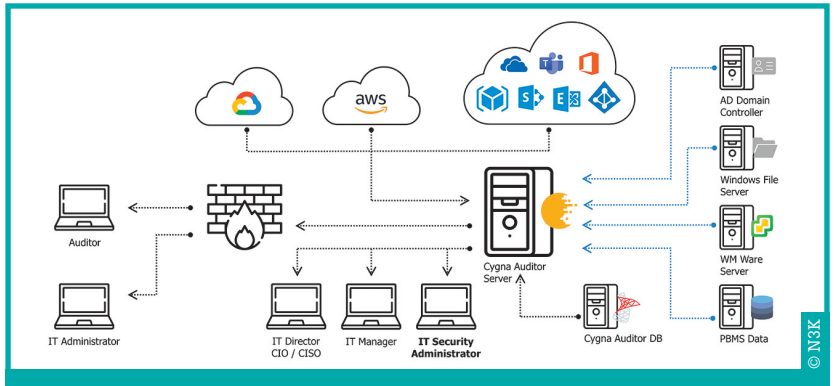
AD-Auditing für einen sicheren Betrieb

Achtzehn Leuchtturm-Projekte hat die Ampel-Koalition in der **Digitalstrategie für Deutschland** definiert, darunter etliche, an denen sich schon die Große Koalition abgemüht hat – oft mit mäßigem Erfolg wie etwa bei der elektronischen Patientenakte oder dem Digitalpakt für die Schulen.

Auch der Digitalisierung der Verwaltung will die Ampel eine hohe Priorität einräumen, aber keine konkreten Termine mehr nennen. Sie wird nun als Daueraufgabe geführt. Eines der Hauptziele der Digitalisierung der Verwaltung ist es, sichere digitale Identitäten zur Verfügung zu stellen, damit sich die Bürger bei verschiedenen Behörden ausweisen können.

Bereits heute spielt die Vergabe und Administration von Nutzeridentitäten in der Verwaltung eine zentrale Rolle. Sie bestimmen, wer auf welche Daten, Anwendungen und Systeme zugreifen darf. Bei der Verwaltung dieser digitalen Identitäten spielt in der Regel das Active Directory (AD) von Microsoft eine wichtige Rolle. Dieser Verzeichnisdienst fungiert als zentrales Nervensystem der IT-Infrastruktur, durch das alle IT-Objekte wie Anwender, Gruppen, Anwendungen oder Geräte verwaltet werden. Darüber hinaus erlaubt es Administratoren, den Zugang zu Ressourcen über die Vergabe und das Management von Zugriffsrechten zu regeln.

Allerdings ist ein AD gerade in größeren Behörden ein komplexes Gebilde, das anfällig für Fehlkonfigurationen mit erheblichen Auswirkungen auf den Betrieb ist. Aus diesem Grund sollte man das Active Directory kontinuierlich auditieren, um Fehler samt ihrer Gründe und Urheber zeitnah erkennen und beheben zu können. Dies schließt auch die frühzeitige Erkennung von Cyberattacken ein, von denen sehr viele einen Angriff auf das Active Directory beinhalten, um die Zugangsrechte des Angreifers auszuweiten.



Architektur der Cygna-Auditor-Plattform

Mit der Cygna Auditor Plattform bietet Cygna Labs über seinen lokalen Reseller N3K, einen spezialisierten, auf den DACH-Raum fokussierten IT-Dienstleister aus Heilbronn, eine umfassende Lösung für das Change Auditing, das Security Alarming und das Rollback und Recovery des Active Directory. Diese wird unter anderem in der gesamten Finanzverwaltung von Nordrhein-Westfalen eingesetzt. Sie überwacht sämtliche administrativen Aktivitäten innerhalb des ADs in Echtzeit und versetzt Administratoren damit in die Lage, alle Änderungen zu erkennen und unautorisierte Änderungen in Echtzeit zu melden. Basierend auf diesen Audit-Daten können jegliche Änderungen bei Bedarf rückgängig gemacht werden - unabhängig davon, ob sie durch Fehlkonfiguration oder externe Angriffe ausgelöst wurden. So kann auf Basis der gesammelten AD-Audit-Daten ein echtes Rollback zu beliebigen Zeitpunkten erfolgen. Dabei ermöglicht der Cygna Auditor eine sehr granulare Wiederherstellung aller AD-Objekte bis hinunter auf die Attribut-Ebene. Hierdurch werden sehr fokussierte Rollbacks mit hoher Zeiteffizienz ermöglicht (wirklich nur dasjenige „zurückrollen“, was benötigt wird). Die Bedienung ist sehr einfach und wird von Nutzern immer wieder als intuitiv beschrieben.

Da Cygna Auditor sowohl das On-Premises-AD als auch das Azure AD in einer On-Prem-Plattform unterstützt, erleichtert er die Migration zu Cloud-basierten Lösungen wie Microsoft 365 erheblich und gestaltet sie transparent und risikoarm. Dabei ist diese Plattform die einzige Lösung, die alle gewonnenen Daten, auch die aus der Cloud, im eigenen Rechenzentrum speichert, um so jederzeit die maximale Datensicherheit zu gewährleisten.

Die Cygna Auditor Plattform ist leicht zu implementieren und im täglichen Betrieb sehr benutzerfreundlich. Sie verfügt über ein einheitliches, Web-basiertes GUI und basiert auf einer Plattformstrategie, die eine Vielzahl von Auditing-Optionen beinhaltet, unter anderem für Microsoft 365, Azure AD, Exchange, File-Services, VM und weitere. Auch die Beschaffung gestaltet sich unkompliziert.

Anders als bei anderen Lösungen erfolgt die Lizensierung pro „biologischen“ Usern im Active Directory und nicht nach Objekten, deren Zahl stark schwanken kann, so dass die Lizenzkosten besser kalkulierbar sind.

Weitere Informationen

Mehr zur Cygna Auditor Plattform und deren Einsatz bei der Finanzverwaltung NRW:

[https://www.n3k.com/government]
[https://www.n3k.com/cygna-auditor-plattform]