

CHANGE-AUDITING UND RECOVERY ZUR OPTIMIERUNG DES ACTIVE DIRECTORY BETRIEBS IN DER FINANZVERWALTUNG NRW

Finanzverwaltung
des Landes Nordrhein-Westfalen



CHANGE-AUDITING UND RECOVERY ZUR OPTIMIERUNG DES ACTIVE DIRECTORY BETRIEBS IN DER FINANZVERWALTUNG NRW

Die Finanzverwaltung des Landes Nordrhein-Westfalen umfasst neben dem Ministerium der Finanzen als oberste Landesbehörde verschiedene Landesoberbehörden und Landesmittelbehörden wie etwa das Landesamt für Besoldung und Versorgung, das Landesamt für Finanzen, die Oberfinanzdirektion sowie die Finanzämter einschließlich der Betriebsprüfung und der Steuerfahndung als untere Landesbehörden. Zudem betreibt die Finanzverwaltung Schulungseinrichtungen wie die Hochschule für Finanzen im Schloss Nordkirchen, die Landesfinanzschule oder die Fortbildungsakademie. Als Landesoberbehörde fungiert zudem das zentrale Rechenzentrum der Finanzverwaltung, das für den gesamten Betrieb der IT verantwortlich ist. Dieses Rechenzentrum dient als zentraler Dienstleister für etwa 140 Standorte mit ca. 30.000 Anwendern im gesamten Bundesland.

In einer Finanzverwaltung ist die Informationstechnik naturgemäß ein sehr sensibles Thema, da ganz überwiegend vertrauliche und personenbezogene Daten verarbeitet werden. Es ist daher unerlässlich, sehr detaillierte Regeln aufzustellen und auch durchzusetzen, welche Mitarbeiter Zugriff auf welche Daten und Anwendungen haben. Zur sicheren Verwaltung der Benutzer und ihrer Zugriffsrechte setzt die Finanzverwaltung des Landes Nordrhein-Westfalen auf das Active Directory (AD) von Microsoft. Als zentraler Verzeichnisdienst verwaltet AD alle IT-Objekte wie Benutzer, Gruppen, Anwendungen oder Geräte und es erlaubt Administratoren, den Zugang zu Ressourcen über die Vergabe und das Management von Zugriffsrechten zu regeln.

„Auch seit wir im produktiven Betrieb sind, haben wir immer jemanden mit sehr viel Kompetenz an der Seite. Allerdings ist der Betrieb so problemlos, dass wir nur sehr selten davon Gebrauch machen müssen.“

*Dietmar Rilk, Leitung Systemtechnik
Windows bei der Finanzverwaltung des*

„In den Planungs- und Implementierungsphasen war die Zusammenarbeit mit N3K als Systemintegrator sehr angenehm und unaufdringlich“

*Dietmar Rilk, Leitung Systemtechnik
Windows bei der Finanzverwaltung
des Landes NRW*

„Seit dem Roll-out im August 2021 läuft die Cygna Auditor Plattform mit den Funktionsmodulen „Cygna Auditor for AD“ und dem „Cygna Recovery for AD“ im Rechenzentrum der Finanzverwaltung störungsfrei.“

*Dietmar Rilk, Leitung Systemtechnik
Windows bei der Finanzverwaltung des
Landes NRW*





ACTIVE DIRECTORY ALS KRITISCHE RESSOURCE

Als zentraler Dienst hat das AD eine ganz erhebliche Bedeutung für die Verfügbarkeit von Daten und Anwendungen im gesamten Netzwerk der Finanzbehörden in NRW. Ausfälle oder auch nur Teilausfälle führen unmittelbar dazu, dass Mitarbeiter ihre Aufgaben nicht erledigen können und die Funktionsfähigkeit aller Dienststellen beeinträchtigt wird. Zudem bietet AD mit Bordmitteln keine einfache Wiederherstellungsmöglichkeit, so dass derartige Probleme nur manuell und mit hohem personellem und zeitlichem Aufwand behoben werden können. Insbesondere bietet AD nur sehr beschränkte Funktionen zur Protokollierung, so dass Änderungen oft nicht nachvollziehbar sind. Allerdings sind es in der Regel gerade solche Änderungen, die zu Fehlfunktionen führen.

Ein solcher Teilausfall des Active Directory mit seinen Folgen war dann auch der primäre Anlass für die Suche nach einer Lösung, die ein effizientes Change-Management inklusive eines umfassenden Auditings ermöglichen sollte. Zudem sollte diese Lösung eine einfache Möglichkeit bieten, Objekte im AD nach einem Vorfall gänzlich wiederherzustellen oder Veränderung wieder zurückrollen zu können, am besten auch inkrementell. Das Auditing sollte zudem der Revisionsicherheit dienen und versprach auch Sicherheitsgewinne, da die meisten Cyberangriffe heute in einer frühen Phase auf Änderungen im Active Directory setzen, um den Angreifern über Rechte-Eskalation erweiterte Zugriffsmöglichkeiten zu eröffnen.

Über eine Empfehlung wurden Dietmar Rilk, Referatsleiter Windows Systemtechnik, und sein Team auf die Cygna Auditor Plattform von Cygna Labs aufmerksam, die in Deutschland unter anderem von N3K Network Systems vertrieben wird. Das Funktionsmodul „Cygna Auditor for Active Directory“ überwacht sämtliche administrativen Aktivitäten innerhalb des kritischen Verzeichnisdienstes Active Directory in Echtzeit und versetzt Administratoren damit in die Lage, alle Änderungen zu erkennen und, wenn gewünscht, auf unautorisierte Änderungen in Echtzeit zu alarmieren. Basierend auf diesen Audit-Daten können jegliche Änderungen bei Bedarf rückgängig gemacht werden - unabhängig davon, ob sie durch Fehlkonfiguration oder externe Angriffe ausgelöst wurden. Hierzu bietet die Cygna Auditor Plattform mit dem Funktionsmodul „Cygna Recovery“ auf Basis der gesammelten AD-Audit Daten eine echte, backupzeitpunktlose Rollback-Funktion zu beliebigen Zeitpunkten und ermöglicht eine sehr granulare Wiederherstellung aller AD-Objekte bis hinunter auf die Attributebene, wenn gewünscht auch inkrementell.

Bei der Finanzverwaltung des Landes Nordrhein-Westfalen unterstützt die Cygna Auditor Plattform mit den Funktionsmodulen „Cygna Auditor for AD“ und dem „Cygna Recovery for AD“ eine Umgebung, in der Hardware, Software und auch Identitäten sehr zentral verwaltet werden. „Es gibt zwar delegierte Verantwortungen an unseren einzelnen Standorten, aber keine lokalen Administratoren“, so Rilk. „Die gesamte Administration erfolgt zentral im Rechenzentrum, und erhöhte Zugriffsrechte an den Standorten werden nur erteilt, wenn es zwingende Gründe dafür gibt - und dann auch nur temporär. Das Prinzip der geringsten Privilegien wird bei uns konsequent umgesetzt.“ Um die zentrale Verwaltung zu vereinfachen, setzt die Finanzverwaltung laut Rilk zudem auf ein Lego-Prinzip - alle Server und auch alle Clients im Netz besitzen identische Konfigurationen.



„Seit dem Roll-out im August 2021 läuft die Cygna Auditor Plattform mit den Funktionsmodulen „Cygna Auditor for AD“ und dem „Cygna Recovery for AD“ im Rechenzentrum der Finanzverwaltung störungsfrei.“

*Dietmar Rilk, Leitung Systemtechnik
Windows bei der Finanzverwaltung des
Landes NRW*



ZENTRALE SAMMLUNG UND AUSWERTUNG VON EREIGNISSEN

Da der vorherige Teilausfall des Active Directory als ernsthaftes Sicherheitsproblem eingestuft wurde, konnte die Finanzverwaltung die Cygna Auditor Plattform in Übereinstimmung mit dem Vergaberecht im August 2021 implementieren. „Uns war es dabei besonders wichtig, Ereignisse im AD zentral sammeln und auswerten zu können“, erläutert Dietmar Rilk. „Das ist die Voraussetzung dafür, kritische Ereignisse zu erkennen und weitestgehend automatisiert darauf reagieren zu können, statt einfach nur Alarmmeldungen auf der Konsole auszugeben.“ Zudem vereinfachte die Cygna Auditor Plattform mit dem „Cygna Auditor for AD“ durch seine lückenlose Dokumentation von Zugriffen und Änderungen die Gewährleistung der DSGVO-Konformität und der Einhaltung aller BSI-Vorschriften (Bundesamt für Sicherheit in der Informationstechnik).

Insbesondere die Nachvollziehbarkeit aller Änderungen im AD war einer der wesentlichen Gründe für die Entscheidung zugunsten der Cygna Auditor Plattform. Zwar bietet auch das Active Directory ein natives Event Logging auf dem Domänencontroller an, doch je nach Konfiguration werden die Log-Einträge nach 30 bis 60 Minuten durch neuere überschrieben, so dass keinerlei Langzeitdokumentation existiert. Die Cygna Auditor Plattform verwendet dagegen eine eigene SQL-Datenbank zur Speicherung von Events, die nicht nur eine lediglich vom Speichermedium abhängige Kapazität bietet, sondern auch einen sehr einfachen Zugriff. Alle Active Directory Veränderungen werden mit eigenem Mechanismus, ohne die Zuhilfenahme der nativen Logfiles, lückenlos eingesammelt. Damit ist eine bessere Datenqualität bei ca. 75% weniger Datenmenge gewährleistet. Zudem verfügt die Cygna Auditor Plattform über ein Einfaches, modernes und aufgeräumtes Web-GUI mit dem sehr einfach und plattformübergreifend gearbeitet werden kann.

Bei der Finanzverwaltung des Landes Nordrhein-Westfalen unterstützt die Cygna Auditor Plattform mit den Funktionsmodulen „Cygna Auditor for AD“ und dem „Cygna Recovery for AD“ eine Umgebung, in der Hardware, Software und auch Identitäten sehr zentral verwaltet werden. „Es gibt zwar delegierte Verantwortungen an unseren einzelnen Standorten, aber keine lokalen Administratoren“, so Rilk. „Die gesamte Administration erfolgt zentral im Rechenzentrum, und erhöhte Zugriffsrechte an den Standorten werden nur erteilt, wenn es zwingende Gründe dafür gibt - und dann auch nur temporär. Das Prinzip der geringsten Privilegien wird bei uns konsequent umgesetzt.“ Um die zentrale Verwaltung zu vereinfachen, setzt die Finanzverwaltung laut Rilk zudem auf hohe Standardisierung und Einheitlichkeit, wodurch alle Server und Klienten identische Konfigurationen besitzen.“

Seit dem Roll-out im August 2021 läuft die Cygna Auditor Plattform mit den Funktionsmodulen „Cygna Auditor for AD“ und dem „Cygna Recovery for AD“ im Rechenzentrum der Finanzverwaltung störungsfrei.

ÜBER CYGNA LABS

Cygna Labs ist ein führender Anbieter von Compliance-Lösungen, der einen einmaligen Einblick in hybride Microsoft IT-Infrastrukturen gewährt. Die Cygna Auditor Plattform wurde von Grund auf entwickelt, um Daten unabhängig von ihrem Standort zu schützen und liefert Einblicke in das Benutzerverhalten, die Systemkonfiguration und die Datensensitivität. Organisationen auf der ganzen Welt verlassen sich auf Cygna Labs, um Bedrohungen der Datensicherheit zu erkennen und proaktiv zu entschärfen, Compliance-Audits kostengünstig und mit weniger Aufwand zu bewältigen und die Produktivität ihrer IT-Abteilungen zu erhöhen.

www.cygnalabs.com

ÜBER N3K: Schnellwachsende IP-Netzwerke erfordern professionelle Lösungen für die verschiedensten Facetten des Netzwerk-Managements. N3K Network Systems hat sich auf die Gebiete IP Address Management, Privilege Management sowie auf Active Directory Management spezialisiert. So können mit hoher Kompetenz auf die individuellen Anforderungen der Kunden zugeschnittene Lösungen entwickelt werden. N3K unterstützt die Kunden über den gesamten Projektzyklus hinweg bei Bedarfsanalyse, Konzeption, Projektplanung, Implementierung und Schulung. Hinzu kommen umfangreiche Wartungs-Services inklusive weltweitem 7x24-Support und direkter Einwahl beim Kunden. Aufbauend auf dieser einfachen und effektiven Philosophie hat sich N3K als führender Anbieter in Deutschland etabliert. Mehr als 50% der DAX-Unternehmen sind N3K-Kunden. Durch Standorte in den USA und in Singapur können die Leistungen weltweit erbracht werden.

