1 | 17

GPOs für Windows 10

Hochverfügbarkeit für PostgreSQL

Collaboration mit Wrike

ISSN 1614-2888
€ 12,60
Österreich € 14,50
Luxemburg € 14,50
Schweiz CHF 20,50

IT Administrator

Das Magazin für professionelle System- und Netzwerkadministration

Hybrid Cloud:

Integration von Cloud-Diensten

AWS, Azure & Co. mit der eigenen IT verbinden

Virtuelle Netze

VMware NSX mit Arista-Switchen optimieren

Zahlreiche Neuerungen

Red Hat Virtualization 4 verwaltet hybride Clouds

Im Test

Cloud-Recovery mit der Veeam Availability Suite

Freie NAS-Software mit ZFS und Support für Windows-Clients

FreeNAS 9.10 auf CD-ROM

4 196583 212605 01

Identitäts- und Berechtigungsmanagementprojekte vereinfachen

Identität geklärt

von Sebastian Rohr

In einer Hybrid-Cloud-Infrastruktur sollten Accounts und Berechtigungen sicher verwaltet werden. Doch die Komplexität von Identitäts- und Berechtigungsmanagementprojekten schreckt viele Unternehmen ab. Dabei lassen sich diese vereinfachen.

Identitäts- und Berechtigungsmanagement – IAM – gehört längst zu den zentralen Aufgaben der IT-Security. Mit der steigenden Anzahl von Rollen, Identitäten und Berechtigungen wächst das Risikopotenzial für Angriffe auf das Unternehmensnetzwerk auch von innen rasant. Dabei ist IAM nicht mit der Implementierung einer Lösung abgeschlossen, sondern bedarf einer Auseinandersetzung mit der Organisationsstruktur, Geschäftsprozessen und Workflows. Die noch immer praktizierte Zuordnung von IAM-Projekten zur IT-Abteilung statt zu einer zentralen Architektur- oder zumindest Business-Abteilung wirkt dabei unrund. So ist es nicht verwunderlich, dass fehlende Ablaufstrukturen und Dokumentationen als Kostentreiber und Zeitfresser in IAM-Projekten auffallen und gleichzeitig die Komplexität eines guten IAM verdeutlichen.

Die Praxis ruft nach IAM

Beispiele, warum IAM in der Praxis dringend nottut, gibt es tatsächlich ausreichend. So sind Werkstudenten in vielen Unternehmen geschätzte Mitarbeiter und bringen heutzutage eine große IT-Affinität mit. Sie erhalten innerhalb kürzester Zeit sogar privilegierte Berechtigungen und Zugriff auf Kernsysteme mit jeweils verschiedenen Attributen. Schon in dieser Zeit fällt es schwer zu identifizieren, wann der Student sich wo anmeldet. Nach dem Ausscheiden vergessen die Verantwortlichen dann in vielen Unternehmen, die Accounts zu deaktivieren beziehungsweise Berechtigungen zu entziehen. Die Gefahr dabei: Mit einem mobilen Gerät loggt sich der Student in der Nähe der Firma ins Netzwerk ein und erhält Zugang zu sensiblen Daten und Systemen.

Es zeigt sich also, dass Unternehmen an unterschiedlichen Fronten mit vielen zusammenhanglosen Faktoren kämpfen, wenn jeder einzelne Benutzer Dutzende Identitäten für ebenso viele Systeme besitzt, wobei jedes System auch noch unterschiedliche Attribute oder Kontrollen innerhalb dieser Identitäten erfordert. Noch komplexer wird es, wenn Organisationen Compliance-Anforderungen nachkommen müssen, da sie hier gefordert sind, Sicherheitslücken nachhaltig zu schließen.

IAM-Projekte sind mehr als Technik

Die Geschichte des "vergessenen" Werkstudenten ist ein Schlüsselargument für die Einführung eines IAM. Doch bei aller Überzeugung für die Notwendigkeit der Etablierung entsprechender Systeme zeigt ein Blick in die Praxis, dass IAM-Projekte immer wieder sowohl budgetär als auch zeitlich aus dem Ruder laufen, einige scheitern sogar gänzlich.

Für die Ursachen gibt es mehrere Erklärungsansätze: Noch vor circa zehn Jahren drehte sich ein IAM-Projekt hauptsächlich darum, den Directory-Eintrag zweier Mitarbeiter quasi zu klonen, weil sie die gleichen Aufgaben erfüllten und daher dieselben IT-Berechtigungen erhalten sollten. Hier ging es vor allem um IT-Automatisierung. Doch seitdem hat sich angesichts der steigenden Anzahl von eingesetzten internen und externen Anwendungen einiges getan. Um IAM sinnvoll umzusetzen, bedarf es tiefgreifender Informationen zu Rollen- und Arbeitsprozessdefinitionen, die vor allem Business-Abteilungen bereitstellen können. Diese Erkenntnis stellt sich häufig erst im Laufe eines Projekts ein.

Die IT-Abteilung fungiert im Grunde vor allem als Werkzeug beziehungsweise stellt am Ende die Konnektoren und die Verbindungen und die Integration zu den Zielsystemen bereit. Projektzahlen belegen, dass circa 40 bis 60 Prozent der Auf-

wände aber in Themen wie Prozessabläufe, Organisation und Integration mit HR-Systemen, circa 20 Prozent in die Basisinstallation und nur weitere 20 Prozent in die IT fließen.

IAM kann Kosten senken

Vor diesem Hintergrund wird deutlich, warum IAM-Projekte budgetär sehr verschieden aufgestellt sind und im Vorfeld nicht selten falsch kalkuliert werden. Die Komplexität und damit am Ende auch der Preis eines solchen Projekts hängen vor allem von der Entwicklungsreife eines Unternehmens beziehungsweise von der Qualität seiner Aufbau- und Ablauforganisation ab. Stehen diese für ein IAM grundlegenden Informationen bereits zur Verfügung und sind sauber dokumentiert und verwendbar, schlägt sich das auch spürbar auf die Projekt- beziehungsweise Dienstleistungskosten um.

Geht es um die Kostenfrage, kommt erschwerend hinzu, dass sich der "Return on Security Investment" (ROSI) nur schwer berechnen lässt, weil es sich im Grunde ausschließlich um die Reduktion operativer oder strategischer IT-Risiken handelt und damit um Wahrscheinlichkeiten möglicher IT-Schäden. Dabei gibt es im IAM-Bereich durchaus Aspekte, die Licht ins Dunkel bringen: Im Falle eines zurückgesetzten Passworts etwa lässt sich nämlich ein Vorfall gut mit einem Kostenfaktor belegen und Einsparungen durch den Einsatz eines IAMs nominal berechnen. Andere Betrachtungsweisen beziehen die entgangene Produktivität, die durch die aufgewendete Zeit für Antragsprozesse entsteht, mit ein. Umfassen entsprechende Berechnungen dann auch noch die Arbeitszeit aller anderen, an diesem Vorgang beteiligten Fachkräfte, erreichen die potenziellen Einsparungen schnell beachtliche Höhen.

Die Einführung eines durchdachten und funktionierenden IAM-Systems und einer klaren Zuweisung von Verantwortlichkeiten reduziert nicht nur diese Vorfälle, sondern verkürzt die Prozesse über einen definierten digitalen Workflow auf bis zu zwei bis vier Stunden. Nicht zuletzt fließen in den ROSI auch weiche Faktoren wie die Transparenz des Bearbeitungsfortschritts für alle Mitarbeiter oder eine daraus resultierende höhere Mitarbeiterzufriedenheit, die sich wiederum positiv auf die Effizienz ihrer Arbeit auswirkt, ein.

Eindeutige digitale Identität als Idealzustand

IAM hilft beim On- und Offboarding von Mitarbeitern in den unterschiedlichen Systemen. Dabei unterscheiden sich die Points-of-Entry je nach dem Status der Identität. Während Vollzeitangestellte, Werkstudenten oder Auszubildende üblicherweise über ein Personalsystem oder eine Human-Ressource-Datenbank Zugang erhalten, wird für externe Fachkräfte mitunter schon eine E-Mail eines Abteilungsleiters als ausreichend angesehen. Viel sinnvoller wäre hingegen vor allem die Vergabe einer einzigen, eindeutigen digitalen Identität – verbunden mit einem einzigen Attribut-Bundle. Die Frage, welche Daten dafür herangezogen werden, steht in jedem Falle am Anfang eines ID-Lebenszyklus.

Möglich wäre in Deutschland zweifelsohne das Auslesen des neuen Personalausweises über die digitale Schnittstelle. Auf diese Weise wäre eine Verknüpfung der staatlich validierten Attribute wie Vorname, Nachname, Geburtsdatum und derzeitiger Wohnort mit der digitalen Identität denkbar. Auch hier wird deutlich, dass das Onboarding, also das Anlegen einer Identität, eher der HR-Abteilung zuzuordnen ist und die IT allenfalls die Instrumente hierfür bereitstellen sollte. Diese eindeutige Identität benötigt zu gegebenen Anlässen Updates, beispielsweise beim Arbeitgeber- oder Positionswechsel innerhalb des Unternehmens.

Einen weiteren relevanten Updateprozess stellt die Rezertifizierung dar. In vielen stark regulierten Unternehmen ist es wichtig und notwendig, Berechtigungen der Mitarbeiter jährlich, halbjährlich, vierteljährlich oder sogar monatlich zu prüfen und zu regulieren und bei Abweichungen korrektive Maßnahmen zu ergreifen. Auch dies erleichtert IAM durch Automatismen deutlich. Zu möglichen Sonderfällen zählen Elternzeit, eine längere Krankheit oder Beurlaubung und vor allem auch gängige Doppelrollen von Führungskräften global aufgestellter Mittelständler oder Konzerne. Gerade in diesen Situationen zahlt sich eine lebenslange, eindeutige, digitale ID aus – auch wenn es um sogenannte "Segregation of Duties" – also Situationen, wo bestimmte Aufgaben eines Geschäftsprozesses nicht durch ein und dieselbe Person oder Organisationseinheit durchgeführt werden sollen – geht.

Nicht nur das Onboarding wäre durch die Vergabe einer eindeutigen, lebenslangen, digitalen Identität vereinfacht, auch das Offboarding ist durch IAM-gestützte Delete-Prozesse einfach und sicher. Denn das System kann für definierbare Rollen und Funktionen ein Offboarding-Datum verlangen, sei es für Auszubildende, Praktikanten und Werkstudenten oder Angestellte mit befristeten Arbeitsverträgen. Insbesondere damit in Verbindung stehende Prüfpflichten sind durch die Automatisierung enorm vereinfacht.

Automatische Warnmeldungen vor Ablauf der Berechtigungen versetzen Verantwortliche gleichzeitig in die Lage, komfortabel diese zu verlängern, sofern eine längere Beschäftigung geplant ist. Eine einfache Bestätigung der Frage "Soll die Berechtigung für Max Mustermann zum 31.12. enden" könnte insbesondere Konzernen erhebliche Aufwände sparen.

Fazit

IAM-Projekte betreffen stets die gesamte Organisation eines Unternehmens. Effiziente und gut dokumentierte Abläufe sind die Basis eines solchen Projekts und gehören, sofern sie im Vorfeld nicht zur Verfügung stehen, zur Aufwandskalkulation dazu. Allein das Bewusstsein für die Komplexität dieses Business-Themas würde eine Bewertung beispielsweise der Budgetfrage im Nachhinein deutlich verbessern. Fakt ist auch: IAM-Systeme sollen die ohnehin schon vorhandene Komplexität verringern. Hierfür bedarf es keines komplexen IAM-Projekts, was über Jahre hinaus Ressourcen bindet und hohe Kosten verursacht. Hier bedarf es vor allem der zentralen Vergabe eindeutiger digitaler Identitäten – mit deren Hilfe IAM plötzlich ganz einfach wird. *(jp)*

Sebastian Rohr ist Technischer Geschäftsführer der accessec GmbH.