechnologien und -ansätze vermitteln und die Herausforderungen für die IT transparent machen. Und da sich die APIs der verschiedenen Dienste ändern und vervielfachen, sollte der Cloud-IAM-Anbieter die Programmierschnittstellen verwalten und Ihrer IT-Abteilung so den technischen Aufwand abnehmen. Das heißt: keine lästige Zusatzarbeit mehr wegen Abhängigkeiten zwischen Konnektoren und Anwendungsversionen.

Und dabei sollte die Einführung einer neuen Anwendung im Netzwerk so einfach wie das Installieren einer neuen App auf einem Smartphone sein. Mit nur minimaler, unternehmensspezifischer Konfiguration sollten Sie in der Lage sein, neue SaaS-Anwendungen mit Single Sign-On und Benutzerverwaltung innerhalb weniger Minuten zu integrieren.

Unterschiedliche Verwaltungsmodelle für verschiedene Anwendungen

Da Cloud-Anwendungen einfacher und kostengünstiger in Betrieb genommen werden können, setzen Unternehmen immer mehr punktuelle SaaS-Lösungen ein. Diese Lösungen werden oft von den entsprechenden Funktionsbereichen in einem Unternehmen verwaltet, also Salesforce.com beispielsweise vom Vertrieb. Dies entlastet die zentrale IT, da die Anwendungsadministration von anderen übernommen wird und mehr Zeit für die Kernaufgaben bleibt. Aber es führt auch zu neuen Problemen durch die fehlende zentrale Benutzer- und Anwendungsadministration und -berichterstattung.

Ein Cloud-IAM-Dienst sollte der IT-Abteilung eine zentrale Verwaltung, Berichterstattung sowie ein Benutzer- und Zugriffsmanagement für alle Cloud-Anwendungen ermöglichen. Darüber hinaus sollte der Dienst über ein integriertes Sicherheitsmodell verfügen, das einen angepassten Zugriff für einzelne Anwendungsadministratoren ermöglicht, damit diese ihre jeweiligen Benutzer und Anwendungen innerhalb des zentralen IAM-Systems selbst verwalten können.

Suboptimale Nutzung und mangelnder Einblick in Best Practices

Einer der Gründe für den Erfolg von Cloud-Anwendungen liegt darin, dass sie die Vorabauch in Anspruch nehmen. Ohne einen zentralen Überblick über die Nutzung fehlen IT- und Finanzverantwortliche jedoch die nötigen Daten, um die Abonnements zu verwalten. Sie können nicht feststellen, ob sie für mehr bezahlen, als sie tatsächlich nutzen.

Ein Cloud-IAM-Service sollte einen besseren Überblick über die Auslastung von Arbeitsplatzlizenzen bieten und der IT-Abteilung helfen, die Ausgaben für SaaS-Abonnements zu optimieren. Manager sollten Echtzeitzugriff auf Berichte zur Dienstauslastung und Daten darüber erhalten, wie viele Benutzer sich wie oft bei den verschiedenen Diensten anmelden. Darüber hinaus sollten Führungskräfte durch die Berücksichtigung des Zugriffsverhaltens besonders produktiver Mitarbeiter einen zentralisierten Benutzerverwaltungsdienst nutzen können, um Best Practices ihrer Mitarbeiter im gesamten Unternehmen nutzen zu können.

Die Herausforderungen mit Okta bewältigen

Okta ist ein On-Demand-Dienst für Identity and Access Management, der Unternehmen dabei unterstützt, diese Herausforderungen zu bewältigen und die Einführung von SaaS-Anwendungen im gesamten Unternehmen zu beschleunigen.

Als schlüsselfertige Komplettlösung erfüllt Okta die Bedürfnisse von IT, Endanwendern und Führungskräften im gesamten Unternehmen.

Endbenutzer: Eine Anlaufstelle für alle Anwendungen

Da es sich um einen Cloud-Dienst handelt, ist das Hinzufügen neuer Benutzer zu Okta so einfach wie das Hinzufügen eines Benutzers zu jeder anderen SaaS-Anwendung. Nach der Aktivierung erhält jeder Endbenutzer eine seine eigene Startseite, über die Single Sign-On und Self-Service für alle Anwendungen und Anmeldeinformationen möglich ist. Der Zugriff auf die Startseite ist mit allen Browsern und Geräten möglich, und die gesamte Startseite oder einzelne Anwendungen lassen sich problemlos in ein eigenes Portal integrieren.

IT: Sichere, integrierte Kontrolle für verschiedene Personen und Anwendungen

Für die IT bietet Okta einen Dienst, von dem aus Sie Personen, Anwendungen und Richtlinien für alle Ihre Cloud- und Webanwendungen verwalten können. Ein zentrales Verzeichnis bietet einen Überblick über alle Mitarbeiter und die Identitäten, denen sie in allen ihren Webanwendungen zugeordnet sind. Das Hinzufügen von Anwendungen ist denkbar einfach: Sie wählen eine vorintegrierte Anwendung aus dem Okta Application Network aus und führen eine zusätzliche Konfiguration für Ihr Unternehmen durch.

Führungskräfte: Einblicke zur Maximierung des ROI und Minimierung des Risikos

Der Okta-Dienst verfügt über ein zentrales Systemprotokoll, das Aktivitätsereignisse sowohl in Okta als auch in den integrierten Anwendungen umfassend protokolliert. Ein vollständiges Reporting-Paket deckt alle integrierten Anwendungen ab, eine separate BI-Lösung ist nicht erforderlich. Die fertigen Berichte helfen Ihnen bei der Verfolgung von Aktivitäten, der Sicherstellung der Compliance und der Überwachung der Anwendungsnutzung und des ROI.

Erste Schritte mit der kostenlosen Testversion

Um selbst zu sehen, wie einfach der Einstieg in Okta ist und damit Sie die umfassende Integration Ihrer SaaS-Anwendungen mit Active Directory und die sichere Skalierung Ihrer Cloud-Anwendungen kennenlernen, besuchen Sie www.okta.com/freetrial.

Über Okta

Okta ist der marktführende On-Demand-Dienst für Identity and Access Management, der es Unternehmen ermöglicht, die sichere Einführung ihrer Web-Anwendungen sowohl in der Cloud als auch hinter der Firewall zu beschleunigen. Okta ist eine Komplettlösung, die die Anforderungen von IT, Endbenutzern und Führungskräften erfüllt. Eine Anpassung ist nicht erforderlich.

Mit einem Katalog vorintegrierter Anwendungen und einer umfassenden Einbindung von Active Directory bietet Okta zentrale Bereitstellung von Benutzerkonten, Zugriffsverwaltung und Reporting. Jeder Endbenutzer erhält eine personalisierte Single-Sign-On-Startseite für alle Anwendungen. Führungskräfte profitieren von den Daten, die sie benötigen, um den ROI zu maximieren und die Compliance zu überwachen.

Der Dienst von Okta basiert zunächst auf einer sicheren, zuverlässigen und erweiterbaren mandantenfähigen On-Demand-Plattform für Cloud-Dienste. Diese Plattform bildet die Grundlage für eine wachsende Anzahl von Kerndiensten von Okta und Partnern, die es Unternehmen ermöglichen, Hindernisse bei der Einführung der Cloud zu beseitigen und das Potenzial der Cloud für Unternehmen und ihre Mitarbeiter überall zu erschließen.

Das Okta-Team hat marktführende On-Demand- und Unternehmenssoftwarelösungen von Unternehmen wie Salesforce.com, SuccessFactors, PeopleSoft, Microsoft, Sun und HP eingerichtet, bereitgestellt und unterstützt. Okta wird von Premiere Angel und Venture-Investoren wie Andreessen Horowitz, FLOODGATE und Ron Conway unterstützt.