CASESTUDY

SICHERHEIT FÜR DAS ACTIVE DIRECTORY - HORNBACH AUDITIERT AD MIT CYGNA

Sicherheit für das Active Directory - Hornbach auditiert AD mit Cygna Auditor Plattform

Mit einem Nettoumsatz von gut 5,8 Milliarden Euro und über 24.000 Mitarbeitern ist die Hornbach-Gruppe eine der größten Baumarktketten in Europa. Etwas mehr als die Hälfte des Umsatzes wird in Deutschland erzielt. Europaweit betreibt Hornbach 167 Einzelhandels-Filialen mit einer Verkaufsfläche von knapp 2 Millionen Quadratmetern, wobei viele der Immobilien sich im Eigenbesitz der Hornbach-Gruppe befinden. Gemessen am Umsatz ist Hornbach in Deutschland der drittgrößte Betreiber von Baumärkten, beim Umsatz pro Markt oder pro Quadratmeter Handelsfläche die Nummer eins. Doch wirtschaftlicher Erfolg ist für Hornbach nur eine Seite der Medaille - das Unternehmen bekannte sich als eines der ersten der Branche zu seiner Verantwortung gegenüber der Umwelt. So hatte das Unternehmen sich bereits 1996 freiwillig gegenüber dem WWF und Greenpeace verpflichtet, keine unzertifizierten Tropenhölzer zu importieren und kümmert sich bei seinen Zulieferern und Produzenten intensiv um eine verantwortungsvolle Holz- und Steinwirtschaft mit hohen Sozial- und Arbeitsschutz-Standards.

Wie alle Unternehmen dieser Größe ist Hornbach für den täglichen Betrieb auf eine umfassende und vor allem zuverlässige IT-Unterstützung angewiesen. Zu den Herausforderungen zählen dabei nicht nur Warenwirtschaft, Logistik und andere Kernfunktionen - als Einzelhandelsunternehmen gehört Hornbach auch zu einer der primären Zielgruppen von Cyberkriminellen. Sicherheit und Verfügbarkeit der IT-Dienste haben daher einen sehr hohen Stellenwert.

„Das Change Management im AD ist heute sehr viel effizienter, und wir wissen zudem, dass wir neue Auditing-Anforderungen sehr einfach in unsere Lösungen integrieren können, sobald sie entstehen.“,

Christian Leingang, Technologie bei Hornbach

“Der Cygna Auditor ermöglicht uns nicht nur einen umfassenden und tiefgehenden Einblick in die Geschehnisse innerhalb unseres Active Directory, sondern ermöglicht uns auch, Fehler auf sehr einfache Weise zu beheben“,

Christian Leingang, Technologie bei Hornbach

Auch wirtschaftlich hat sich der Umstieg auf Cygna Labs gelohnt. „Die neue Lösung ist zwar von der Lizensierung her nicht unbedingt preisgünstiger als die bisherige“, so Johann, „aber durch die zusätzlichen Features sind wir wesentlich effizienter und auch effektiver geworden - und Zeit ist auch Geld.“

Florian Johann, Teamleiter Technologie bei Hornbach

“Der Cygna Auditor hat unsere Erwartungen voll erfüllt“,

resümiert Florian Johann, Teamleiter Technologie bei Hornbach

Das zentrale Nervensystem der IT ist bei Hornbach das Active Directory (AD) von Microsoft, das als Verzeichnisdienst alle IT-Objekte wie User, Gruppen, Anwendungen oder Geräte verwaltet und es Administratoren erlaubt, den Zugang zu Ressourcen über die Vergabe und das Management von Zugriffsrechten zu regeln. Dabei hat Hornbach das Ziel, das Prinzip der minimalen Rechte konsequent durchzusetzen; d.h. Mitarbeiterinnen und Mitarbeiter sollen nur diejenigen Zugriffsrechte besitzen, die sie für die Erledigung ihrer Aufgaben tatsächlich benötigen. Dies gilt auch für die Administratoren. So vergibt Hornbach Berechtigungen User- oder Rollen-basiert sehr granular, und die Administratoren in den einzelnen Filialen können lediglich auf den lokalen Domain Controller zugreifen.

Active Directory braucht Auditierung

Allerdings ist ein Active Directory mit knapp 25.000 Usern und vielen weiteren Objekten ein komplexes Gebilde, das anfällig für Fehlkonfigurationen mit potentiell erheblichen Auswirkungen auf den Geschäftsbetrieb ist. Und niemand ist fehlerfrei. Bei Hornbach gibt es unternehmensweit über 150 Administratoren, die Änderungen am Active Directory vornehmen können, wie etwa die Einrichtung neuer User oder Geräte oder die Ausweitung oder Einschränkung von Zugriffsrechten einzelner Anwender und Gruppen. Die Frage ist nicht, ob dabei Fehler passieren, sondern wann, wo und welche. Für Hornbach ist es daher unerlässlich, sein Active Directory kontinuierlich zu auditieren, um Fehlkonfigurationen 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.

Ein fortlaufendes Auditing sollte für Hornbach daher ein umfassendes Change Management im AD implementieren, die Forensik und insgesamt einfach einen Überblick ermöglichen, wer eigentlich was im Active Directory macht. Bereits vor Jahren hatte das Unternehmen daher eine kommerzielle Auditing-Lösung implementiert, die jedoch im Laufe der Zeit den gestiegenen Ansprüchen nicht mehr gerecht werden konnte. Als Florian Johann, Teamleiter Technologie bei Hornbach im Gespräch mit N3K auf den Cygna Auditor von Cygna Labs aufmerksam wurde, vereinbarten beide Unternehmen daher schnell eine Testinstallation. Bereits knapp drei Monate später wurde der Proof of Concept (PoC) erfolgreich abgeschlossen, und die Ergebnisse sprachen deutlich für einen Umstieg auf den Cygna Auditor.

Umstieg von vorhandener Lösung

„Der Cygna Auditor ermöglicht uns nicht nur einen umfassenden und tiefgehenden Einblick in die Geschehnisse innerhalb unseres Active Directory, sondern ermöglicht uns auch, Fehler auf sehr einfache Weise zu beheben“, so Florian Johann. „Mit der integrierten Rollback-Funktion, die wir bei unserer bisherigen Lösung vermisst hatten, können wir unerwünschte Änderungen an einzelnen AD-Objekten sehr granular und innerhalb kürzester Zeit rückgängig machen.“ Zudem ist der Cygna Auditor laut Florian Johann erheblich performanter als die frühere Auditing-Lösung. „Bei problematischen Änderungen dauerte es früher oft mehrere Stunden, bis die Auditing-Lösung einen Alarm generierte. Das geht heute innerhalb von Minuten, so dass wir sehr zeitnah agieren und potentielle Sicherheitslücken schließen können.“

Auch die Benutzerfreundlichkeit war ein weiteres Argument für den Umstieg auf den Cygna Auditor. Die neue Lösung verfügt über ein einheitliches, Web-basiertes GUI und einen ebenfalls einheitlichen Speicherbereich für alle auditierten Daten statt wie bisher einzelner Management-Oberflächen und Datensilos. Zudem sprach die Erweiterbarkeit und damit die Zukunftssicherheit für den Cygna Auditor. Dieser folgt einer Plattformstrategie, die eine Vielzahl von Auditing Modulen unterstützt, darunter solche für Office 365, Teams, Azure AD, Exchange, SharePoint und andere, so dass Hornbach bei zusätzlichen Auditing-Anforderungen entsprechende Module einfach integrieren, lizensieren und aktivieren kann.

Lizensierung pro User statt pro Objekt

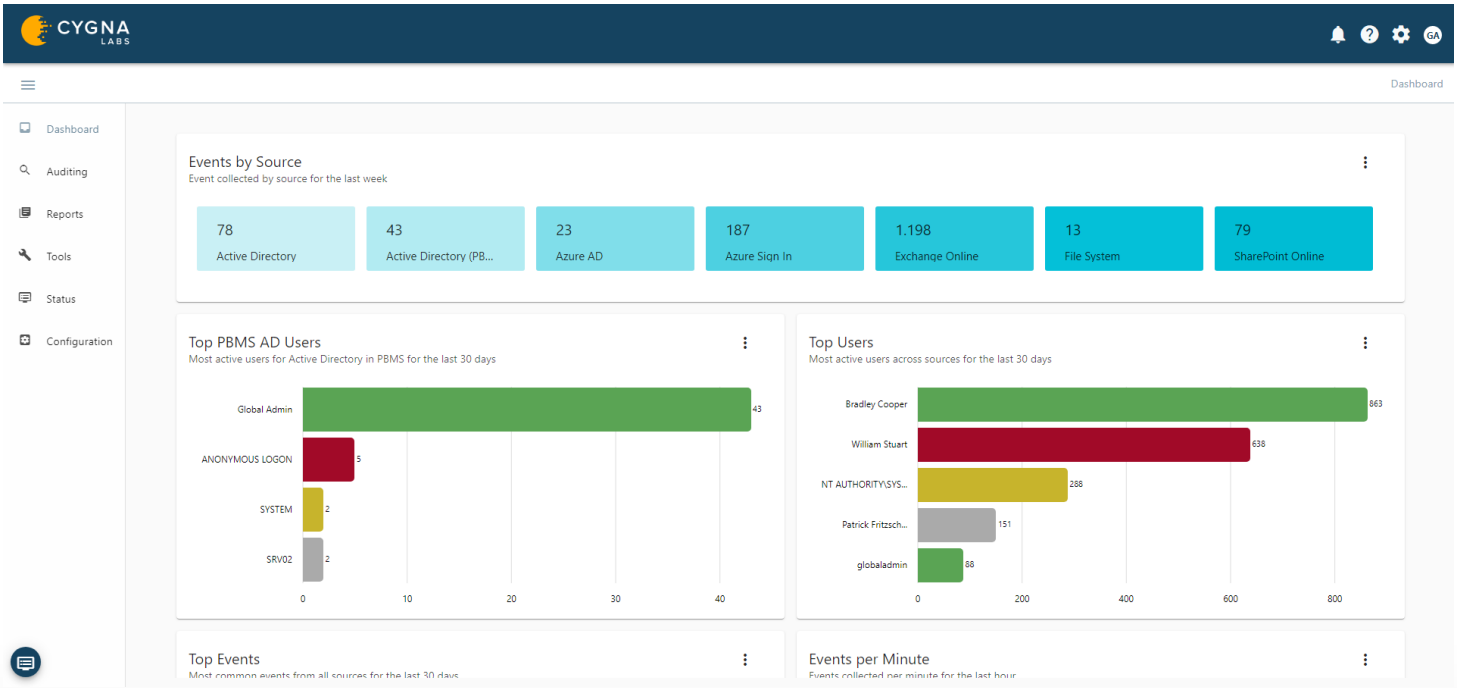
Auch wirtschaftlich hat sich der Umstieg auf Cygna Labs gelohnt. „Die neue Lösung ist zwar von der Lizensierung her nicht unbedingt preisgünstiger als die bisherige“, so Johann, „aber durch die zusätzlichen Features sind wir wesentlich effizienter und auch effektiver geworden - und Zeit ist auch Geld.“ Zudem lizensiert Cygna Labs pro User im Active Directory statt nach Objekten, deren Zahl stark schwanken kann, so dass die Lizenzkosten besser kalkulierbar sind. „Wir hatten bei unserer früheren Lösung schon einmal eine ziemlich unangenehme Erfahrung mit einer heftigen und überraschenden Nachlizensierung“, so Johann. „Das ist bei Cygna Labs nun ausgeschlossen - wir kennen die Kosten genau.“

Während der Umstieg von einer etablierten auf eine neue Lösung oft sehr komplex und mit viel Adaptions- und Trainingsaufwand verbunden sein kann, fiel Hornbach die Migration auf Cygna Labs nicht schwer. „Die Datensammlung funktioniert bei allen kommerziellen Auditing-Lösungen im Prinzip gleich - da mussten wir uns nicht großartig umstellen“, so Johann. „Aber durch das einheitliche und intuitive Benutzerinterface hatten wir plötzlich ein wesentlich einfacheres Handling, so dass unsere AD-Administratoren mit der neuen Lösung ohne eine lange Lernkurve sofort produktiv werden konnten.“ Zudem wurde der Umstieg von den erfahrenen Ingenieuren des deutschen Cygna-Integrators N3K Network Systems umfassend begleitet, so dass kleinere Anfangsschwierigkeiten schnell beseitigt werden konnten.

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.