CUSTOMER CASE STUDY

Global geschützt, lokal handlungsfähig: Wie die KLINGER Holding mit Sophos MDR ihre internationale IT-Landschaft absichert

Mit Managed Detection and Response (MDR) von Sophos sichert die KLINGER Holding ihre internationale IT-Landschaft ab. Die Lösung ermöglicht es dem Industriekonzern, Bedrohungen gruppenweit zu erkennen und abzuwehren, während die lokalen IT-Teams weiterhin autonom agieren können.

SOPHOS

KLINGER trusted. worldwide.

KLINGER Holding GmbH

Industrie
Industrielle Dichtungs- und Fluidtechnik

Sophos-Lösungen
Sophos Managed Detection and Response

Nutzer
2.100

Sophos-Partner
ARTAKER IT Group

Die Fertigungsindustrie, zu der auch die österreichische KLINGER Holding zählt, steht besonders im Fokus von Cyberkriminellen: Laut dem Sophos State of Ransomware Report 2025 sind ausgenutzte Schwachstellen die häufigste Ursache für Ransomware-Angriffe in der Fertigungsindustrie und verantwortlich für 32 Prozent der Vorfälle. Die Branche bleibt weiterhin ein bevorzugtes Ziel von Cyberkriminellen. Allein im vergangenen Jahr wurden 99 verschiedene Bedrohungsgruppen aktiv, die gezielt produzierende Unternehmen ins Visier nahmen.

„Das Sicherheitsgefühl in der Gruppe hat sich deutlich verbessert. Wir wissen, dass uns Sophos MDR und das SOC gut schützen, egal zu welcher Uhrzeit."

Gernot Leithner
Head of Group IT & Digitalization
KLINGER Holding

Die Herausforderung

Die KLINGER Holding ist ein international agierender Industriekonzern mit dezentraler Infrastruktur, der in den Bereichen Dichtungen, Flüssigkeitsregelung und Flüssigkeitsüberwachung tätig ist. Das Unternehmen stand vor einer doppelten Herausforderung im Bereich IT-Sicherheit: Einerseits galt es, einen globalen Schutz vor Cyberangriffen zu gewährleisten, der den Anforderungen einer weltweit vernetzten Gruppe gerecht wird. Andererseits musste eine 24/7-Überwachung sichergestellt sein, um auf Bedrohungen in Echtzeit reagieren zu können.

Die IT-Landschaft der KLINGER Holding war geprägtvon einer Kombination aus Cloud-Services und lokaler Infrastruktur, was die Sicherheit komplex gestaltete. Bisher betrieben die einzelnen Unternehmen der Gruppe heterogene Sicherheits-Lösungen ohne nennenswerte Synergien. „Diese Situation beeinträchtigte nicht nur die Effizienz unserer IT-Arbeit, sondern begünstigte auch Angriffe", erklärt Gernot Leithner, Head of Group IT & Digitalization der KLINGER Holding. „Besonders kritisch war die fehlende Möglichkeit, Bedrohungen über die Grenzen einzelner Unternehmen hinweg zu erkennen und für die gesamte Unternehmensgruppe wirksam abzuwehren."

Eine weitere Anforderung an eine neue Security-Lösung bestand darin, dass die lokalen IT-Teams weiterhin die Freiheit behalten sollten, ihre Infrastruktur selbst zu verwalten und bei Bedarf direkt einzugreifen. „Wir brauchten eine Lösung, die uns global schützt, aber regional administrierbar bleibt, ohne uns mit unzähligen Meldungen zu überfluten, die am Ende niemand mehr ernst nimmt", ergänzt Leithner.

Die Lösung

Nach einer sorgfältigen Evaluierung entschied sich die KLINGER Holding für Sophos MDR (Managed Detection and Response) in Kombination mit dem Sophos SOC (Security Operations Center). Ausschlaggebend für diese Wahl waren mehrere Faktoren: Zum einen bot Sophos die einzigartige Möglichkeit, globalen Schutz mit regionaler Administration zu verbinden. Dies war besonders wichtig, da die Gruppe aus rund 50 Unternehmen in Europa, APAC, Afrika und Amerika besteht, die jeweils eigene

Anforderungen an die IT-Sicherheit stellen. Zum anderen überzeugte das intelligente Monitoring, das nicht mit einer Flut an Sicherheitsmeldungen überwältigt, sondern gezielt Meldungen mit hohen Risiken herausfiltert und priorisiert.

Ein weiterer entscheidender Vorteil war das lernende und KI-gestützte System von Sophos MDR, das verdächtige Aktivitäten nicht nur anhand fester Parameter, sondern auch durch die Erkennung von anomalem Verhalten identifiziert. Das Sophos SOC sichert die Gruppe zudem rund um die Uhr vor Bedrohungen ab – ein entscheidender Faktor für ein Unternehmen, das weltweit über viele Zeitzonen hinweg operiert. Nicht zuletzt spielte die Sophos Breach Protection Warranty innerhalb von Sophos MDR Plus eine entscheidende Rolle für die Entscheidung. Neben Diensten wie dem 24/7-Monitoring oder dem kontinuierlichen KI-gestützten Threat Hunting deckt die Sophos Breach Protection Warranty die Kosten für eine Reaktion auf Sicherheitsvorfälle von bis zu 1 Million US-Dollar ab.

Die Implementierung der Lösung erfolgte schrittweise und umfasste das Onboarding von rund 50 Unternehmen in den Verbund. Unterstützt von dezentralen Administratoren entstand so eine globale Übersicht, die gleichzeitig die lokale Flexibilität bewahrt. Dieser Prozess erforderte eine enge Abstimmung zwischen den verschiedenen Standorten, um sicherzustellen, dass alle Unternehmen nahtlos in das neue Sicherheitskonzept integriert werden konnten.

Das Ergebnis

Mit Sophos MDR hat die KLINGER Holding eine zukunftssichere Sicherheitsarchitektur geschaffen, die sowohl global als auch lokal überzeugt. Die Lösung ermöglicht es der Gruppe, Risiken frühzeitig zu erkennen und proaktiv abzuwehren, bevor sie Schaden verursachen können. Das Sophos SOC übernimmt dabei die kontinuierliche Überwachung und reagiert auf Bedrohungen auch außerhalb der regulären Arbeitszeiten, an Wochenenden und an Feiertagen.

Ein besonderer Vorteil der neuen Lösung ist die Fähigkeit, Seitwärtsbewegungen von Angreifern zu erkennen und zu verhindern. Dadurch können sich Bedrohungsakteure nicht mehr unbemerkt zwischen den Unternehmen der Gruppe bewegen. Aus Sicht der Mitarbeitenden arbeitet Sophos MDR im Hintergrund, ohne den Arbeitsalltag zu stören. Dies war ein zentrales Anliegen, um die Akzeptanz der Lösung im gesamten Unternehmen sicherzustellen.

Das IT-Personal hat die neue Lösung gut angenommen. Gezielte Schulungen halfen dabei, sich mit den Funktionen von Sophos MDR vertraut zu machen und das volle Potenzial der Technologie auszuschöpfen. „Das Sicherheitsgefühl in der Gruppe hat sich

deutlich verbessert. Wir wissen, dass uns Sophos MDR und das SOC gut schützen, egal zu welcher Uhrzeit", so Gernot Leithner. Auch die Entlastung der IT-Abteilung ist deutlich spürbar, da die permanente Überwachung im Hintergrund ein höheres Schutzniveau und zusätzlich Freiräume für strategische Aufgaben schafft.

Der Partner: ARTAKER IT

ARTAKER IT begleitet die KLINGER Holding seit Jahren bei der Auswahl und Implementierung von IT-Sicherheitslösungen. Die Enterprise-Erfahrung des Partners zeigte sich bereits in einem umfangreichen Infrastruktur- und Modernisierungsprojekt bei KLINGER: Innerhalb von 22 Monaten wurden rund 50 Unternehmen, mehr als 2.100 Nutzer sowie über 20 Tenant- und mehr als 30 EXO-Migrationen betreut. Zum Abschluss würdigte KLINGER den Einsatz des gemeinsamen Projektteams und bezeichnete das Ergebnis als „one incredible success story".

Die Artaker IT Group ist eine österreichische IT-Unternehmensgruppe mit Sitz in Wien. Seit über 30 Jahren begleitet die Gruppe mit rund 40 Mitarbeitenden Unternehmen auf ihrem Weg in die digitale Zukunft – getreu dem Claim „Get IT done". Als verlässlicher Partner erweitert ARTAKER IT bestehende Stärken intelligent, statt sie zu ersetzen. Unter dem Dach der Gruppe sind zwei Marken vereint: Artaker IT Services als Trusted Advisor und Managed Service Provider für den Mittelstand sowie Artaker Transformation, die die Gruppe mit einem AI-first-Ansatz für die Digitalisierung zentraler Geschäftsprozesse ergänzt. Damit kombiniert die Gruppe ihre Expertise aus IT-Betrieb, Security, Prozessdigitalisierung und Automatisierung. Die Schwerpunkte reichen von Enterprise Content Management und Geschäftsprozessautomatisierung über digitales Vertragsmanagement, Cloud- und Microsoft-Lösungen bis zu IT-Infrastruktur, Compliance und KI.

Mehr Informationen unter www.sophos.de

2026-08-12 CCS-DE (NP)