KuppingerCole-Bericht

EXECUTIVE VIEW

von Martin Kuppinger | April

ManageEngine AD360

ManageEngine AD360 ist ein Werkzeug speziell zum tiefgehenden Microsoft-Active-Directory-Management und verbundener Systeme wie Microsoft Office 365. Seine Fähigkeiten gehen durch zusätzliche Authentifizierungsfunktionen, UBA (Nutzerverhaltensanalyse) bis hin zu SSO (Einmalanmeldung) an unterschiedlichen Cloud-Services weit über reine Berechtigungen hinaus. Die Kernfunktionen des Werkzeugs liegen dabei in der Unterstützung eines effizienten, automatisierten Microsoft-Active-Directory-Managements sowie der Risikominimierung in solchen Umgebungen durch Automatisierung und Optimierung von Berechtigungen.

von **Martin Kuppinger**
mk@kuppingercole.com
April 2019

Inhalt

Zugehörige Forschungsdokumente

Architecture Blueprint: Access Governance and Privilege Management - 79045

Executive View: ManageEngine Password Manager Pro - 70613

Leadership Compass: Privileged Access Management - 79014

KuppingerCole Executive View
ManageEngine AD360
Berichtsnummer:
79070

1 Einleitung

Digitale Identität ist bei kleinen bis mittelständischen Unternehmen (SMB) ein unverzichtbares Element moderner Geschäftsführung. Allerdings wird digitale Identität laut Cyberkriminalitätsberichten auch Jahr für Jahr als primärer Angriffsvektor auf SMB missbraucht. Bei vielen SMB fehlt es an gut besetzten IT-Abteilungen, die sich komplizierten Aufgaben wie Einsatz, Wartung und Absicherung komplexer IAM-Lösungen hinreichend widmen können. Ein Faktor, der den Bedarf an zielgerichteten Lösungen anfeuert, die solche Unternehmen beim Management ihrer Umgebungen effizient unterstützen.

Die Risiken nicht optimal unterhaltener und abgesicherter IAM-Lösungen bei SMB können sich immens auswirken - von Produktivitätseinbußen durch Kennwortrücksetzungen und fehlerhafte Berechtigungen, Datenverlusten wie Verlusten personenbezogener Daten von Mitarbeitern und Kunden, Verlust von Handelsgeheimnissen und anderen unverzichtbaren Geschäftsdaten, vermindertem Ertrag durch Reputationsverluste und Betrug bis hin zur ungewollten Rolle als Angriffseinstieg auf andere Mitglieder einer Lieferkette. Zahlreiche SMB-Manager und -Eigentümer gehen blauäugig davon aus, dass Ihr Unternehmen schlicht zu unbedeutend sei, um für Angreifer interessant zu werden. Allerdings belegen **Cyberkriminalitätsstudien**, dass SMB immer häufiger zu Angriffszielen werden – eben weil der Absicherungsbedarf geringer als bei größeren Organisationen erscheint.

Um IAM-Voraussetzungen gerecht zu werden, gibt es zahlreiche Anwendungsfälle und technische Voraussetzungen. Hinsichtlich Anwendungsfällen benötigen sämtliche Unternehmen B2E IAM, viele Unternehmen B2B, einige Unternehmen B2C. Bei B2E wird Microsoft Active Directory in den meisten Fällen eingesetzt. Zahlreiche Organisationen nutzen darüber hinaus unterschiedliche Cloud-basierte SaaS-Anwendungen, verzichten jedoch auf zentralisierte IAM-Funktionen oder haben solche Funktionen nicht unter Kontrolle. Oft fehlt es auch an produktivitätssteigernden SSO-Möglichkeiten (Einmalanmeldung).

Nicht nur bei SMB braucht es oftmals mehr, um Umgebungen wie Microsoft Active Directory wirklich im Griff behalten zu können, als IGA-Werkzeuge (Identity Governance and Administration, Werkzeuge zur Identitätskontrolle und -administration) für Unternehmen liefern können. Tiefgehendes Management von Active Directory und zugehörigen Umgebungen verlangt nach bestimmten Fähigkeiten, die beispielsweise auch bei SAP-Umgebungen unerlässlich sind. Daher gibt es einen eindeutigen Bedarf an solchen Lösungen, kombiniert mit voll ausgestatteten IGA-Werkzeugen.

Eine oftmals übersehene Fähigkeit von IAM-Systemen besteht darin, dass diese die Einhaltung gesetzlicher Konformitätsvorgaben unterstützen können. Im Rahmen der Datenschutz-Grundverordnung (DSGVO) der EU wird eine klare, unmissverständliche Einwilligung von Kunden in die Nutzung ihrer Daten zur Einhaltung von Konformitätsvorgaben zwingend vorausgesetzt. Sinnvoll ausgelegte IAM-Lösungen können Konformität mit Vorgaben erzwingen und demonstrieren, die eine Trennung unterschiedlicher Pflichten voraussetzen – beispielsweise SOx in den USA.

Es gibt drei maßgebliche IAM-Funktionskategorien, die insbesondere aus der SMB-Perspektive beleuchtet werden sollten:

Identitätsadministration: Die Fähigkeit zur Administration von Identitätszyklusereignissen einschließlich Bereitstellung/Aufhebung von Nutzerkonten, Unterhaltung von Identitätsdepots, Verwaltung von Zugriffsberechtigungen sowie Synchronisierung von Nutzerattributen. Eine SB-Nutzeroberfläche ermöglicht Zugriffsanfragen, Profilmanagement, Kennwortrücksetzungen und Synchronisierungen. Konfigurierbare Cloud-native Connectoren bieten automatisierte Nutzerbereitstellung betriebsintern sowie bei SaaS-Applikationen. Zu weiteren allgemeinen Identitätsadministrationsfunktionen zählen administrative Weboberfläche, Massenimportoberfläche, delegierte Administration, SPML und SCIM-Unterstützung.

Zugriffsmanagement: Diese Kategorie umfasst Authentifizierung, Autorisierung, Einmalanmeldung und Identitätsverbund betriebsinterner und SaaS-Applikationen, die als Cloud-Service zur Verfügung gestellt werden. Die zugrundeliegende Unterstützung von Industriestandards wie SAML, Oauth und OpenID Connect kann dabei variieren.

Zugriffskontrolle: Diese Fähigkeitengruppe fehlt oft im Portfolio vieler auf AD konzentrierter IAM-Werkzeuge der Einstiegsstufe, da die meisten SMB lediglich nach einer leicht bedienbaren, administratorzentrierten Lösung zur Unterhaltung der Zugriffskontrolle und Durchsetzung minderprivilegierter Prinzipien suchen.

ManageEngine als Teil der Zoho Corporation bietet ein umfangreiches Werkzeug zum Identitäts- und Zugriffsmanagement in Umgebungen, die typischerweise in SMB eingesetzt werden, sich auf Microsoft Active Directory konzentrieren. ManageEngines AD360-Angebot bietet vielfältige Möglichkeiten zum gründlichen IAM.

2 Produktbeschreibung

ManageEngine AD360 ist eine Lösung, die umfangreiche IAM-Möglichkeiten rund um Microsoft Active Directory bietet. Wie der Name schon andeutet, handelt es sich um eine Lösung für Umgebungen, in denen Active Directory (AD) als Kernelement eingesetzt wird. Der Fokus liegt (noch) nicht auf der Zurverfügungstellung eines lückenlosen IGA-Werkzeugs (Identitätskontrolle und -administration), das mit jedem System einer komplexen IT-Umgebung verknüpft werden kann, sondern auf der Automatisierung administrativer Aufgaben sowie Sicherheitsverbesserung AD-zentrischer Umgebungen. Allerdings lässt sich AD360 anhand vordefinierter Integrationspunkte mit zusätzlichen Zielen einschließlich IGA-Systemen integrieren, ManageEngine plant zusätzlich, Anzahl und Einsatzgebiete der bereits mitgelieferten Connectoren weiter auszubauen.

Nutzerlebenszyklusmanagement und Automatisierung

Das AD360-Zentrum bilden Funktionen zur Verwaltung von Nutzern und deren Konten auf automatisierte Weise, die den gesamten Lebenszyklus solcher Konten abdecken. Der Fokus liegt dabei auf Konten in AD selbst sowie in direkt verwandten Systemen wie Microsoft Office 365, Microsoft Exchange Server und Lync. Darüber hinaus bietet AD360 integrierte Unterstützung der Google G Suite. Im Gegensatz zu ausgewachsenen IGA-Lösungen gibt es keine einsatzfertigen Integrationen mit weiteren Zielsystemen wie SAP, Mainframes und dergleichen. Allerdings werden – wie bereits erwähnt – entsprechende Integrationspunkte zur Verfügung gestellt.

Andererseits ermöglicht AD360 eine tiefergehende Integration mit unterstützten Zielumgebungen, beispielsweise durch Unterstützung der Erstellung von Microsoft-Exchange-Mailboxen und Automatisierung weiterer typischer Aufgaben solcher Umgebungen. Dadurch lässt sich das System als Erweiterung üblicher IGA-Werkzeuge einsetzen, das detailliertes Management von AD und einiger verbundener Systeme ermöglicht. Im letzteren Fall mausert sich das System auch zu einer praktikablen Lösung für deutlich größere Organisationen.

Der Fokus der AD360-Möglichkeiten liegt auf dem Management des gesamten Lebenszyklus von Konten mit gleichartigen Konten über das gesamte Nutzervolumen, der Vermeidung von Duplikaten, Beseitigung inaktiver Konten sowie der Prävention versehentlichen Löschens. Neue Nutzer können entweder manuell oder durch Dateiimport aus Quellsystemen wie HR hinzugefügt werden. AD360 bietet anschließend Möglichkeiten zur Automatisierung entsprechender Folgeschritte – über eine grafische Oberfläche, die beispielsweise Konfiguration und Planung von Importen sowie richtlinienbasierte Verknüpfung von AD-Gruppen ermöglicht. AD360 bietet Flexibilität bei der Erstellung spezifischer Logik für sofortige und Folgeaufgaben, allesamt per grafischer Oberfläche. Dadurch lassen sich unter anderem effiziente und robuste Abläufe zum Entfernen inaktiver Konten erstellen, die auf passender Logik sowie Abstufungen zwischen Deaktivierung (sofortige Aufgabe) und Löschung (Folgeaufgaben) beruhen.

Berechtigungsmanagement

Wie zuvor bereits erwähnt, ist AD360 in der Lage, bei Nutzererstellung oder -änderung Verknüpfungen mit AD-Gruppen gemäß Richtlinien zu verwalten, die unterschiedliche Attribute wie Titel oder Abteilung zur automatisierten Verknüpfung von Nutzern mit bestimmten AD-Gruppen einsetzen. Diese Fähigkeit zum regelbasierten (oder richtlinienbasierten) Gruppenmitgliedschaftsmanagement bildet die Grundlagen zur Verwaltung unterschiedlicher AD-Berechtigungen.

ManageEngine nutzt den Begriff „Privileged Access Management“ (PAM) auch für weitere Fähigkeiten, die in dieser Umgebung unterstützt werden. Dies kann etwas missverstanden werden, da ManageEngine auch eine separate PAM-Lösung anbietet, und aufgrund der Tatsache, dass viele dieser Funktionen auch für sämtliche Typen von Nutzerkonten relevant sind.

An dieser Stelle unterstützt AD360 zahlreiche Möglichkeiten:

- Verwaltung von Gruppenmitgliedschaften, sowohl manuell als auch über Richtlinien
- Analyse und Optimierung von Gruppenstrukturen, insbesondere verschachtelten Gruppen
- Bereinigung von Berechtigungen und Erzwingen auf geringster Berechtigung beruhenden Prinzipien durch Innovationsanalyse kritischer Objekte und einzelner Nutzer
- Isolation administrativer Konten zum spezifischen Unterbinden des Zugriffs auf maßgebliche Einrichtungen wie Domänencontroller und Dateiserver, zusätzlich zur Trennung z. B. externer Konten wie Anbietern und Vertragspartnern
- Überwachung heikler Konten

Im Vergleich mit AD-Standardwerkzeugen trägt AD360 deutlich zur Vereinfachung maßgeblicher Aufgaben bei, automatisiert das Management von Nutzern in AD sowie verbundenen Systemen.

Delegierung und Rollenmanagement

Neben der direkten Verknüpfung von Berechtigungen ergänzt AD360 weitere Möglichkeiten in drei Bereichen:

- Verwaltung administrativer Aufgaben über Rollen
- Änderungsverfolgung in AD
- Genehmigungsworkflows bei Änderungen in AD

Administrative Aufgaben hinsichtlich AD, Windows-Servern sowie Office 365 lassen sich über eine zentrale Konsole bewerkstelligen, die auch Verknüpfungen von Aufgaben mit Rollen ermöglicht. Dies bildet die Grundlage zum Wechsel von hochgradig problematischen integrierten Administratorkonten oder anderen Konten mit vollständigen Berechtigungen zu eingeschränkten Operatorrollen.

Änderungsverfolgung ist faktisch Teil der Protokollierungs-, Überwachungs- und Auditierungsfunktionen, absolut essenziell wenn es um Aktivitätsüberwachung von Administratoren und Operatoren geht.

Workflows unterstützen letztendlich bei der Verwaltung von Zugriffsberechtigungen, die über das IT-Team hinausreichen. AD-Aufgaben lassen sich in Tickets verwandeln, die in mehrstufigen Workflows eingesetzt werden. Dies ermöglicht auch Erstellung von Nutzeranfrageportalen für unterschiedliche Nutzertypen, Genehmigungen von Berechtigungsanfragen durch verantwortliche Manager sowie Genehmigungen kontrollierten Zugriffs auf Dateifreigaben.

Protokollierung und Überwachung

AD360 bietet von Haus aus starke Auditierungsfunktionen, obwohl sich die Lösung – anders als andere Lösungen – nicht auf interaktive Echtzeitanalyse aktueller AD-Berechtigungen bis zur ACL-Einzelebene, eher auf Berichte zu Berechtigungsstrukturen und potentielle diesbezügliche Problemstellungen konzentriert. Der Fokus liegt auf der

Optimierung administrativer Prozesse und Identifizierung kritischer Berechtigungen, verwaister Konten sowie betrügerischen Nutzerverhaltens.

Dazu zählen auch UBA-Fähigkeiten (User Behavior Analytics, Nutzerverhaltensanalyse) die kürzlich in AD360 eingeführt wurden. Auf dieser Grundlage lässt sich das Nutzerverhalten überwachen, Ausreißer können einfach identifiziert werden. Die Technologie basiert auf ML-Algorithmen (maschinelles Lernen).

Darüber hinaus unterstützt AD360 auch gewohnte Auditing- und Berichtsfunktionen.

Authentifizierung

Letztendlich unterstützt AD360 ebenfalls Authentifizierungsmöglichkeiten, die weit über den Umfang hinausreichen, der üblicherweise von Produkten dieser Kategorie geboten wird. Zu Fähigkeiten dieses Gebietes zählen:

- Verwaltung von Kennwortrichtlinien und Kennwort-SB-Service
- Maßgeschneiderte Authentifizierungsmethoden für heikle und privilegierte Konten
- Integration mit Windows MFA/2FA (Multifaktor-/Zwei-Faktor-Authentifizierung)
- SSO (Einmalanmeldung) an Cloud-Services

Adaptive Authentifizierung, Unterstützung risiko- und kontextbasierter Authentifizierung, z. B. Schritt für Schritt-Authentifizierung, wurden für kommende Versionen geplant.

Im Bereich Einmalanmeldung werden unterschiedliche geschäftliche Applikationen wie Salesforce, Office 365 oder Dropbox von Anfang an unterstützt. Dank SAML-Unterstützung wird auch SSO an anderen Services wie geschäftlichen SAML-fähigen Applikationen unterstützt. Darüber hinaus bietet AD360 auch Möglichkeiten zur Kennwortsynchronisierung, zum Beispiel mit AD LDS sowie weiteren Systemen wie Salesforce.

3 Stärken und Herausforderungen

Alles in allem ist AD360 ein leistungsfähiges Werkzeug zur Verwaltung von Nutzern und deren Konten in Microsoft AD und bestimmten verbundenen Systemen, das sich durch einen großen Funktionsumfang auszeichnet. Obwohl AD360 keine voll ausgestattete IGA-Lösung ist, bietet das Paket umfangreiche Fähigkeiten zur Verwaltung von AD, Office 365 und zugehörigen Umgebungen, lässt sich darüber hinaus als integrierte Lösung mit IGA-Werkzeuge auf Unternehmensebene einsetzen. Beim letzteren Einsatz bietet AD360 detaillierte Möglichkeiten zum Microsoft-Active-Directory-Management, vergleichbar mit SAP Access Control in SAP-Umgebungen.

Nicht zuletzt durch den weit gefächerten Funktionsumfang bietet sich ManageEngine AD360 als gute Lösung für SMB an, deren IT auf Microsoft Active Directory aufbaut. Mit Workflowfähigkeiten sowie SSO-Unterstützung für Cloud-Services dehnt sich die Reichweite der Lösung auch auf zusätzliche Plattformen aus, die immer häufiger in solchen Unternehmen eingesetzt werden.

Während sich UBA-Fähigkeiten noch in der Frühphase befinden, demonstriert ManageEngine einen deutlichen Fokus auf Ergänzung wesentlicher Funktionen, die Unternehmen bei der Minimierung von Risiken unterstützen, die sich häufig aus suboptimaler Administration von AD-Umgebungen ergeben.

Innerhalb des Kernfunktionsumfangs gibt es vielleicht noch etwas Raum für weitere Unterstützung detaillierte Analysen von Berechtigungen in AD-Umgebungen sowie für mehr Flexibilität zur einfachen Verknüpfung zusätzlicher Systeme, insbesondere im SMB-Umfeld. Allerdings ist AD360 definitiv eine äußerst starke Lösung in Nutzungsszenarien, für die das Werkzeug entwickelt wurde.

Stärken	Herausforderungen
• Speziell auf optimierte Administration von Microsoft Active Directory ausgelegt • Starke Workflowfähigkeiten, die den üblichen Leistungsumfang dieses Produkttyps übersteigen • Rollenbasierte Verknüpfung administrativer Aufgaben • Grundlegende UBA-Fähigkeiten zur Identifizierung missbräuchlicher Nutzung • Sofort einsatzbereite Integration mit Office 365 und einigen weiteren Zielsystem • Durchdachte, leicht bedienbare Nutzeroberfläche • Richtlinienbasiertes Berechtigungsmanagement mit einem substantiellen Grad an Flexibilität	• Keine voll ausgestattete IGA-Lösung, jedoch auf Microsoft-Active-Directory-Umgebungen fokussiert, bietet Integrationspunkte für weitere IGA-Produkte und Zielsysteme • Gute Auditing- und Analysefähigkeiten, jedoch begrenzte interaktive Analyse komplexer Berechtigungsstrukturen • Eingeschränkte Konnektivität mit Zielsystemen

4 Copyright

Die Zukunft der Datensicherheit – Heute

KuppingerCole unterstützt IT-Fachleute mit herausragender Kompetenz rund um Definition effizienter IT-Strategien und perfekt informierter Entscheidungsfindung. Als führendes Beratungsunternehmen bietet KuppingerCole anbieterunabhängige Informationen aus erster Hand. Unsere Dienstleistungen gewährleisten sichere Entscheidungsfindung bei sämtlichen geschäftskritischen Fragen.

KuppingerCole wurde im Jahre 2004 gegründet, zählt heute zu den führenden europäischen Identitätsberatungsunternehmen mit dem Schwerpunkt Datensicherheit in klassischen und Cloud-Umgebungen. KuppingerCole steht für Sachkunde, innovative Ideen und anbieterunabhängige Einschätzung der Datensicherheitsbranche einschließlich sämtlicher relevanter Aspekte wie Identitäts- und Zugriffsmanagement (IAM), Zugriffskontrolle, Risikomanagement und Konformität (GRC), IT-Risikomanagement, Authentifizierung und Autorisierung, Einmalanmeldung, Identitätsverbund, nutzerzentriertes Identitätsmanagement, eID-Karten, Cloud-Sicherheit und -Management und Virtualisierungen.

Weitere Informationen erhalten Sie hier: **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstr. 20 – 22
65185 Wiesbaden |

Tel.: +49 (211) 23 70 77-0
Fax + 49 (211) 23 70 77-11
www.kuppingercole.com