

# Mehr Sicherheit für das Active Directory — Hornbach auditiert AD mit dem Cygna Auditor

**HORNACH**

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

according to Florian Johann, technology team leader at Hornbach

## 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 HornbachGruppe 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, im Bezug auf Umsatz pro Markt oder pro Quadratmeter Handelsfläche ist Hornbach die führende Kraft am Markt. 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 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.



**Auch wirtschaftlich hat sich der Umstieg auf Cygna Labs gelohnt. „Die neue Lösung ist zwar von der Lizenzierung 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

### Active Directory braucht Auditing

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.

### Lizenzierung pro User statt pro Objekt

Auch wirtschaftlich hat sich der Umstieg auf Cygna Labs gelohnt. „Die neue Lösung ist zwar von der Lizenzierung 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 lizenziert 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 Nachlizenzierung“, 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.

Wir stehen Ihnen gerne mit weiteren Informationen zu unseren Produkten und Leistungen zur Verfügung

Telefon: +49 7131 59495 0 | Email: [sales-europe@cygnalabs.com](mailto:sales-europe@cygnalabs.com)

Cygna Labs Germany | Ferdinand-Braun-Str. 2/1 | 74074 Heilbronn | Germany