IAM für das Cloud-Zeitalter

**„Herausforderungen beim Identity & Access Management in der Cloud“:
Erkenntnisse und Handlungsempfehlungen aus der Diskussionsrunde von iC Consult und Ping Identity**

Im Fokus der Diskussion:

- Identity & Access Management in der Cloud und für die Cloud
- Handling von IAM-Umgebungen mit multiplen Identitätstypen
- Die verschiedenen Cloud-Consumption-Modelle
- IAM für kritische Infrastrukturen
- Herausforderungen von IAM in M&A-Szenarien
- Trends bei der Verifizierung von Identitäten

Weltweit treiben die Unternehmen die Digitalisierung ihrer Infrastrukturen voran und verlagern immer mehr und immer kritischere Business-Prozesse in die Cloud, um agiler, produktiver und effizienter zu arbeiten. Damit gewinnt ein durchgängiges, sicheres und nahtlos integriertes Management der digitalen Identitäten rasant an Bedeutung.

Wer zuverlässig ausschließen will, dass ungesicherte Remote-Zugriffe für Angriffe und Datendiebstähle missbraucht werden, ist mehr denn je auf robuste und bedienfreundliche IAM-Lösungen angewiesen, mit denen sich Kunden-, Partner- und Mitarbeiteridentitäten in der Cloud und aus der Cloud heraus managen lassen.

Vor diesem Hintergrund veranstaltete die iC Consult Group GmbH zusammen mit dem Hersteller Ping Identity einen virtuellen Roundtable zum Thema „IAM im Cloud-Zeitalter“. Mehmet Yaliman, Solutions Architect bei Ping Identity und Heiko Hütter, CEO von Service Layers führten durch die Diskussion und gaben den geladenen Enterprise-Kunden praxisnahe Tipps und Ratschläge, aber auch den Raum, ihre Meinungen und Erfahrungen rund um Identity & Access Management auszutauschen.

In der einstündigen Diskussion adressierten die Teilnehmer eine Reihe spannender Fragestellungen, die über die Gesprächsrunde hinaus wichtige Trends und Lösungsstrategien für IAM aufzeigen.

Identity & Access Management in der Cloud und für die Cloud

1. Die Migration in die Cloud geht in der Regel mit einer deutlichen Vergrößerung der Angriffsfläche einher. Welche Rolle kommt dem Identity & Access Management beim Schutz kritischer Daten in Cloudanwendungen zu?

In den zunehmend komplexen hybriden Umgebungen von heute geht die Transparenz über die Datenzugriffe immer mehr verloren – und damit steigt das Risiko kritischer Datenverluste. Viele Unternehmen entscheiden sich daher für einen Zero-Trust-Ansatz, bei dem sämtliche Datenzugriffe so lange als unsicher bewertet werden, bis die Iden-

Handling von IAM-Umgebungen mit multiplen Identitätstypen

tität des Users (oder, im Falle von API-Zugriffen, des externen Systems) zuverlässig verifiziert wurde. Die Teilnehmer erklären auf Anfrage, dass sie diesem Modell bislang noch abwartend gegenüberstehen. Dennoch findet die Runde rasch zu einem Konsens: Ein robustes Identity & Access Management, das eindeutig regelt, wer wer ist und wer was darf, sei für die sichere Anbindung der Cloud unerlässlich.

Die Teilnehmer weisen außerdem darauf hin, dass sich das Thema „IAM und Cloud" nicht nur darum dreht, die Identitäten beim Zugriff auf Cloud-Anwendungen zu managen („IAM für die Cloud"). Ein ebenso wichtiger Aspekt sei es, dass immer mehr IAM-Systeme selbst Cloud-basiert sind („IAM in der Cloud"). Auch dieses Konzept stellt viele IT-Abteilungen vor erhebliche Herausforderungen und muss sorgfältig im Blick behalten werden.

2. Unternehmen müssen heute individuelle Zugriffsrechte für multiple Identitätstypen (Kunden, Mitarbeiter, Partner, Zulieferer usw.) managen. Sollten diese Rollen in dedizierten Systemen verwaltet werden, oder ist es effizienter, sie in einer Lösung zusammenzuführen?

Mehrere Diskussionsteilnehmer bestätigen, dass sie sich aktuell mit der Frage nach der Verwaltung multipler Identitätstypen beschäftigen, und dass es wünschenswert wäre, diese in einer einheitlichen Lösung zusammenzuführen. Die meisten von ihnen geben aber an, dass sie die Communities bislang noch nach ihrer jeweiligen Rolle (typischerweise: Endkunde, Mitarbeiter und Partner) unterteilen und für jede Gruppe eine dedizierte Lösung nutzen. Diese strikte Trennung wird allerdings als nicht ideal eingestuft, da die Rollen zunehmend aufweichen und heute beispielsweise viele Kunden Zugriff auf APIs haben, die früher ausschließlich Mitarbeitern vorbehalten waren. Ein Teilnehmer merkt darüber hinaus an, dass man auch die Partner nicht pauschal zusammenfassen, sondern lieber nach der Art der Zusammenarbeit, dem Skill-Set und den in Anspruch genommenen Services untergliedern sollte.

Wie komplex das Thema de facto ist, zeigt sich, als ein Teilnehmer darauf hinweist, dass die Identitäten in seinem Unternehmen nicht nur nach Identitätstypen unterschieden werden, sondern dass darüber hinaus auch mehrere Divisions dedizierte IAM-Systeme vorhalten, was zu einem Mix unterschiedlichster Systeme und Identitäten geführt habe. Die Vereinheitlichung dieser Systeme habe aber hohe Priorität.

Die verschiedenen Cloud-Consumption-Modelle

3. Bei der Integration einer modernen IAM-Lösung können Unternehmen derzeit aus einer Reihe von Deployment-Optionen wählen. Welche Möglichkeiten gibt es?

Im ersten Schritt müssen die Unternehmen entscheiden, ob sie eine vollständig cloud-basierte, eine hybride oder eine On-Premises betriebene Lösung favorisieren.

Wer sich für ein cloudbasiertes Identity-as-a-Service-Modell entscheidet, kann im einfachsten Fall eine weitgehend standardisierte Multi-Tenant-Lösung wie Ping One implementieren, bei der sämtliche Komponenten und Services vorausgewählt und vorkonfiguriert sind. Für Kunden, die ein höheres Maß an Kontrolle und Wahlfreiheit wünschen, sind alternativ aber auch wesentlich stärker individualisierbare Single-

Tenant-Lösung verfügbar: So stehen Unternehmen etwa bei den Ping One Advanced Services umfassende Customizing-Optionen wie die IAM Plattform von Service Layers zur Verfügung.

Wer mit seinem Identity & Access Management nicht vollständig in die Cloud wechseln möchte, der kann alternativ auf zahlreiche hybride Modelle ausweichen, bei denen einige Komponenten der Lösung im eigenen Rechenzentrum gehostet und andere über SaaS bezogen werden. Welche Bereiche dabei ausgelagert und welche inhouse betrieben werden, ist dabei ganz dem Unternehmen selbst überlassen. Letztlich hängt die genaue Zusammenstellung des hybriden Modells ja maßgeblich von den individuellen Anforderungen des Kunden ab. Ein Modell nach dem Motto „One Size fits all" ist, so die Teilnehmer, keine probate Lösung.

Am anderen Ende des IAM-Spektrums stehen schließlich klassische On-Prem-Lösungen, bei denen die Kontrolle und die Verantwortung in der Regel in weiten Teilen beim Kunden liegen. Warum diese für viele Umgebungen nach wie vor die beste Option sind, zeigt sich im weiteren Diskussionsverlauf.

4. Nicht jede Unternehmensform kann bzw. darf auf eine Cloud-Lösung zurückgreifen. Warum?

IAM für kritische Infrastrukturen

Ein Teilnehmer aus der Militärindustrie meldet sich zu Wort. In seiner Branche, erzählt er, sei ein cloudbasiertes Identity & Access Management derzeit schon aus Gründen der Compliance keine Option. Mit Blick auf die hochgradig kritischen Daten des Unternehmens müssten die digitalen Identitäten ausschließlich On-Premises verwaltet werden. Die Nutzung einer Cloud käme in diesem Bereich nicht in Frage. Man habe, um zumindest in Teilbereichen von den Möglichkeiten der Cloud-Technologie profitieren zu können, eine eigene Private Cloud implementiert. Diese werde bislang aber vollständig im eigenen Rechenzentrum gehostet. Das Unternehmen habe allerdings erfolgreich Ping Directory als Alternative zu gängigen LDAP-Directories im Einsatz, und angesichts der Fortschritte im Bereich Cloud-Security stehe auch die Frage im Raum, ob sich die strikten Compliance-Vorgaben nicht ohnehin ändern werden.

Ein anderer Teilnehmer der Runde schaltet sich ein und bestätigt, dass dies durchaus möglich ist. Er arbeite schon länger mit Unternehmen aus der Militärindustrie zusammen und habe mit diesen auch schon Cloud-Projekte realisiert.

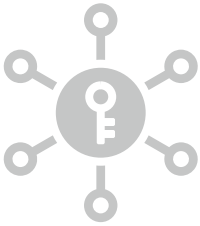
5. Was gilt es bei IAM-Projekten im Nachlauf eines Mergers oder einer Akquisition zu beachten?

Herausforderungen von IAM in M&A-Szenarien

Zum Aufgabenfeld einiger Teilnehmer gehört die Zusammenführung von IAM-Architekturen nach Mergern und Akquisitionen (M&A). Auch in diesem Umfeld gilt es eine Reihe spezifischer Herausforderungen zu beachten. Stand in der bisherigen Diskussion vor allem die Sicherheit im Vordergrund, rückt nun der Umgang mit großen Datenmengen in den Mittelpunkt. Eine IAM-Lösung müsse, so die Diskussionsrunde, stets auf ganzheitliche Lösungsansätze fokussieren, um auch die Anforderungen global agierender Unternehmen abzubilden – etwa, wenn es gilt, im Nachlauf eines Mergers Tausende von Identitäten, Gruppierungen und Systemen zu vereinheitlichen und zusammenzuführen.

6. Welche Möglichkeiten stehen Unternehmen bei der Verifizierung von Identitäten in der Cloud zur Verfügung. Welche Trends zeichnen sich für die Zukunft ab?

Grundsätzlich findet der Ping Stack in der Gesprächsrunde hohen Zuspruch. Mehrere Teilnehmer bestätigen, dass ihre Unternehmen schon heute weite Teile des Ping-Portfolios (genannt werden Ping Directory, Ping Federate, Ping One) nutzen, um ihre Identitäten und Zugriffe zu managen. Auch wenn sich die Teilnehmer einig sind, dass der Ping-Stack seine Stärken vor allem in cloudbasierten Umgebungen ausspielen kann, räumen zwei Teilnehmer ein, dass sie die Lösungen in ihren Unternehmen teilweise oder vollkommen On-Prem nutzen. Der eine begründet dies mit den Compliance-Vorgaben in der Militärindustrie, der andere gibt an, die Migration in die Cloud sei fest geplant, aber eben noch nicht abgeschlossen.



Trends bei der Verifizierung von Identitäten

Grundsätzlich decken die anwesenden Unternehmen eine breite Palette von Ping-Use-Cases und Deployment-Optionen ab. Der Tenor der Teilnehmer: Es gebe im IAM-Bereich zwar nach wie vor zahlreiche On-Prem-Anwendungen, der Trend gehe aber eindeutig zu Cloud-nativen Architekturen. Schon heute haben viele von ihnen Multicloud und mehrere IAM-Anbieter im Einsatz, um die steigenden Datenmengen und Anforderungen zu bewältigen. Darüber hinaus müsse man auch die Erwartungshaltung der Endkunden berücksichtigen. Und schließlich gelte es natürlich auch, die richtige Balance zwischen der Sicherheit des Unternehmens und dem Wunsch nach einer einfachen Bedienbarkeit der IAM-Lösung zu finden.

Ein Teilnehmer verweist an dieser Stelle auf einen Trend, der sich in China entwickelt hat und inzwischen zunehmend auch die Diskussion in den USA prägt: Single-Identity, also die Möglichkeit, sich mit einer Identität in multiplen Communities einzuloggen. Das Thema Single-Sign-on rückt in den Fokus.

7. Haben Passwörter im Identity & Access Management eine Zukunft?

Zum Abschluss der Diskussion steht die Frage im Raum, ob Passwörter als Mittel zur Bestätigung der Identität noch zeitgemäß und sicher sind. Die Gruppe ist sich einig: Nein. Nicht nur, weil Passwörter unsicher sind, und der Diebstahl von Credentials immer wieder dazu führt, dass wertvolle Daten verloren gehen. Sondern auch, weil sie alles andere als bedienfreundlich sind und Password-Resets nach wie vor enorme Kosten verursachen. Als mögliche Alternative bringt ein Teilnehmer die etwa in China populäre SMS-Bestätigung ins Spiel. Doch die Runde widerspricht: Auch dies sei längst kein zeitgemäßes Verfahren mehr. Die Teilnehmer favorisieren stattdessen Multi-Faktor-Authentisierung, Push-Benachrichtigungen und biometrische Maßnahmen wie Fingerprints. Dennoch schwingt bei einigen Teilnehmern Skepsis mit: Die Diskussion um das Aus der Passwörter werde bereits seit über zehn Jahren geführt und noch immer sei keine Lösung in Sicht.

Fazit: Mit den richtigen Partnern lösbare Herausforderungen

Nach sechzig spannenden Minuten fällt das Fazit der Diskussionsteilnehmer weitgehend einhellig aus: Das Thema Identity & Access-Management wird die Unternehmen noch lange beschäftigen. Immerhin stehen die Verantwortlichen vor der

anspruchsvollen Aufgabe, maßgeschneiderte Lösungen zu entwickeln, die nicht nur den Ansprüchen der eigenen Stakeholder gerecht werden, sondern auch eine breite Palette strenger gesetzlicher und branchenspezifischer Vorgaben (z.B. KRITIS) erfüllen. Mit zeitgemäßen IAM-Lösungen wie dem breiten Ping Stack oder der IAM-Plattform von Service Layers lassen sich all diese Anforderungen schon heute abbilden. Mit Blick auf die hohe Komplexität des Gesamtprojekts sind die Unternehmen aber gut beraten, frühzeitig erfahrene Consultants und Integratoren hinzuzuziehen.