Verstärkung von Active Directory – für mehr Sicherheit und Effizienz

RECHERCHIERT VON:

Jay Bretzmann
Program Director,
Security Products, IDC

Frank Dickson
Program Vice President,
Cybersecurity Products, IDC

Active Directory und Azure Active Directory sind die Basis vieler erfolgreicher Identitätsmanagementprogramme. Aufgrund des Risikos von Sicherheitsverletzungen sollten Unternehmen jedoch die nativen Active Directory-Funktionen möglichst mit Toolkits für mehr Effizienz und Sicherheit verstärken.

Was wichtig ist

Identitätssicherheit steht bei Führungskräften im Bereich Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) ganz oben auf der Tagesordnung, v. a. bei ihrer Suche nach Lösungen zur Absicherung bestehender Angriffsflächen. 95 % aller Fortune-1000-Unternehmen vertrauen bei Management und Speicherung von Identitäts- und Kontodaten auf Microsoft Active Directory und Azure Active Directory (Azure AD). Daher hat die Verstärkung der Sicherheit hier kritische Bedeutung.

Active Directory (einschließlich Azure AD) ist für sich allein ein leistungsfähiges Managementtool. Seine nativen Funktionen lassen sich jedoch erweitern und ausbauen, um die Benutzererfahrung über Sicherheit, Identität und fachliche Rollen hinweg individuell zu gestalten.

Dieser Industry Spotlight behandelt die Möglichkeiten zur Schließung von Lücken bei Management und Sicherheit von Active Directory und soll so einen Leitfaden für Unternehmen bieten, die Schwachstellen begrenzen und die IT-Sicherheit in Active Directory-Umgebungen verstärken müssen.

In diesem Spotlight

Klicken Sie hier, um die entsprechenden Abschnitte aufzurufen.

Active Directory bildet in den meisten Unternehmen die Basis des Identitäts- und Zugriffsmanagements und ist somit wahrscheinlich die wichtigste Technologie im Netzwerk.

Einführung

Sicherheit und Effizienz stehen bei IAM-Führungskräften ganz oben auf der Tagesordnung, v. a. wenn sie nach Lösungen zur Abwehr von Angriffen und Ermöglichung von Zero Trust suchen. Active Directory bildet in den meisten Unternehmen die Basis des IAM und ist somit wahrscheinlich die wichtigste Technologie im Netzwerk. Immer mehr Systeme und Anwendungen sind im Hinblick auf Authentifizierungs-, Richtlinien-, Berechtigungs- und Konfigurationsmanagement von Active Directory und Azure AD abhängig.

Die Absicherung von Active Directory/Azure AD spielt für die Risikokontrolle und die Gewährleistung der Compliance eine entscheidende Rolle. Aber die Beibehaltung eines sauberen, organisierten und sicheren Zustands von Active Directory stellt eine Herausforderung dar, v. a. bei den Benutzerkonten, welche die Basis für die Authentifizierung und den Zugriff auf Netzwerke, Systeme und Anwendungen darstellen. Ohne geeignete Tools lassen sich Benutzerkonten über mehrere Plattformen und ihren gesamten Lebenszyklus (von der Erstellung bis zur Schließung) hinweg nur schwer managen. Wenn der Wechsel zu Azure AD noch nicht erfolgt ist, muss Active Directory unbedingt möglichst sauber organisiert werden, damit sich Fehler nicht summieren und Sicherheitsprobleme nicht verschleppt werden. Werden fehlerhafte Daten von Active Directory in Azure AD synchronisiert, verschlimmert sich die Lage nur weiter. Daher ist der Einsatz eines Toolkits für das Active Directory-Management als Lösung zur Unterstützung bei der Verzeichnisbereinigung vor der Migration nach Azure AD ein wichtiger Schritt.

Sicherheitsgewinne sind für Active Directory und Azure Active Directory in Reichweite

Während „Zero Trust Security" der Slogan des Tages ist – lautet der andere „digitale Transformation". Unternehmen streben die Einbindung von Technologie in ihre geschäftlichen Abläufe an: für bessere Sicherheit, besser auf die Kunden abgestimmte Lösungen und mehr Agilität. Ohne Disziplin, Sorgfalt und gezielte Planung kann die digitale Transformation für Sicherheits- und Identitätsfachkräfte zu einem Minenfeld werden, da jede Identität leicht zu einem (einzigartigen) rollenbasierten Unikat werden kann.

Daher fragen sich Unternehmen oft, wie sich Zero Trust in ihrer Umgebung praktisch umsetzen lässt. Angesichts der anhaltenden Auswirkungen der COVID-19-Pandemie weltweit und der Anpassung des geschäftlichen Betriebs daran, hat sich die digitale Transformation zur betrieblichen Resilienz weiterentwickelt. Unternehmen versuchen, den Mangel an Sicherheits-Fachkräften und die sich daraus ergebenden Anforderungen an das Personal zu bewältigen, und gleichzeitig suchen viele Firmen nach einer für sie geeigneten, stabilen und modernen Zero-Trust-Plattform.

Strenge Endpoint-Zugriffskontrollen, einfacher und sicherer Zugriff und die Eliminierung von Unsicherheiten bei der Bereitstellung sind sicherlich die wesentlichsten Merkmale von Zero Trust. All diese Merkmale stützen sich auf eine gemeinsame Säule der Sicherheit: die Identität. Das Fundament dieser Säule ist Microsoft Active Directory. Identitätsexperten sind nun mit der Frage konfrontiert, wie die volle Leistungsfähigkeit von Active Directory zur Förderung der digitalen Transformation und von Zero Trust eingespannt werden kann.

Active Directory

Active Directory ist die Basis der Identitätsstrategie der meisten Unternehmen. Active Directory spielt für Sicherheit und IT eine grundlegende Rolle: Es autorisiert alle Benutzer und Rechner in einem Netzwerk vom Windows-Domänentyp. Dafür weist es einer Identität Richtlinien auf Basis definierter Rollen oder Attribute zu und setzt diese durch. Angesichts des zunehmenden Trends zu SaaS und der Suche nach Zero-Trust-Sicherheitsmodellen (bedingt durch die Hybridarbeit) ist die Bedeutung von Active Directory noch gewachsen, da Azure AD die integrierte Lösung für das Identitätsmanagement in Office 365 ist.

Azure Active Directory

Azure AD ist das neueste Angebot der Produktfamilie und soll eine Grundlage für das hybride Arbeiten bereitstellen. Azure AD ist eine von vielen Sicherheitstechnologien, die zur Unterstützung von Microsoft Azure (dem Cloud-Dienst) entwickelt wurden. Wie auch bei den anderen Lösungen eröffnet sich hier unmittelbar die Möglichkeit zur Erweiterung der Optionen von Azure-Kunden, da ein Massenmarkt für einen auf Standards basierenden Ansatz für Identität und Datenzugriff entsteht. Azure AD hat den offenen Kreis für die Definition von SAML-, OAuth-, OData- und SCIM-kompatiblen kommerziellen Implementierungen geschlossen, welche sowohl kostenlos als auch in kostenpflichtigen (Premium-)Lösungen verfügbar sind.

Beim Kauf von Premium-Lizenzen wollen Kunden von einer oder mehreren der folgenden Leistungen profitieren:

- Unbegrenztes einmaliges Anmelden (Single Sign-On, SSO)
- Kennwortzurücksetzung per Selbstbedienung (Self-Service Password Reset, SSPR)
- Berechtigungsmanagementsystem (Entitlement Management System, EMS)
- Management privilegierter Identitäten (Just In Time [JIT])
- Azure AD Conditional Access
- Azure AD Identity Protection

Microsoft befindet sich hinsichtlich einer dominierenden Rolle bei der Cloud-Identität in der Pole-Position und ist sich dessen durchaus bewusst. Diesen Wettlauf kann Microsoft nur verlieren, wenn der Konzern die Anforderungen an die IT-Konnektivität und -Kommunikation der Plattformen von Drittanbietern nicht erfüllt. Die neu entwickelten Standardspezifikationen der Branche für Webanwendungen sind derzeit noch so unklar, dass der Einsatz einer vorhandenen, kommerziellen Implementierung empfehlenswert ist. Azure AD verfügt bereits über mehr als 1000 SSO-Implementierungen und 120 SCIM-Implementierungen. Das lässt sich mit der Entscheidung für DOS in den Anfängen des Personal Computings vergleichen: Sichert man sich einen ausreichenden Anteil am frühen Markt und beteiligt sich an der Definition zukünftiger Standards, hat man mit hoher Wahrscheinlichkeit ein nachhaltiges Geschäft.

Azure AD managt aktuell über 425 Millionen aktive Benutzer pro Monat (hauptsächlich Office 365-Abonnenten) und verarbeitet über 90 Milliarden Authentifizierungsanfragen pro Tag. Der Premium-Kundenstamm umfasst 300.000 Firmen und wächst schnell. Es gibt noch viel Luft nach oben, und die Entwicklung zu passwortloser Technologie wird rasch an Tempo aufnehmen, da Azure AD Conditional Access Kontrollen jetzt automatisch implementieren kann: basierend auf Benutzerreputation, Gerätestatus, Netzwerkquelleninformationen und laufender Threat Intelligence.

Optimierung von Active Directory für Sicherheitsanwendungsfälle mit neuen Tools

Active Directory und Azure AD sind zwar die Basis der IT, wurden jedoch beide meist als IT-Zugriffsfunktion eingesetzt. Wenn spezialisierte IT-Fachkräfte, insbesondere Sicherheitsexperten, die Leistungsfähigkeit von Active Directory geschickt für mehr Sicherheit und Integrität nutzen wollen, stellen sie oft fest, dass bestehende Tools und Schnittstellen nicht für ihre anspruchsvollen Anforderungen gebaut sind.

Zu den für moderne Sicherheitsexperten entscheidenden Merkmalen gehören:

- Delegieren von privilegierten Berechtigungen
- Ausgereifter rollenbasierter Zugriff auf Attribute und Richtlinien
- Automatisierung des Lebenszyklusmanagements von Identitäten
- Vereinfachung von Arbeitsabläufen und Zugriffsbereitstellung über mehrere Geräte hinweg anhand von PKI-Zertifikaten und Push-Technologie
- Erleichterte Berichterstellung für Governance und Compliance
- Integration von Active Directory in Anwendungen über APIs zum Austausch des Identitätskontextes
- Ermöglichung von Automatisierung (Robotic Process Automation, RPA) für weniger Personalaufwand

Zwar kann Active Directory für Sicherheitszwecke genutzt werden, aber es wurde nicht allein für Sicherheitsexperten entwickelt, sondern ist eine Allzweckplattform mit vielen Zielgruppen. Aus diesem Grund gibt es nun neue Tools zur Ergänzung von Active Directory, die eine umfassendere Lösung für den Bedarf von Sicherheits- und Identitätsexperten beim Management von Active Directory bieten.

Vorteile

Active Directory verfügt über die erforderlichen Komponenten für die erfolgreiche Bereitstellung einer Identitätsplattform. Mit dem Unternehmenswachstum müssen auch Sicherheitskomponenten verbessert und skaliert werden. Ziel ist die Bereitstellung erweiterter Active Directory-Managementtools, mit denen Identitätssicherheitsexperten die Kapazitäten ausschöpfen und Sicherheitsverletzungen verhindern können: durch die Begrenzung von Schwachstellen, Gefahren und kompromittierten Anmeldedaten, die laut IDC-Studie für 52 % der jüngsten IaaS-Sicherheitsverletzungen verantwortlich sind (siehe **Abbildung 1**). Für 14 % der jüngsten IaaS-Sicherheitsverletzungen wurde das „Fehlen ausreichender Sicherheitstools" als Grund genannt – und dabei ist beachtenswert, dass die Behebung jeder Sicherheitsverletzung die Unternehmen Millionen kostet (laut 2019 Cost of a Data Breach Report des Ponemon Institute belaufen sich die Kosten einer Sicherheitsverletzung auf durchschnittlich 3,92 Millionen USD). Die sich abzeichnende Bedrohung und ihre Tragweite führen zur Entwicklung und Einführung neuer Sicherheitstools, um Abhilfe zu schaffen.

Für die Gewährleistung und Verbesserung der Sicherheit brauchen Unternehmen Tools, mit denen Sicherheitsexperten genauer, effizienter und effektiver arbeiten können. Ziel dieser Tools ist die Vereinfachung des Managements komplexer Umgebungen: mit Funktionen wie der einfachen Delegierung und des Managements von Berechtigungen sowie der Gewährleistung der Datenkonsistenz zwischen Active Directory-Bereitstellungen. Automatisierung ist von grundlegender Beteutung: Sie erleichtert Kontoaufgaben, das dynamische Gruppenmanagement, die Erstellung von Arbeitsabläufen und das Change Management.

Vorteile von Active Directory Management Toolkits

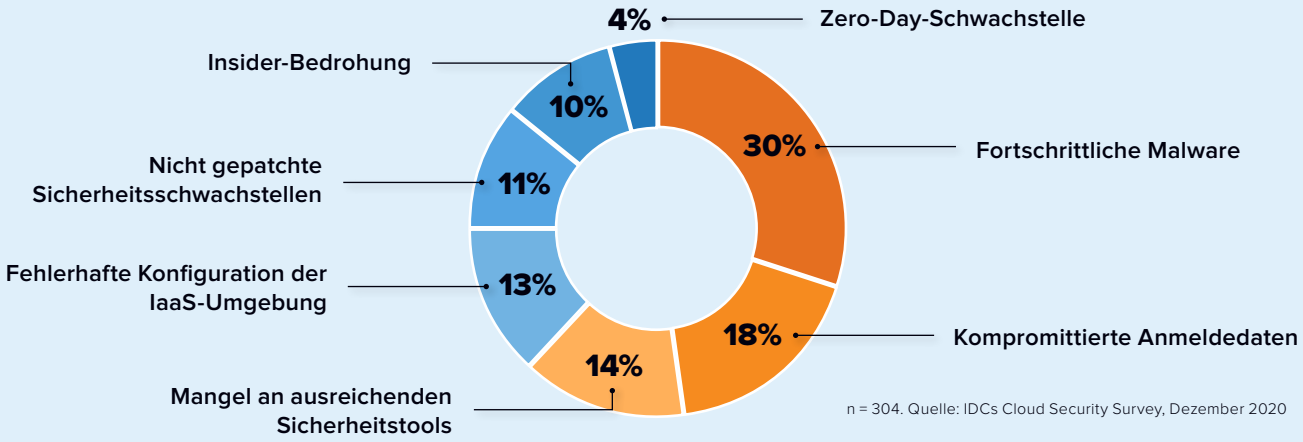
Unternehmen, die die gezielte Verbesserung ihrer Active Directory- und Azure AD-Umgebungen anstreben, können anhand folgender Funktionen von mehr Effizienz und Sicherheit profitieren:

- Einfacheres Management komplexer Umgebungen
- Ermöglichung von Zero Trust und privilegierter Sicherheit für Active Directory/Azure AD
- Automatisierung von Active Directory/ Azure AD-Kontoaufgaben und dynamischer Gruppenverwaltung
- Delegierung und Management von Berechtigungen
- Erstellung von Arbeitsabläufen und Handhabung von Änderungen, v. a. bei Fusionen und Übernahmen sowie Standortverlegungen/Remote Work
- Gewährleistung der Datenkonsistenz und Durchsetzung von Richtlinien

Von kritischer Bedeutung ist die Möglichkeit, einem Mitarbeiter in einer Abteilung die Berechtigung zur Erstellung neuer Benutzer zu erteilen – ohne volle Berechtigungen als Active Directory-Administrator. Ohne ein Toolkit zum Ausbau von Active Directory wäre die Zuweisung derartiger delegierter Berechtigungen nicht möglich.

ABBILDUNG 1
Faktoren bei Sicherheitsverletzungen

F: Was war bei der jüngsten Sicherheitsverletzung in Ihren IaaS-Umgebungen der wichtigste ursächliche Faktor hierfür?



n = 304. Quelle: IDCs Cloud Security Survey, Dezember 2020

Von kritischer Bedeutung ist die Möglichkeit zur Zuweisung von Berechtigungen – ohne volle Berechtigungen als Active Directory-Administrator zu vergeben. Ohne ein Toolkit zur Erweiterung von Active Directory wäre die Zuweisung derartiger delegierter Berechtigungen nicht möglich.

Überlegungen zu One Identity für Sicherheit, Automatisierung und Effizienz bei Active Directory

One Identity möchte den Bedarf von Sicherheits- und Identitätsexperten beim Management von Active Directory und Azure AD mit One Identity Active Roles decken. Tausende Unternehmen weltweit verlassen sich auf Active Roles als ihre Plattform für die Automatisierung von Benutzerkonten und das Gruppenmanagement. Diese Unternehmen setzen Active Roles für die Bereitstellung von Identitätsmanagement-Funktionen ein. Sie ermöglichen Sicherheits- und Identitätsexperten ein effizienteres und effektiveres Arbeiten durch den Einsatz von Automatisierung für die Delegierung und die Schaffung einer zentralen Stelle für die Administration.

Zu den wichtigsten Vorteilen gehören:

- Vereinfachte Active Directory/Azure AD-Administration
- Automatisierung von Active Directory/Azure AD-Kontoaufgaben, wenn Benutzer neu zum Unternehmen kommen, die Position wechseln oder das Unternehmen verlassen
- Regelung des Administratorzugriffs für mehr Sicherheit von privilegierten AD-Konten
- Unterstützung mehrerer Betriebssysteme

Die Funktionen von Active Roles, die speziell auf die hohen Anforderungen von Sicherheitsexperten eingehen, umfassen:

- Management aller Systeme über eine zentrale Stelle für die Administration oder eine einzige Oberfläche („Single Pane of Glass“)
- Schnellere Bereitstellung mithilfe vereinfachter Zugriffsvorlagen

Darüber hinaus bietet Active Roles folgende Funktionen:

- Vereinfachte, aber leistungsstarke Workflow-Engine
- „Leitplanken“ zur Gewährleistung der Datenkonsistenz in Active Directory
- Änderungshistorie mit „Wer/Was/Wann/Wo“ für bestimmte Objekte

Herausforderungen

Wie so oft, gilt auch für Identitätsplattformen, dass man das herausbekommt, was man hineinsteckt. Active Directory ist da keine Ausnahme. Active Roles kann leistungsfähige Tools für Automatisierung und Datenvalidierung für ein effizienteres Arbeiten der Sicherheitsexperten bereitstellen, Unternehmen müssen jedoch Einsatz zeigen, um die Plattform optimal auszuschöpfen. Active Directory kann die leistungsstärkste Sicherheitsplattform oder die größte Schwachstelle eines Unternehmens sein: Die Entscheidung darüber trifft das Unternehmen. Mit dem richtigen Toolkit für das Management von Active Directory zu seiner Erweiterung rücken erhöhte Sicherheit und Effizienz in Reichweite.

Fazit

Active Directory ist eine Identitätsplattform, die die Basis moderner Unternehmen bildet. Sie ist ein wesentlicher Bestandteil von Sicherheit und IT. Active Directory authentifiziert und autorisiert alle Benutzer und Rechner in einem Netzwerk vom Windows-Domänentyp. Dafür weist es Richtlinien auf Basis definierter Rollen oder Attribute einer Identität zu und setzt diese durch. Ein Großteil der digitalen Transformation steht in Verbindung mit Active Directory und seinem Cloud-Äquivalent Azure AD.

Wie jede leistungsfähige Plattform hat Active Directory viele Zielgruppen, u. a. IT, Betrieb, Compliance und Sicherheit, die jeweils eigene Zwecke und Absichten verfolgen. Eine Allzweckplattform kann – unabhängig von ihrer Leistungsfähigkeit – nicht die gezielten Anforderungen aller Anwendungsfälle geeignet erfüllen. Seit der Einführung von Active Directory im Jahr 1999 und seiner darauffolgenden Verbreitung in Unternehmen ist eine Optimierung von Active Directory für den Anwendungsfall Sicherheit erforderlich geworden: damit Sicherheitsexperten sowohl effizienter automatisieren als auch Daten effektiver validieren können. IDC ist der Überzeugung, dass der Markt für Managementtools für Active Directory weiter an Bedeutung gewinnen wird, und dass die digitale Transformation weiterhin immersive Erfahrungen für das hybride Arbeiten fördern wird. One Identity bieten sich große Erfolgschancen, wenn es ihnen gelingt, die in diesem Dokument beschriebenen Anforderungen mit Active Roles zu erfüllen.

Wie jede leistungsfähige Plattform hat Active Directory viele Zielgruppen, u. a. IT, Betrieb, Compliance und Sicherheit, die jeweils eigene Zwecke und Absichten verfolgen.

ÜBER DIE ANALYSTEN

Jay Bretzmann
Program Director,
Security Products, IDC

Jay Bretzmann ist Program Director für IDC Security Products und verantwortlich für Identity & Digital Trust und Cloud Security. Bretzmanns Schwerpunkte sind Identitätsmanagement, Privileged Access Management, Identity Governance, B2C-Identitätsmanagement und eine Vielzahl anderer Themen zu Identität und Cloud-Sicherheit.

Mehr über Jay Bretzmann

Frank Dickson
Program Vice President,
Cybersecurity Products, IDC

Frank Dickson leitet das für spannende Studien in folgenden Bereichen zuständige Team: Netzwerksicherheit, Endgerätsicherheit, Cybersicherheits-Analytik, -Intelligenz, -Reaktion und -Orchestrierung (AIRO), Identi-tät und digitales Vertrauen, Recht, Risiko und Compliance, Datensicherheit, IoT-Sicherheit und Cloud-Sicherheit. Thematisch unterstützt er Kunden mit Einsichten und Ratschlägen zu einer großen Bandbreite von IT-Sicherheitsprodukten, u. a. Endpunktsicherheit, Identitäts- und Zugriffsmanagement, Authentifizierung und Gefahrenanalytik sowie zu in der Entwicklung begriffenen Produkten zum Schutz von sich verändernden Architekturen und Geschäftsmodellen.

Mehr über Frank Dickson

MITTEILUNG DES SPONSORS

Wenn Identitäten über verschiedene Verzeichnisse und mehrere Systeme verteilt sind und Benutzerberechtigungen locker gehandhabt werden, ist Ihr Unternehmen für Cybersicherheits-Risiken anfällig. One Identity Active Roles und Microsoft AD/Azure AD liefern im Zusammenspiel höchste Leistung – für mehr Sicherheit, Effizienz und geringere Risiken.

Erfahren Sie hier mehr: One Identity

Erfahren Sie hier mehr: Microsoft and Azure

IDC Custom Solutions

Diese Veröffentlichung wurde von IDC Custom Solutions erstellt. Als weltweit führender Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informationstechnologie und der Telekommunikation sowie der Verbrauchertechnologiemärkte hilft IDC Custom Solutions Kunden bei Planung, Marketing, Vertrieb und Erfolg auf dem Weltmarkt. Wir erstellen umsetzbare Marktinformationen und einflussreiche Content-Marketing-Programme, die messbare Ergebnisse liefern.