systrade

JOVYATLAS GmbH

Case Study: Netzwerk- und Sicherheitheitsmodernisierung

Einleitung

JOVYATLAS ist ein renommierter Hersteller von USV-Systemen (Unterbrechungsfreie Stromversorgung) sowie kostengünstiger und stabiler Lösungen für Serverräume. Das Unternehmen beschäftigt mehrere hundert Mitarbeiter und ist an verschiedenen Standorten in Deutschland vertreten. Um die Sicherheit und Effizienz seiner IT-Infrastruktur zu erhöhen, entschied sich das Unternehmen für eine umfassende Modernisierung der Netzwerksicherheit und der zentralen IT-Managementstruktur.

Ausgangslage und Herausforderungen

JOVYATLAS stand vor der Herausforderung, die Sicherheit und Effizienz des Datenaustauschs zwischen dem Hauptstandort und den deutschlandweit agierenden Servicetechnikern zu verbessern. Die bestehende IT-Infrastruktur war heterogen, was eine einheitliche Verwaltung erschwerte. Zudem war die Absicherung der Kommunikation und der Endgeräte ein zentraler Aspekt zur Gewährleistung des Unternehmensbetriebs. Die Erhöhung der IT-Sicherheit ist essenziell, da durch zunehmenden Datenverkehr zwischen Hauptstandort und Servicetechnikern eine robuste Sicherheitsinfrastruktur notwendig wird. Gleichzeitig muss die bestehende IT-Architektur standardisiert werden, um eine effizientere Verwaltung zu ermöglichen. Eine dezentrale Verwaltung soll eine einheitliche Steuerung und Überwachung der Endpunkte ermöglichen. Zudem ist die Integration einer zentralen Firewall-Lösung erforderlich, inklusive Managed Detection and Response (MDR). Ein weiteres Ziel ist die sichere E-Mail-Kommunikation durch automatische E-Mail-Verschlüsselung für dedizierte Mitarbeiter. All diese Maßnahmen sollen im laufenden Betrieb eingeführt werden, ohne den Unternehmensablauf zu stören.

Technische Lösung

Zur Bewältigung dieser Herausforderungen wurde eine ganzheitliche Lösung mit Sophos-Sicherheitsprodukten implementiert. Eine Sophos-Firewall wurde eingeführt und zusätzlich dazu wurden die MDR-Lizenzen für User und Server ausgerollt. Sophos MDR (Managed Detection and Response) ist ein proaktiver Sicherheitsdienst, der Bedrohungen rund um die Uhr überwacht, analysiert und darauf reagiert. Mithilfe von KI-gestützten Analysen und einem Expertenteam werden verdächtige Aktivitäten identifiziert und Sicherheitsvorfälle verhindert, bevor sie Schaden anrichten können. Sophos MDR ist eng mit einem Security Operation Center (SOC) verbunden, das kontinuierlich sicherheitsrelevante Ereignisse überwacht, Bedrohungen analysiert und gezielte Gegenmaßnahmen einleitet. Dadurch wird eine schnelle Reaktionszeit auf Sicherheitsvorfälle gewährleistet und die allgemeine IT-Sicherheitslage erheblich verbessert. Die flächendeckende Implementierung von Sophos auf allen Geräten sorgte für ein einheitliches Sicherheitsniveau. Die zusätzliche Integration einer Sophos-Firewall ermöglicht eine zentrale Bedrohungserkennung und -abwehr in Echtzeit. Die Kommunikation zwischen dem Hauptstandort und den Servicetechnikern wurde durch verschlüsselte VPN-Verbindungen abgesichert. Dedizierte Mitarbeiter wurden mit einer automatisierten E-Mail-Verschlüsselung ausgestattet, sodass interne und externe Kommunikation sicher bleibt. Als zusätzliche Absicherung aller Benutzerkonten wurde für alle Office 365 Benutzer eine 2-Faktor-Authentifizierung aktiviert. Zudem wurde eine zentrale Verwaltung eingeführt, wodurch alle Sicherheitsmechanismen effizient in einem Dashboard überwachbar und steuerbar sind. Als zusätzliche Maßnahme zur Erhöhung der IT-Sicherheit wurde ein Notfalldienst Vertrag mit einem externen Dienstleister abgeschlossen.

Durch den Notfalldienst sollen Sicherheitsproblematiken, Sicherheitsaspekte und ausgeführte Angriffe mit Bezug auf die IT-Infrastruktur des Unternehmens beseitigt oder gestoppt werden. Der Notfalldienst greift mit dem Kunden aktiv in den Prozess des Angriffs ein, um so das Unternehmen vor fortlaufenden Schäden zu schützen.

Ergebnisse und Vorteile

Die Modernisierung führte zu einer erhöhten Sicherheit, da die gesamte Infrastruktur nun gegen externe Bedrohungen abgesichert ist, insbesondere durch die Integration der Sophos-Firewall mit MDR. Die einheitliche und einfache Verwaltung ermöglichte eine effizientere Steuerung aller Endgeräte. Zudem wurde der IT-Betrieb optimiert, da die Einführung ohne Unterbrechung des laufenden Betriebs erfolgte. Die sichere Kommunikation wurde durch die E-Mail-Verschlüsselung gewährleistet, sodass vertrauliche Informationen nur von berechtigten Empfängern gelesen werden können. Durch die Vereinheitlichung der Sicherheitsarchitektur ist das Unternehmen langfristig auf künftige Bedrohungen vorbereitet und sichert somit seine Investition in eine zukunftssichere IT-Struktur.