Cornell wird in die Ehrenliste für Active Directory Sicherheit aufgenommen

Active Roles von One Identity hilft der Cornell University dabei, eine verteilte, vielfältige und unzusammenhängende AD-Umgebung abzusichern

Land: **USA**

Mitarbeiter: **Lehrkräfte 1.679 | Verwaltungsmitarbeiter 8.000**

Studenten: **23.000**

Branche: **Hochschulwesen**

Website: **www.cornell.edu/about/**

Herausforderungen

- Schaffung von Konsistenz in einer stark verteilten und vielfältigen AD-Umgebung
- Schutz der Daten der Universität vor AD-basierten Angriffen
- Vermeidung menschlicher Fehler und des Missbrauchs von AD-Administrator-Anmeldeinformationen

Ergebnisse

- Das gewünschte komplexe Delegierungsmodell für AD-Administratoren wurde implementiert.
- Die Unix/Linux Authentifizierung und -Autorisierung auf Basis von AD-gestützten Verwaltungsaufgaben wurden optimiert.
- Das Risiko eines uneingeschränkten Administratorzugriffs über alle AD-Domänen hinweg wurde beseitigt, ohne dabei die IT-Aktivitäten zu beeinträchtigen.

Lösungen

- Active Directory Sicherheit

Produkte

- Active Roles von One Identity

Im Hochschulwesen lauern überall Risiken. Angesichts der Fülle an personenbezogenen Daten, Finanzdaten und geistigem Eigentum sind Universitäten bevorzugte Ziele für Kriminelle. Die Situation wird darüber hinaus noch dadurch verschlimmert, dass ein Großteil der IT-Aufgaben an Hochschulen von Studenten, Auftragnehmern und befristet Beschäftigten über weit verstreute und nur lose kontrollierte Netzwerke abgewickelt wird. Glücklicherweise hat die Cornell University eine Lösung für diese seit Langem bestehenden Herausforderungen gefunden.

„Eine Kompromittierung unserer Active Directory Domänen ist eine unserer größten Sicherheitsbedenken“, berichtete Muhammad Arif, Identity Management, CIT an der Cornell University. „Wir dürfen uns nicht mit dem Diebstahl sensibler Daten und dem Reputationsschaden für die gesamte Universität abfinden, den eine solche Kompromittierung mit sich bringen würde.“ „Früher hatten wir eine sehr dezentrale Umgebung mit mehr als hundert völlig unabhängigen Active Directory (AD)-Domänen“, sagte Arif. „Es gab keine Überwachung dieser Domänen. Es interessierte nicht, wie sie konfiguriert waren, inwieweit die Sicherheitseinstellungen umgesetzt wurden, welche Art der Authentifizierung es gab und welche Zugriffsrechte gewährt wurden. All das waren Faktoren, die die Daten und den Ruf der Universität gefährdeten. Wir hatten keine Kenntnis davon, wie sicher diese Domains waren, und keinen Einblick in die Tätigkeiten eines Mitarbeiters der IT-Abteilung.“

Eine der größten Herausforderungen bei der Absicherung von AD sind die Einschränkungen der nativen Tools. Das AD-Administratorkonto wird in der Regel von allen IT-Mitarbeitern gemeinsam genutzt, die die entsprechenden Berechtigungen benötigen. Die Berechtigungen werden in der Regel nach dem „Alles-oder-nichts"-Prinzip vergeben, es gibt keine individuelle Rechenschaftspflicht für Aktionen, die als Administrator ausgeführt werden. Und Aufgaben wie die Delegierung, die vorübergehende Erweiterung von Rechten sowie die Duplizierung von Richtlinien domänenübergreifend sind äußerst schwierig, wenn nicht gar unmöglich.

„Angesichts einer derart stark verteilten AD-Umgebung und der Vielzahl von Administratoren in verschiedenen Abteilungen benötigten wir eine Möglichkeit, die Zugriffsrechte zur Verwaltung von AD-Objekten zu delegieren", erklärte Arif. „Ferner müssen wir die Möglichkeit haben, Administratoren in anderen Abteilungen die Befugnis zu erteilen, Zugriffsrechte weiterzugeben. Mit diesem Delegierungsmodell entstand die Notwendigkeit, die Benennung von Objekten in AD sowie die Protokollierung der mit Administratorrechten durchgeführten Aktionen ordnungsgemäß zu überprüfen." Die Universität kam zu dem Schluss, dass sie zur Bewältigung der Sicherheitsherausforderungen, die sich aus ihrer AD-Umgebung ergaben, am besten nach einer handelsüblichen Standardsoftware suchen sollte. Diese muss die nativen Funktionen der AD-Tools um die gewünschte Detailgenauigkeit und Kontrollmöglichkeiten erweitern, um so Risiken zu verringern und die Sicherheit zu erhöhen. „Wir suchten nach einer Lösung, die unseren Anforderungen gerecht wird, ausgereift ist und sich bei Kunden bewährt hat, deren Umgebungen ähnliche Herausforderungen und Komplexitäten aufweisen wie unsere", erklärte Arif. „Zudem suchten wir einen Anbieter, der einen hervorragenden Support bietet – einen, auf den wir uns verlassen können, wenn wir Hilfe benötigen."

> **Active Roles bot von Anfang an mehrere wichtige Funktionen und Merkmale, darunter die Delegierung und Weiterübertragung von Berechtigungen, die Durchsetzung von Namenskonventionen, den Änderungsverlauf sowie die Durchsetzung von Richtlinien für AD-Objekte.**
>
> *Muhammad Arif, Identity Management, CIT, Cornell University*

> **Mit Active Roles haben wir ein gutes Modell für die Verwaltung von Delegierungen, Namensstandards, OU-Strukturen und den Zugriff auf AD für mehrere Hundert Administratoren entwickelt. Und dieses Modell ist mittlerweile seit fast zehn Jahren im Einsatz.**
>
> *Muhammad Arif, Identity Management, CIT, Cornell University*

Active Roles von One Identity erfüllt seit fast 20 Jahren die Anforderungen von mehr als 3.500 Unternehmen, darunter die Cornell University, hinsichtlich der AD-Administration und -Sicherheit. Die Lösung überwindet die Einschränkungen nativer Tools durch Automatisierung, Workflows, Genehmigungsverfahren und die Zentralisierung von Verwaltungsaufgaben für AD-Konten, wie die Provisionierung und Gruppenverwaltung. Des Weiteren ermöglicht das rollenbasierte Zugriffsparadigma von Active Roles Unternehmen, die Sicherheit für Administratoren nach dem Prinzip der geringstmöglichen Zugriffsrechte umzusetzen. Dafür stehen zahlreiche flexible Optionen zur Sicherheitsoptimierung zur Verfügung wie temporäre Gruppen und vorlagenbasierte Workflows. „Active Roles bot von Anfang an mehrere wichtige Funktionen und Merkmale, darunter die Delegierung und Weiterübertragung von Berechtigungen, die Durchsetzung von Namenskonventionen, den Änderungsverlauf sowie die Durchsetzung von Richtlinien für AD-Objekte", fügte Arif hinzu. „Die einfache Anpassung der Weboberfläche und die Unterstützung der von uns verwendeten Programmierschnittstellen, darunter VBScript, PowerShell und SPML, gab uns mehr Flexibilität. Dank der Anpassungsmöglichkeiten konnten wir den Zugriff so implementieren, dass Administratoren nur ihre eigenen OU in AD einsehen und bearbeiten können."

Mit Active Roles kann die Universität ihre vielfältigen AD-Umgebungen in der Gewissheit betreiben, dass nichts geschehen kann, was aus dem Rahmen der festgelegten Richtlinien fällt (und viele Aktionen können nun ganz ohne Eingreifen der IT-Abteilung ablaufen). Ferner erhalten Administratoren ausschließlich die Berechtigungen, die sie zur Erfüllung ihrer Aufgaben benötigen – nicht mehr und nicht weniger –, und alle Aktionen werden geprüft und nachverfolgt und können bei Bedarf sogar rückgängig gemacht werden.

ONE IDENTITY

„Mit Active Roles haben wir ein gutes Modell für die Verwaltung von Delegierungen, Namensstandards, OU-Strukturen und den Zugriff auf AD für mehrere Hundert Administratoren entwickelt", erklärt Arif. „Dieses Modell hat sich nun schon seit fast zehn Jahren bewährt. Außerdem ist es uns gelungen, mithilfe von Skripten, virtuellen Attributen und Webanpassungen neue Funktionen zu implementieren, um neuen Anforderungen gerecht zu werden." „Ich glaube, dass durch Active Roles das Vertrauen in die Fähigkeit unserer zentralen IT-Organisation, zuverlässige Services zu liefern, gestiegen ist – ganz zu schweigen von der Verringerung des Risikos und der entsprechenden Erhöhung der Sicherheit." Muhammad Arif, Identity Management, CIT, Cornell University

Ein wesentlicher Vorteil von „Active Roles von One Identity" ist, dass die Lösung über die Grenzen von AD hinaus erweitert werden kann. Sie unterstützt zudem Entra ID (und alles, was damit zusammenhängt) und lässt sich über eine Active Directory-Brücke wie One Identity Authentication Services auf Unix/Linux Systeme sowie über den SCIM-Standard auf eine Vielzahl von Webanwendungen ausweiten. „Da wir eine Bildungs- und Forschungseinrichtung sind, nutzen viele Lehrkräfte, Mitarbeiter und Studenten Linux Systeme als ihr Hauptarbeitssystem", sagte Arif. „Nachdem AD zum zentralen Anbieter von Authentifizierungs- und Autorisierungslösungen geworden war, benötigten wir eine Möglichkeit, die Linux Systeme für diese Funktionen in AD zu integrieren." Wir nutzen Active Roles, um Unix Attribute auf der Grundlage von AD-Benutzer- und Gruppenobjekten automatisch zu veröffentlichen. „Dadurch erhalten die Abteilungsadministratoren die Möglichkeit, Benutzerkonten innerhalb von Active Roles als ‚Unix Konten' freizuschalten. Das bedeutet, dass die Abteilungsadministratoren diese Aufgabe selbst übernehmen können, ohne bei Bedarf eine Anfrage an die zentrale IT-Abteilung richten zu müssen, um einzelne Unix Konten freizuschalten." „Ich glaube, dass durch Active Roles das Vertrauen in die Fähigkeit unserer zentralen IT-Organisation, zuverlässige Dienste zu liefern, gestiegen ist – ganz zu schweigen von der Verringerung des Risikos und der entsprechenden Erhöhung der Sicherheit", stellte Arif fest.

> **Ich glaube, dass durch Active Roles das Vertrauen in die Fähigkeit unserer zentralen IT-Organisation, zuverlässige Services zu liefern, gestiegen ist – ganz zu schweigen von der Verringerung des Risikos und der entsprechenden Erhöhung der Sicherheit."**
>
> *Muhammad Arif, Identity Management, CIT, Cornell University*

Über One Identity

One Identity bietet vertrauenswürdige Identitätssicherheit für Unternehmen weltweit, um alle Identitäten zu schützen, ob menschlich oder nicht menschlich. Mit flexiblen Bereitstellungsoptionen und Abonnementbedingungen, von selbstverwaltet bis vollständig verwaltet, lassen sich unsere Lösungen direkt in die Identitäts-Fabric eines Unternehmens einbinden, um den Identitätsperimeter zu stärken, das Risiko von Sicherheitsverletzungen zu verringern und die Governance und Compliance in großem Umfang zu gewährleisten. One Identity mit Hauptsitz in Cork, Irland, dem 80 der Fortune 100 Unternehmen vertrauen, ist ein führender Anbieter von integrierter Identity Governance und Administration (IGA) und Privileged Access Management (PAM) für kompromisslose Identitätssicherheit. Weitere Informationen erhalten Sie auf www.oneidentity.com.

CaseStudy-Cornell-University-PG-DE-WL-105183

ONE IDENTITY