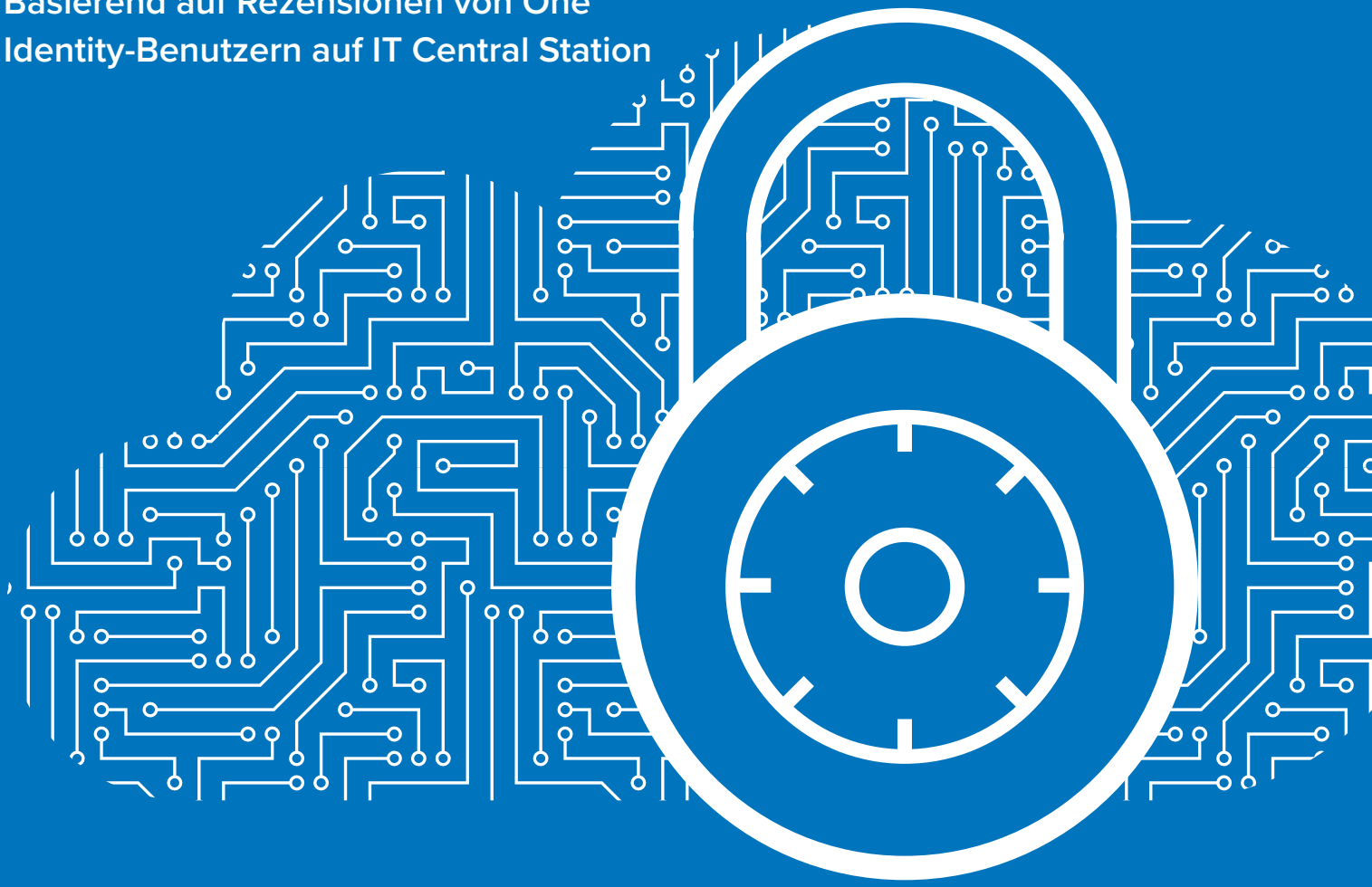
PeerPaper™ Report 2021

10 Best Practices zur Verwaltung und Absicherung von Microsoft Active Directory in einer dynamischen IT-Welt

Basierend auf Rezensionen von One Identity-Benutzern auf IT Central Station



IT Central Station
Unbiased reviews from the tech community

CSO
FROM IDG

KURZDARSTELLUNG

Die meisten IAM-Programme (Identity and Access Management, Identitäts- und Zugriffsmanagement) setzen fest auf Microsoft Active Directory (AD) und Azure AD (AAD). Da jedoch IAM-Umgebungen zunehmend in die Cloud übertragen, modernisiert und in Richtung Governance ausgeweitet werden, stehen IT-Manager vor der Aufgabe, die Sicherheits- und Effizienzlücken im nativen AD zu schließen. Aus diesem Grund suchen sie nach Lösungen, mit denen sie die häufig unzureichenden Funktionen von AD ergänzen können. Führende Unternehmen definieren praxistaugliche Ansätze zur Absicherung und Verwaltung von Hybrid-AD, da sich die Governance für Identitäten und Konten durch den Cloud-Einsatz in neue Richtungen entwickelt. Im vorliegenden Whitepaper werden diese neuen Best Practices vorgestellt, die auf Erfahrungen verifizierter Benutzer mit der Lösung One Identity Active Roles basieren und in Rezensionen auf IT Central Station beschrieben wurden.

INHALT

EINLEITUNG

Für alle CISOs und IT-Führungskräfte steht Sicherheit an erster Stelle. Bei ihrer Cybersicherheitsstrategie spielt ein sicheres und gut verwaltetes IAM-Framework (Identitäts- und Zugriffsmanagement) eine tragende Rolle. Tatsächlich betrachten die wichtigsten Sicherheits-Frameworks wie die des NIST eine effektive Kontrolle von Benutzeridentitäten und Zugriffsrechten als zentralen Faktor bei zahlreichen Gegenmaßnahmen. In diesem Bereich bilden Microsoft Active Directory (AD) und Azure AD (AAD) den Kern der meisten IAM-Programme. Sicherheitsmanager sind jedoch häufig mit AD unzufrieden, da die IT-Umgebungen zunehmend auf Hybridbetrieb setzen und immer komplexer werden. Daher suchen sie nach Möglichkeiten, die unzureichenden und ineffizienten Funktionen der nativen AD-Tools zu ergänzen. Neue innovative Lösungen bieten praxistaugliche Ansätze, damit AD weiter genutzt werden kann, während sich die Identity Governance durch einen zunehmenden Cloud-Einsatz weiterentwickelt.

Sofern nicht anders angegeben, verfügen alle in diesem Whitepaper aufgeführten Unternehmen über mehr als 10.000 Mitarbeiter.

IAM in einer dynamischen IT- und Sicherheitswelt

Wenn Organisationen ihre digitalen Assets in die Cloud verlagern und ihre Abläufe modernisieren, stehen sie vor neuen IAM-Herausforderungen. Ihre Anwendungsfälle für One Identity Active Roles zeigen, wie Identity Manager ihre IAM-Lösungen an die Cloud anpassen. Beispielsweise setzt ein IT-Sicherheitsverantwortlicher bei einem Aerospace/Rüstungsunternehmen für das lokale Active Directory auf Active Roles. Die Server selbst werden jedoch in Azure gehostet.

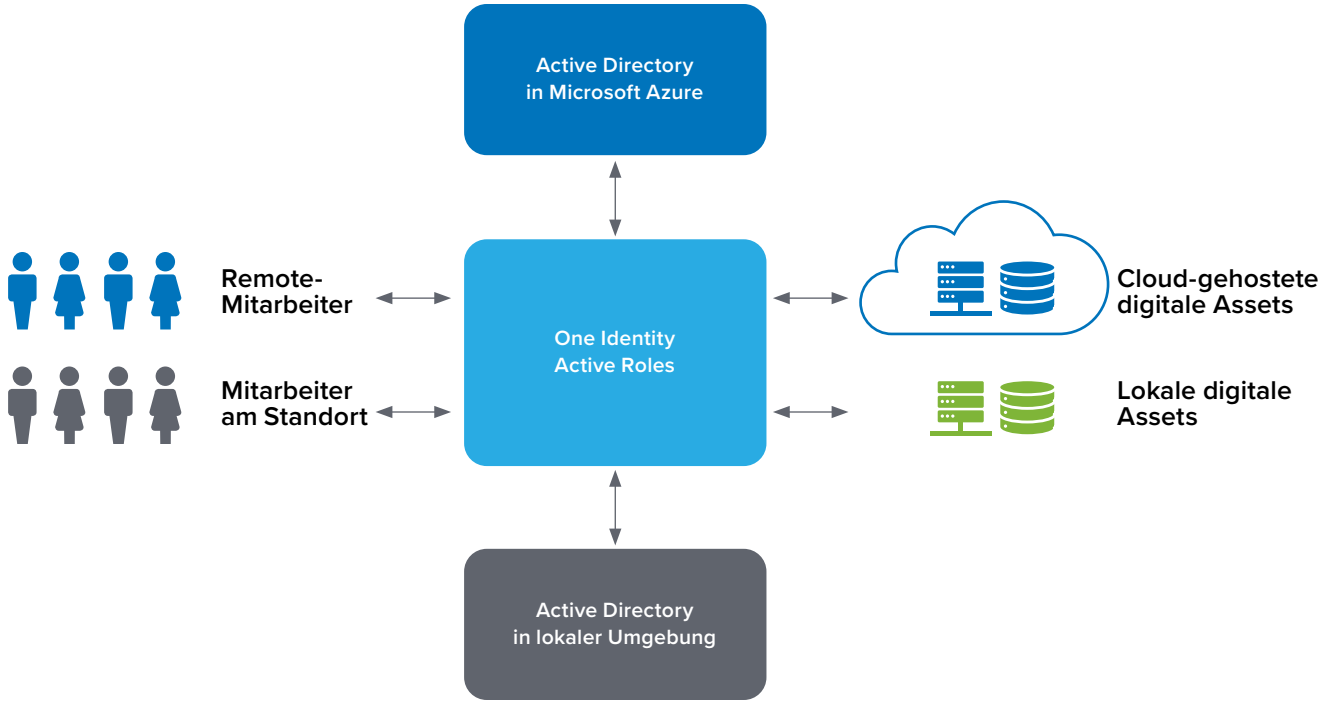


Abbildung 1: Die Cloud-Migration macht zentralisiertes IAM erforderlich, um den Zugriff auf digitale Assets unabhängig von ihrem Hosting-Ort zu verwalten.

Eine Senior Business Analyst an der George Washington University (GWU) nutzt Active Roles für viele AD-Verwaltungsprozesse, einschließlich der grundlegenden Funktion der Kontoerstellung. Sie erklärte dazu: „Wir machen native Eigenschaften von Azure AD-Benutzergruppen nutzbar, um der gesteigerten Support-Nachfrage Rechnung zu tragen. Dabei stellen wir Anwendungen bereit, nehmen sie wieder außer Betrieb und erstellen die jeweils notwendigen Berichte.“ Abbildung 1 zeigt eine einfache Referenzarchitektur, in der digitale Assets und AD-Instanzen standortnah und lokal gehostet werden.

Probleme mit AD und anderen Legacy-Systemen

Hintergrund für den Wechsel zu erweiterten IAM-Lösungen wie Active Roles sind die Probleme, die Benutzer von AD- und anderen Legacy-Systemen haben, sowie die Lücken in nativen AD-Tools. Ein Technical Manager of Security beim Kommunikationsanbieter Liberty Global blickte zurück: „Der Grund für unsere Entscheidung für diese [Active Roles]-Lösung – das muss 10 oder 15 Jahre her sein – war die Active Directory-Delegierung. Wir konnten keine unregulierten nativen Zugriffe auf unser Active Directory zulassen. Eine Möglichkeit wäre die Microsoft-Lösung gewesen, da sie kostenlos, integriert und bereits implementiert war. Aber wenn Sie eine bestimmte Größe überschreiten, stellen Sie schnell fest, dass die Microsoft-Lösung einfach nicht mithalten kann. Die AD- und AAD-Verwaltungsfunktionen unserer Lösung sind wirklich gut – und sie sind besser als die nativen Tools."

Ein Information Security Manager bei einem großen Fertigungsunternehmen mit mehr als 5.000 Mitarbeitern sagte: „Wir nutzten [ursprünglich] die nativen Microsoft-Tools, wechselten jedoch zu Active Roles, da die Microsoft-Tools vor allem zur Verwaltung der Kernkomponenten dienten und nicht alle notwendigen Funktionen für Provisionierung, Deprovisionierung, rollenbasierte Zugriffsbeschränkung und Änderungsverläufe bereitstellten. Sie erlaubten keine Proxy-Ansatz, um Active Directory zentralisiert zu verwalten. Bei Microsoft ist Active Directory standardmäßig verteilt, während Active Roles die Zentralisierung erlaubt."

„Vor dem Wechsel zu Active Roles nutzten wir eine intern entwickelte Skriptlösung", berichtete ein Senior IT Manager des Toronto District School Board. „Grund für unseren Wechsel war der bessere Support, aber auch der Wunsch, die alten und nicht mehr unterstützten manuellen Buildskripts in Rente zu schicken. Nun verfügen wir über ein zukunftstaugliches Produkt, für das es guten Support gibt. Im Vergleich dazu bieten die nativen Microsoft-Tools praktisch keine für uns wichtigen Funktionen. Es gibt keine Connectoren für den Benutzerverbund und die Synchronisierung mit den anderen Lösungen."

Wie die Senior Business Analyst der George Washington University weiter berichtete, konnte ihr Team mit Active Roles die Lösung Oracle Identity Manager (OIM) außer Dienst stellen. Sie erklärte dazu: „Leider wurde OIM vor etwa neun Jahren eingeführt. Es kostete jedoch viel Zeit, Anwendungen zu integrieren und die rollenbasierte Provisionierung einzurichten. Aus diesem Grund sind wir nie über die erste Phase hinausgekommen. Wir haben unsere Lektion gelernt und haben quasi ein komplett neues Active Roles erstellt, das alle bislang in OIM gespeicherten Informationen verarbeiten kann. Wenn OIM überlastet war, mussten wir ständig Neustarts durchführen. Seit der Einführung von Active Roles ist das nicht mehr notwendig. Nach der Migration vor einem Jahr mussten wir kein Neustart-Ticket mehr einreichen."

> **Grund für unseren Wechsel war der bessere Support, aber auch der Wunsch, die alten und nicht mehr unterstützten manuellen Buildskripts in Rente zu schicken.**

Stärkung der Sicherheit durch bessere IAM-Lösungen

Besseres IAM, das sicherer, einfacher zu verwalten und effizienter ist, ist unverzichtbar für die Verbesserung der allgemeinen Sicherheitssituation einer Organisation. Es hilft auch bei der Implementierung eines zuverlässigen Ansatzes für AD/AAD-Governance und Administration (AGA). Die Umsetzung dieser Idee ist jedoch nicht immer ganz einfach. Mittlerweile kristallisieren sich zehn Best Practices heraus, die einen stärkeren, sichereren und effizienteren IAM-Einsatz ermöglichen. Die IAM-Lösung muss den Benutzern nicht autorisierte Änderungen erschweren. Da die Verwaltung aufwändig sein kann, setzen die Verantwortlichen bevorzugt auf Lösungen, die Automatisierung sowie Integration in andere Systeme ermöglichen. Effizientes und effektives IAM muss auch Möglichkeiten zum Delegieren der Steuerung bieten. Idealerweise sollten IAM-Lösungen bei der Zugriffssteuerung auf ein Least-Privilege-Modell setzen und damit Zero Trust ermöglichen.

1. Verringerung nicht autorisierter Änderungen reduziert das Risiko

Nicht autorisierte Änderungen bei der Identitäts- und Zugriffssteuerung sind eine Risikoquelle, da unbekannte Benutzer Zugang erlangen können, ohne dass die Administratoren in vollem Maße davon erfahren. Active Roles ergänzt die standardmäßig vorhandenen AD-Funktionen und kann die möglichen Konsequenzen von solchem Verhalten minimieren. Der Information Security Manager des Fertigungsunternehmens erklärte dazu: „Da wir die wichtigsten Administratorrechte sperren konnten, gibt es weniger unkontrollierte Änderungen, sodass wir von größerer Dienstverfügbarkeit und weniger Audit-Beanstandungen profitieren." Er fügte hinzu: „Die [Active Roles]-Lösung verringert absolut das Risiko für unsere Organisation. An den nativen Active Directory-Sicherheitsfunktionen können keine Änderungen vorgenommen werden, zudem verfügen wir über rollenbasierte Zugriffskontrollen, mit denen wir Active Directory direkt aus der Anwendung heraus verwalten können. Damit haben wir unsere Risiken erheblich verringert."

> **Die Entscheidung für diese Lösung fiel, da wir die Umgebung absichern und schützen mussten.**

Der Technical Manager of Security bei Liberty Global gab seine Sicht der Dinge wieder: „Der Nutzen von [Active Roles] liegt im Minimieren von Risiken, z. B. dem Risiko nicht autorisierter Zugriffe oder dem Risiko von Active Directory-Störungen." Er führte weiter aus: „Diese Risiken führen dazu, dass Personen Zugriff auf Bereiche und Daten bekommen, für die sie nicht autorisiert sind. Es besteht auch das Risiko, dass es für die gleiche Sache mehrere Konten gibt."

„Die neue Lösung verbessert unsere Situation, da keine ungenehmigten Änderungen an AD mehr vorgenommen werden, von denen wir nichts wissen", betonte ein Identity Senior Analyst bei einem Konsumgüterunternehmen. „Unsere Mitarbeiter müssen immer noch ihre Aufgaben erledigen, aber wir können jetzt sicherstellen, dass alles im zulässigen Rahmen bleibt. Zuvor konnten sie AD direkt ändern. Wir haben das minimiert, indem jetzt alles über Active Roles läuft. Die Entscheidung für diese Lösung fiel, da wir die Umgebung absichern und schützen mussten."

2. Integration von IAM in Sicherheitssysteme

IAM ist ein IT- und Sicherheitsbereich, der von der einfachen Integration in andere Systeme in der Organisation profitiert. Im Falle des Information Security Managers bei dem Fertigungsunternehmen bedeutet das, Active Roles zur Bereitstellung von Active Directory-Objekten zu nutzen. Gleichzeitig greift er über den Active Roles-Synchronisierungsdienst auf ein Personalsystem zu, um Mitarbeiter zu provisionieren und zu deprovisionieren. Er sagte dazu: „Typischerweise provisionieren wir damit alle Objekte wie Sicherheitsgruppen und Computerobjekte auf delegierte Weise. Mit Active Roles Server kann die Sicherheit von Active Directory angepasst werden, um den Provisionierungszugriff für unterschiedliche IT-Teams zu delegieren, ohne die eigentliche Sicherheit von Active Directory zu ändern."

> **... wir provisionieren damit alle Objekte wie Sicherheitsgruppen und Computerobjekte auf delegierte Weise.**

Der IT-Sicherheitsverantwortliche des Aerospace-Unternehmens setzt auf die PowerShell-Schnittstelle von Active Roles. Damit können andere Teile seiner Umgebung sowie weitere Anwendungen, die darauf zugreifen müssen, mithilfe von PowerShell-Befehlen Änderungen an Active Directory vornehmen. Er bemerkte: „Wir können die gleichen Prinzipien wie bei unseren Sicherheitsberechtigungen anwenden, sodass sie Active Roles verwenden müssen. Dadurch sinkt unser Risiko aus Sicherheitsperspektive."

3. Delegierung für verbesserte Sicherheit

Mitglieder von IT Central Station sprachen darüber, dass sie den Zugriff auf AD-Prozesse gern delegieren. Beispielsweise arbeitet BeClever IT Solutions, ein kleines Technik-Dienstleistungsunternehmen, mit einem Kunden zusammen, der ein Problem mit seinen Berechtigungen und Delegierungen hat. Viele Benutzer bei diesem Unternehmen müssen in AD Verwaltungsaufgaben durchführen. Das war problematisch, da diese Benutzer potenziell Fehler verursachen konnten. Mit Active Roles können sie nun jedoch auf die Domänenadministratoren verzichten und bei standardmäßigen Benutzern bleiben. Sie können Werte für bestimmte Felder im Voraus ausfüllen.

Der Beauftragte des Unternehmens erklärte: „Für dieses Unternehmen ist das großartig, weil einige der Mitarbeiter nur einfache IT-Techniker sind, die sich nicht mit den erweiterten AD-Funktionen auskennen. Dank dieser Lösung wurden aufwändige IT-Provisionierungsabläufe überflüssig.“ Auch der Information Security Manager des Fertigungsunternehmens betonte: „Durch den delegierten Zugriff auf Active Directory konnten wir viele Administratorrechte widerrufen. Dadurch können wir die Umgebung besser kontrollieren und absichern als zuvor.“

4. Implementierung des Least-Privilege-Modells und Umsetzung von Zero Trust

Einige Active Roles-Benutzer auf IT Central Station nutzen die Lösung zum Implementieren des Least-Privilege-Modells für das Zugriffsmanagement. Dieser Ansatz setzt sich immer mehr durch, insbesondere da sich der herkömmliche Sicherheitsperimeter zunehmend auflöst und Organisationen den Wechsel zum Zero-Trust-Modell planen. Der IT-Verantwortliche des Aerospace-Unternehmens beschreibt das wie folgt: „Wir setzen verstärkt auf das Least-Privileged-Modell und weisen nur minimale native Active Directory-Berechtigungen zu, da wir uns auf diese Weise später Probleme ersparen. Weniger Mitarbeiter mit nativen Active Directory-Berechtigungen bedeuten, dass weniger potenzielle Probleme auftreten, die wir aufwändig beheben müssen.“ Abbildung 2 zeigt eine Darstellung des Least-Privilege-Modells mit den „Ringen“ der zunehmenden Berechtigungen, wobei der äußere Ring die geringste Berechtigung besitzt.

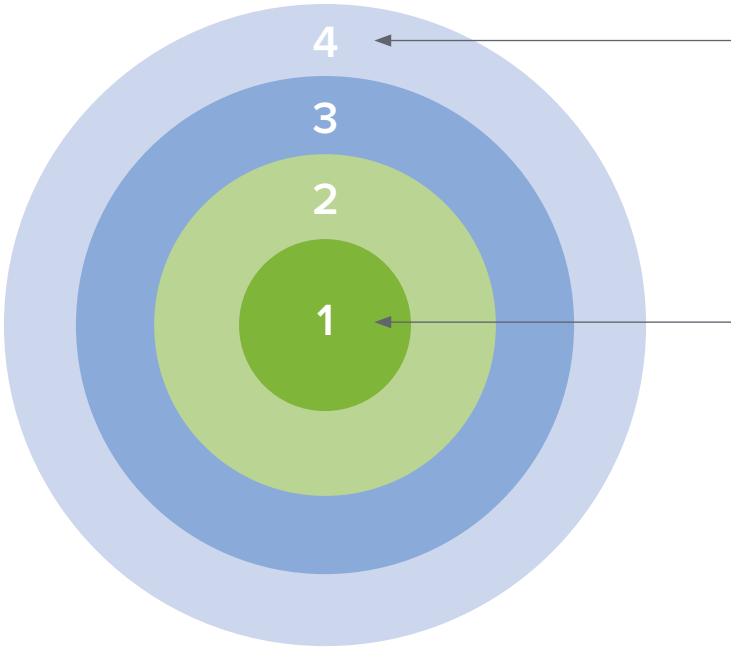
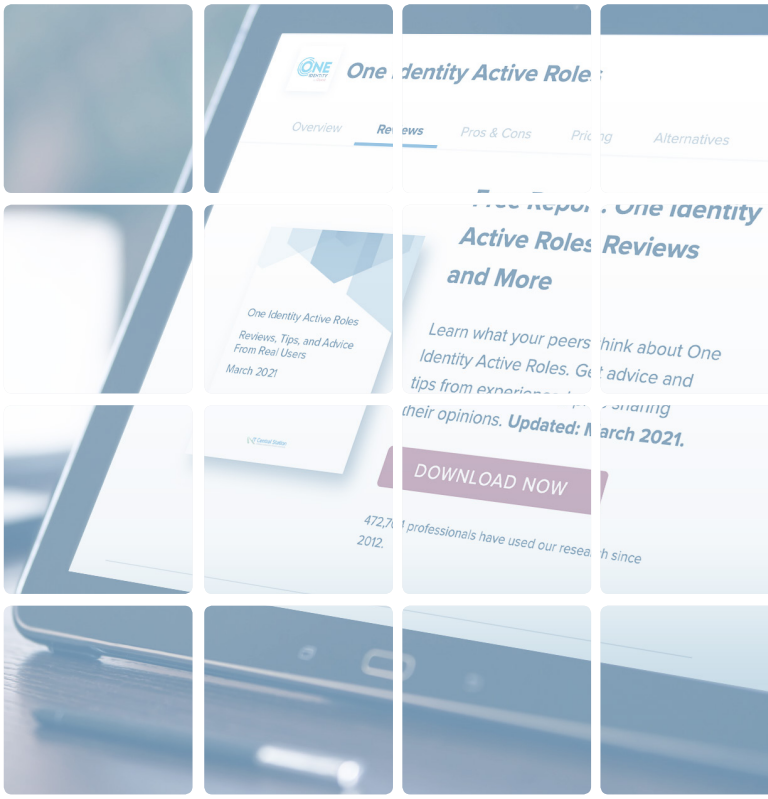


Abbildung 2: Das Least-Privilege-Modell weist den Benutzern standardmäßig die geringsten Zugriffsberechtigungen zu. Nur mit einer besonderen Genehmigung erhalten Benutzer höhere Berechtigungen und können auf sensiblere Zonen der Infrastruktur, Daten usw. zugreifen.

Verbesserung der Prozesse für die Identitätsverwaltung

Da die Sicherheit durch besseres IAM gestärkt werden muss, stellt sich die Frage, wie der Prozess für die Identitätsverwaltung verbessert werden kann. Den Mitgliedern von IT Central Station ist ein zentraler Kontrollpunkt wichtig, der jedoch detaillierte Steuerungsmöglichkeiten bietet. Ebenfalls wichtig sind ihnen Zeitersparnis sowie ein effizienter Onboarding-Prozess. Hinzu kommt, dass es Möglichkeiten zur Automatisierung der Workflows für die Identitätsverwaltung, zur Verwendung von Richtlinien und Vorlagen sowie zur Nutzung dynamischer Gruppen geben muss, um maximale Effektivität zu erreichen.



5. Zentrale Verwaltung mit einer konsolidierten Oberfläche

Benutzer von Active Roles, z. B. der IT-Verantwortliche des Aerospace-Unternehmens, freuten sich darüber, dass sie mehrere Active Directory-Strukturen in einer Konsole verwalten und eine konsolidierte Benutzeroberfläche lokal nutzen können: „Wir verfügen über mehrere Active Directory-Umgebungen, die wir nun an einer zentralen Stelle kontrollieren und verwalten können.“ Die Senior Business Analyst stimmte dem zu: „Die Flexibilität und Erweiterbarkeit dieser Plattform ermöglichen erheblich größere Effizienzen, als wir je erwartet haben. Mit Active Roles erhalten wir auch eine konsolidierte Benutzeroberfläche zur Verwaltung von AD und Azure AD. Besonders gut fanden wir, dass wir ausgehend von Active Roles auf alles zugreifen können, was wir brauchen.“

Ein Mitarbeiter bei Marriott Phoenix kommentierte das Thema der Kontrolle: „Mit Active Roles erhalten wir granulare Kontrollen, die AD einfach nicht bietet. Ein Tool, mit dem wir alle Änderungen an AD über eine konsolidierte Benutzeroberfläche verwalten können, ist großartig. Damit kann unser Helpdesk-Personal sehr schnell reagieren, auch ohne über detailliertes technisches Fachwissen zu verfügen.“

6. Verbesserung von Onboarding und Benutzer-Lifecycle-Management

Die Verwaltung der Identitäts- und Zugriffsaspekte des Mitarbeiterlebenszyklus ist potenziell zeitaufwändig und gleichzeitig ein Schwachpunkt. Beispielsweise stellen ehemalige Mitarbeiter, die weiterhin Zugriffsmöglichkeiten haben, eine Sicherheitsbedrohung dar. Um diese Risiken zu minimieren, sollte eine IAM-Lösung effiziente und effektive Benutzer-Lifecycle-Kontrollen bereitstellen. Beispielsweise erklärte der Information Security Manager des Fertigungsunternehmens, dass seine Lösung die Provisionierung automatisiert. Er fügte hinzu: „In unserem Personalsystem automatisieren wir die Einstellungen, Kündigungen sowie die laufende Verwaltung unseres gesamten Mitarbeiterstamms. Wir haben 5.000 bis 6.000 Mitarbeiter, und all diese Prozesse sind vollständig automatisiert, wobei die IT nicht mehr eingreifen muss. Dadurch sparen wir erheblich Arbeitszeit, ohne Weiteres hunderte Stunden pro Jahr."

Dieser Benutzer kommentierte anschließend: „One Identity Active Roles hat auch die Zuverlässigkeit unseres Onboarding-Prozesses verbessert. Bei unserem Unternehmen unterliegt der Onboarding-Prozess für Mitarbeiter den Audit-Vorschriften des SOX [Sarbanes Oxley Act]. Vor zehn Jahren verzeichneten wir noch hunderte Compliance-Verstöße – heute praktisch null." Der Senior IT Manager des Toronto School Boards stimmte zu: „Active Roles hat die Zuverlässigkeit unseres Onboarding-Prozesses verbessert. Während der Synchronisation treten weniger Fehler auf."

7. Automatisierung der Workflows für die Identitätsverwaltung

Ein übermäßiger Einsatz manueller Prozesse zur IAM-Verwaltung ist sowohl ineffizient als auch fehleranfällig. Aus diesem Grund bevorzugen Administratoren IAM-Lösungen, mit denen sich Sicherheitsprozesse automatisieren lassen. Der IT-Verantwortliche des Aerospace-Unternehmens dazu: „Durch die Automatisierung mit Active Roles für unser Onboarding, Richtlinien und Workflows können wir sicherstellen, dass die Daten aus den Onboardings beliebiger Objekttypen in Active Directory zuverlässig sind und unsere Qualitätsstandards einhalten. Dadurch konnten wir unsere Prozesse optimieren."

> **Wir sparen erheblich Arbeitszeit, mehrere hundert Stunden pro Jahr.**

Er erklärte weiter: „Einer der kompliziertesten Aspekte, wenn es um die Active Directory-Verwaltung ohne ein Tool wie Active Roles geht, ist die Kontrolle der Vorgehensweise von Mitarbeitern. Meine Methode beim Installieren oder Einrichten eines neuen Benutzers unterscheidet sich vielleicht von meinem Kollegen. Beispielsweise können Sie für jemanden einen Satz zu befolgender Richtlinien festlegen, doch wenn Sie nicht ein Produkt wie Active Roles nutzen, liegt es ganz an dieser Person, wie diese Richtlinien interpretiert und befolgt werden. Mit Active Roles können wir diese Richtlinien erzwingen, sodass die in Active Directory übertragenen Daten ordnungsgemäß und konsistent sind. Konsistente Daten wiederum erlauben mehr Automatisierungen und gewährleisten, dass Personen und Objekte ordnungsgemäß eingerichtet sind."

Andere Mitglieder sagten zu Automatisierung:

- „Wir konnten mit der Lösung auch unsere Automatisierung verbessern. Die Automatisierung war bereits vorhanden, wurde aber verbessert. Die Lösung konnte mehr Daten aus Trillium und SAP erfassen und Active Directory mit einem offeneren Ansatz befüllen. Wir haben zwei Mitarbeiter und sparten pro Mitarbeiter mit Active Roles 0,2 Vollzeitäquivalente." – Senior IT Manager beim Toronto District School Board

- „Unsere IT-Abteilung wurde von aufwändigen Aufgaben entlastet, insbesondere dank bestimmter Workflow-Automatisierungen. Mit dem Active Roles-Synchronisierungsdienst können wir Daten der Personalabteilung verarbeiten und diese Attribute und Datenfelder direkt in Active Directory aktualisieren, anstatt das manuell oder mit Massenimporten tun zu müssen.“ – Information Security Manager bei einem Fertigungsunternehmen mit mehr als 5.000 Mitarbeitern

- „Mit Active Roles konnten wir zum ersten Mal automatisierte rollenbasierte Provisionierung einführen. Außerdem war es uns mithilfe von Workflows und den geplanten Aufgaben möglich, eine Reihe von Prozessen zu automatisieren sowie zentral zu verwalten. Auch konnten wir damit weitere Produkteinschränkungen umgehen. Dazu gehört unter anderem das Synchronisieren größerer Gruppen mit mehr als 50.000 Mitgliedern mit Azure AD.“ – Senior Business Analyst an der George Washington University

8. Zeiteinsparung und Erhöhung der Effizienz

Mit der richtigen IAM-Lösung können IT- und Sicherheitsmitarbeiter erheblich Zeit sparen. Dass bestätigte die Senior Business Analyst der George Washington University, deren Team mit Active Roles mehr erreichte und effizienter wurde. Der Technical Manager of Security bei Liberty Global hatte ähnliche Erfahrungen gemacht und stellte fest, dass die Lösung zahlreiche zeitaufwändige IT-Aufgaben überflüssig gemacht hat, insbesondere wenn Angestellte das Unternehmen verlassen.

Dieser Benutzer erklärte: „Active Roles übernimmt 10 oder 15 skriptgesteuerte Aktionen – immer auf die gleiche Weise und zur gleichen Zeit. Zuvor gab es eine ganze Liste von Aufgaben, die der Administrator übernehmen musste, beispielsweise das Postfach verbergen, den Benutzer deaktivieren oder die Gruppen entfernen. Außerdem ist der Überprüfungsverlauf dieser Lösung sehr praktisch für uns. Damit erhalten wir einen Datensatz der Änderungen, die an einem Benutzer vorgenommen wurden und erfahren, wer wann dafür verantwortlich war. Das hilft uns enorm. Da wir zahlreiche Aktivitäten auslagern, verändert sich unsere Zielgruppe. Tools wie dieses gewährleisten, dass alle Vorgänge strukturiert ablaufen und das alles auf die gleiche Weise und zur gleichen Zeit durchgeführt wird.“

> **Die Lösung hat unseren Kunden Zeit eingespart, da sie Aufgaben automatisiert, die 30 bis 45 Minuten in Anspruch nahmen.**

Einige Benutzer konnten ihre Zeiteinsparungen quantifizieren. Der CTO von BeClever IT Solutions erklärte: „Die Lösung hat unseren Kunden Zeit eingespart, da sie Aufgaben automatisiert, die 30 bis 45 Minuten in Anspruch nahmen.“ Der IT-Verantwortliche des Aerospace-Unternehmens mit 55.000 Angestellten bemerkte: „Täglich werden Mitarbeiter eingestellt und verlassen die Organisation wieder. In dieser Umgebung können wir mit Active Roles mehr als 500 Anfragen pro Woche einsparen. Die Lösung hat Verwaltungsaufgaben überflüssig gemacht, die erhöhten Aufwand für unsere IT-Abteilung bedeuteten. Jetzt müssen IT-Mitarbeiter nicht mehr die Gruppe aktualisieren, wenn jemand ein Arbeitsverhältnis bei dem Unternehmen beginnt oder beendet.“ Die Senior Business Analyst der GWU betonte: „Mit Active Roles sparen wir pro Monat mindestens zwei Wochen Arbeitszeit ein. Wir konnten unseren Arbeitsaufwand um mindestens 50 % senken.“

9. Nutzung von Richtlinien und Vorlagen für verbesserte rollenbasierte Kontrollen

Rollenbasierte Richtlinien und Vorlagen verbessern die Zugriffssteuerung, sparen Zeit und erhöhen die Genauigkeit der AD-Governance und Verwaltung. Der Mitarbeiter bei Marriott Phoenix erklärte dazu: „Die integrierten Vorlagen in Active Roles ermöglichen die Erstellung von Sicherheitsgruppen, ohne dass wir sie selbst entwickeln müssen. Die Lösung vereinfacht den Prozess erheblich, und wenn wir Änderungen vornehmen, ist es auch deutlich einfacher, sie zu überprüfen.“ Der Technical Manager of Security bei Liberty Global stimmte zu: „Active Roles ermöglicht die Nutzung von Richtlinien und bietet zahlreiche Beispielrichtlinien.“ Er fügte hinzu: „Es gibt Zugriffsvorlagen, die sehr viele Beispiele für Zugriffsvorlagen enthalten. Auch Workflows sind verfügbar, die durchaus leistungsstark sind.“

10. Dynamische Gruppen zur Risikominimierung und Automatisierung von Aktualisierungen

„Die Funktion von Active Roles, die mir am besten gefällt, sind wahrscheinlich die dynamischen Gruppen, die sich praktisch im Handumdrehen erstellen und aktuell halten lassen. Für uns ist das ein sehr wichtiger Aspekt“, so der IT-Verantwortliche des Aerospace-Unternehmens. Er fügte hinzu: „Wir erhalten regelmäßig Anfragen aus dem Unternehmen nach Gruppen, die alle Personen in einer bestimmten Abteilung umfassen. Dabei kann es sich beispielsweise um eine Verteilerliste nur für E-Mails oder eine Gruppe zur Sicherung eines Dateiservers handeln. Mit Active Roles können wir diese Gruppe erstellen und Active Roles anweisen, jedes gefundene Konto, dessen Abteilung einem bestimmten Wert entspricht, dieser Gruppe zuzuweisen.“

> **“Wir müssen nicht mehr darauf warten, dass ein Mitarbeiter jede einzelne Gruppe darauf untersucht, ob sich diese Person darin befindet.**

Die Senior Business Analyst der GWU nutzt dynamische Gruppen, um Risiken zu minimieren und die Sicherheit zu verbessern, indem verwaiste Konten – eine erhebliche Schwachstelle – entfernt werden. Sie erklärte dazu: „Wenn sich bei einer dynamischen Gruppe die Person nicht mehr im Feed aus dem Personalsystem befindet, wird sie sofort und automatisch aus dieser Gruppe entfernt. Wir müssen nicht mehr darauf warten, dass ein Mitarbeiter jede einzelne Gruppe darauf untersucht, ob sich diese Person darin befindet. Damit erfüllen wir interne Best Practices, wonach lediglich der geringstmögliche Zugriff gewährt werden soll.“

FAZIT

IAM wird immer schwieriger, da IT-Umgebungen immer komplexer und – zumindest teilweise – in die Cloud ausgelagert werden. Auch wenn Microsoft Active Directory gut für grundlegende IAM-Aufgaben geeignet ist, erfordert die Verwaltung des Identitäts- und Zugriffsmanagements hoch entwickelte und automatisierte Lösungen, die auf AD aufbauen. Benutzer von One Identity Active Roles betonten in Rezensionen auf IT Central Station, dass sich mit der richtigen Lösung die IAM-Effizienz steigern und Zeitaufwand einsparen lässt. Eine solche Lösung kann auch nicht autorisierte Änderungen minimieren und die Sicherheitssituation durch Delegierung, dynamische Gruppen, Richtlinien und Vorlagen verbessern. Weitere Effizienzsteigerungen lassen sich durch zentrale Kontrollpunkte erreichen. Lösungen wie Active Roles, die in der Cloud, in lokalen Umgebungen sowie in Hybridmodi arbeiten können, bilden die Basis für ständige Verbesserungen des Identitäts- und Zugriffsmanagements sowie der allgemeinen Sicherheitslage eines Unternehmens – auch angesichts dynamischer IT- und Sicherheitsentwicklungen.

INFOS ÜBER IT CENTRAL STATION

Beurteilungen durch Benutzer, offene Gespräche und mehr für Technologieprofis in Unternehmen.

Das Internet hat die Art und Weise, wie wir Kaufentscheidungen treffen, vollständig verändert. Bevor wir Elektronikartikel kaufen, einen Hotelaufenthalt buchen, uns einen Arzttermin geben lassen oder ein Restaurant wählen, lesen wir heute Bewertungen und rufen entsprechende Webseiten auf, um uns über die Erfahrungen echter Benutzer zu informieren. Doch in der Welt der Technologieprodukte für Unternehmen kommen die meisten Informationen, die wir online oder in unserem Posteingang erhalten, von Herstellern und Vertreibern. In Wirklichkeit möchten Sie objektive Informationen von anderen Benutzern. IT Central Station bietet Technologiefachleuten eine Community-Plattform, auf der sie Informationen über Unternehmenslösungen austauschen können.

IT Central Station engagiert sich für die Bereitstellung von wertvollen, objektiven und relevanten Informationen, die von Benutzern zur Verfügung gestellt werden. Wir prüfen alle Beurteilenden mit einem dreifachen Authentifizierungsprozess und schützen Ihre Privatsphäre durch die Bereitstellung einer Umgebung, in der Sie anonym posten und Ihre Ansicht frei wiedergeben können. Auf diese Weise wird die Community zu einer wertvollen Ressource, die sicherstellt, dass Sie Zugang zu den richtigen Informationen erhalten und sich mit den richtigen Personen vernetzen können, wann immer Sie das benötigen.

www.itcentralstation.com

IT Central Station unterstützt oder empfiehlt keine Produkte oder Dienstleistungen. Die Ansichten und Meinungen von Benutzern, die in diesem Dokument, auf Websites von IT Central und anderem Material von IT Central Station wiedergegeben werden, spiegeln nicht die Meinung von IT Central Station wider.

INFOS ÜBER ONE IDENTITY

Das Quest Software-Unternehmen One Identity ermöglicht es Unternehmen, lokal, in der Cloud oder in einer Hybrid-Umgebung eine identitätszentrierte Sicherheitsstrategie zu implementieren. Mit unserem einzigartigen, umfassenden und integrierten Portfolio an Identity Management-Lösungen, darunter Kontoverwaltung, Identity Governance, Administration und Privileged Access Management, können Unternehmen ihr vollständiges Potenzial entfalten, da die Sicherheit gewährleistet wird, weil Identitäten das Herzstück eines Programms sind. Dadurch kann für verschiedene Benutzertypen, Systeme und Daten der jeweils angemessene Zugriff bereitgestellt werden. Weitere Informationen erhalten Sie unter OneIdentity.com.