

„Mit dem Managed SOC-Service schützt Axians unsere IT-Infrastruktur proaktiv und reaktionsschnell, was unser internes IT-Security-Team entlastet. Dabei war die nahtlose und schnelle Integration unserer bestehenden Systeme und Prozesse entscheidend.“

Philipp Schmeißer, Leiter IT Security, HPM

REFERENZ

HPM

Maßgeschneiderter SOC-Service für HPM die Handwerksgruppe

Sichere Heimat fürs Handwerk

Mit über 4.000 Mitarbeitenden und mehr als 80 Standorten zählt die HPM Handwerksgruppe zu einer führenden Größe im deutschen Handwerk. Als familiengeführte Unternehmensgruppe bietet sie rund 160 Betrieben eine stabile unternehmerische Basis, um sich weiterzuentwickeln und nachhaltig erfolgreich zu bleiben.

Doch mit der Expansion wächst auch die Herausforderung im digitalen Bereich: Moderne Handwerksunternehmen steuern unter anderem das Projektmanagement, die Buchhaltung und Materialbestellungen digital und sind zunehmend auf eine stabile und sichere IT angewiesen. Gleichzeitig steigt auch hier die Gefahr durch Cyber-Angriffe, die sensible Kundendaten, Baupläne und Auftragsdetails ins Visier nehmen.

Zentrale Sicherheitsleitstelle benötigt

Zur gezielten Stärkung der Cybersicherheit entschied sich das Unternehmen für die Implementierung eines Security Operations Centers (SOC) – umgesetzt und betrieben von Axians als erfahrenem Cyber-Security-Dienstleister. Das zentrale Ziel war es, das interne IT-Security-Team zu entlasten und gleichzeitig einen umfassenden Schutz vor Cyber-Bedrohungen zu gewährleisten. Besonders wichtig war eine nahtlose Integration in die bestehende IT-Infrastruktur sowie ein 24/7-Überwachungsdienst, der Bedrohungen in Echtzeit erkennt und darauf reagiert. Darüber hinaus sollte der Managed SOC-Service einen optionalen Cyber-Response-Support beinhalten,

der sowohl remote als auch vor Ort verfügbar ist. Neben der technischen Umsetzung stand die kontinuierliche Weiterentwicklung der Sicherheitsstrategie im Fokus: Axians sollte mit den HPM Verantwortlichen auf Augenhöhe agieren und nicht nur den laufenden Betrieb optimieren, sondern die Sicherheitsinfrastruktur fortlaufend an neue Bedrohungslagen anpassen.

Maßgeschneiderte Managed-SOC-Lösung

Axians entwickelte für HPM eine maßgeschneiderte SOC-Lösung, die Extended Detection and Response (XDR) mit Security Information and Event Management (SIEM) kombiniert. Da bisher kein SIEM-System im Einsatz war, lag der Fokus auf der nahtlosen Integration von SentinelOne und der Ablösung vorhandener Endpoint Protection Lösungen.

Die Lösung wird nun als Cloud-Service bereitgestellt, wodurch sie flexibel skalierbar ist und ohne aufwendige lokale Infrastruktur auskommt. Agenten auf den Endpunkten überwachen die Geräte kontinuierlich und melden verdächtige Aktivitäten in Echtzeit an das SOC-Team, um eine schnelle Reaktion zu ermöglichen.

AUFGABE / ZIEL

- Zentrale Überwachung und Verwaltung von Sicherheitsvorfällen
- Nahtlose Integration und Entlastung des IT-Security-Teams
- 24/7-Überwachung und schnelle Reaktion auf Bedrohungen

LÖSUNG

- Einführung eines SOC mit XDR und SIEM
- Cloudbasierte Integration für Skalierbarkeit und Effizienz
- Automatisierte Workflows zur schnellen Bedrohungsabwehr

NUTZEN

- Strukturierte Sicherheitsverwaltung mit voller Transparenz
- 24/7-Schutz durch Echtzeit-Überwachung und Reaktionsmechanismen
- Skalierbare Lösung, die mit den Anforderungen von HPM wächst

REFERENZ

HPM

Effektive Entlastung durch umfassenden Service

Der SOC-Service umfasst die detaillierte Analyse von Security Incidents auf Tier-Level 1 & 2, eine proaktive Bedrohungssuche (Threat Hunting) nach kundenindividuellen Kriterien sowie ein umfassendes Incident Management. Die EDR/XDR-Technologie schützt dabei eine Vielzahl von Endpoints, Workstations sowie Windows- und Linux/Unix-Servern, indem Log-Daten aus verschiedenen Quellen gesammelt und analysiert werden.

Zur kontinuierlichen Optimierung entwickelt Axians Playbooks, die eine schnelle und koordinierte Reaktion auf Bedrohungen ermöglichen. Ergänzend dazu erhält HPM monatliche Berichte über Sicherheitsvorfälle, inklusive Empfehlungen zur Verbesserung.

Proaktives Monitoring für schnelle Reaktion

Mit der neuen SOC-Lösung profitiert HPM von einer nahtlosen Integration bestehender IT-Systeme, einem proaktiven Monitoring durch das Axians SOC-Team und einer deutlich reduzierten Fehlerquote dank automatisierter Workflows. Durch den 24/7-Betrieb lassen sich potenzielle Bedrohungen rund um die Uhr analysieren und reaktionsschnell entschärfen. Sicherheitsvorfälle werden je nach Schweregrad innerhalb von 30 Minuten bis zwei Stunden bearbeitet, während ein dedizierter Ansprechpartner die Reaktionsmaßnahmen koordiniert und die gesamte Kommunikation übernimmt.

Nahtlos integrierte Sicherheit

Dank der nahtlosen Integration schützt die Cloud-Plattform die gesamte HPM Infrastruktur einschließlich aller 84 Standorte. Die EDR/XDR-Technologie überwacht sämtliche Endgeräte in Echtzeit und ermöglicht eine schnelle Reaktion auf Bedrohungen. Die SOC-Lösung ist dabei nicht nur leistungsstark, sondern auch hoch skalierbar und passt sich flexibel an steigende Sicherheitsanforderungen an.

Im Ergebnis sichert sich HPM mit dem Managed SOC-Service von Axians eine zukunftsfähige Cyber-Security-Lösung, die nicht nur schützt, sondern die Handwerksgruppe gezielt auf digitale Herausforderungen vorbereitet. Dabei steht Axians der Handwerksgruppe als strategischer Partner zur Seite, um gemeinsam auf neue Bedrohungen zu reagieren und die Sicherheitsstrategie kontinuierlich weiterzuentwickeln.

KUNDENINFO



Unternehmen: HPM Service und Verwaltung GmbH

Branche: Handwerk und Baugewerbe

Sitz: Hamburg, Deutschland

Dimension: HPM zählt mit über 4.000 Mitarbeitenden und mehr als 80 Standorten zu den führenden Unternehmensgruppen im deutschen Handwerk.

Internet: www.handwerksgruppe.de

ÜBER AXIANS

Die Unternehmensgruppe Axians in Deutschland ist Teil des globalen Markennetzwerks für ICT-Lösungen von VINCI Energies. Mit einem ganzheitlichen ICT-Portfolio unterstützt die Gruppe Unternehmen, Kommunen und öffentliche Einrichtungen, Netzbetreiber sowie Service Provider bei der Modernisierung ihrer digitalen Infrastrukturen und Lösungen. In den fünf Geschäftsbereichen Business Applications & Data Analytics, IT & Managed Services, TI Fixed Networks, TI Mobile Networks & Infrastructure Services und Public Software sorgen Berater:innen, Entwickler:innen und Techniker:innen dafür, das Leben von Menschen zu verbessern – etwa durch Cloud- und Data-Center-Infrastrukturen, Cybersicherheit, Unternehmens- und Breitbandnetze, IoT-Lösungen, Managed Services sowie führende Software für Abfallwirtschaft, Schüttgutindustrie, technischen Service und die öffentliche Verwaltung.

KONTAKT

E-Mail: info-itsecurity@axians.de · Tel: +49 40 271661-0

axians.de

Stand 07/26