„Für uns war entscheidend, dass Angriffe nicht nur erkannt, sondern auch außerhalb der Geschäftszeiten automatisch gestoppt werden. Genau das leistet die von Axians implementierte Ransomware-Lösung."

Daniel Zehner, IT-Administrator, MOLL Batterien GmbH

REFERENZ

MOLL Batterien

Automatisierter Ransomware-Schutz für kritische Produktionsprozesse

Zuverlässige Energie für die Automobilindustrie

Seit ihrer Gründung im Jahr 1945 hat sich die MOLL Batterien GmbH zu einem anerkannten Entwicklungspartner der Automobilindustrie entwickelt. Am einzigen Produktionsstandort in Bad Staffelstein sind rund 240 Mitarbeitenden beschäftigt. Zu den wichtigsten Abnehmern zählen die Werke des Volkswagen-Konzerns, darunter Audi, Škoda, SEAT und Porsche.

Für ein Unternehmen dieser Größe ist ein Produktionsstillstand kein abstraktes Risiko, sondern eine reale Bedrohung mit messbaren Folgen für Lieferketten und Kundenbeziehungen. MOLL Batterien begegnete diesem Risiko mit einem klar definierten Ziel: Ransomware-Angriffe nicht nur erkennen, sondern vollautomatisch und rund um die Uhr stoppen, ohne das IT-Team zusätzlich zu belasten.

Cyberangriffe kennen keine Geschäftszeiten

Das mittelständische Unternehmen verfügt über ein schlankes IT-Team und betreibt kein eigenes SOC (Security Operations Center). Die vorhandene EDR-Lösung (Endpoint Detection and Response) bot zwar eine solide Grundlage im Tagesgeschäft, konnte jedoch keine vollautomatisierten Reaktionen auf komplexe Bedrohungsszenarien wie Zero-Day-Attacken oder Ransomware gewährleisten.

Besonders kritisch ist, dass Cyberangriffe selten während der Geschäftszeiten stattfinden. Ohne automatisierte Abwehr fehlte genau dann die notwendige Reaktionsfähigkeit, wenn sie am dringendsten benötigt wurde, also nachts, an Wochenenden und an Feiertagen.

Hinzu kamen wachsende regulatorische Anforderungen aus NIS2, TISAX, ISO und DSGVO, die eine strukturierte und nachvollziehbare Sicherheitsarchitektur voraussetzen.

Schutz vor Ransomware als gezielte Systemerweiterung

Gemeinsam mit Axians entschied sich MOLL Batterien bewusst gegen einen kostenintensiven SOC- oder MDR-Service (Managed Detection and Response) und für den gezielten Ausbau der bestehenden Sicherheitsarchitektur. Die Wahl fiel auf die spezialisierte Cyber-Security-Lösung von BullWall, die sich auf den aktiven Schutz vor Ransomware und anderen Angriffen konzentriert. Zum Einsatz kamen die Komponenten Ransomware Containment, Server Intrusion Protection sowie Virtual Server Protection. Die Lösung integriert sich über eine flexible API-Schnittstelle nahtlos in die bestehende EDR-Umgebung.

Das Sperren oder Isolieren eines Clients wird weiterhin über den EDR angestoßen, sodass beide Systeme ihre jeweilige Stärke ausspielen und funktional ineinandergreifen.

Im Ergebnis entsteht ein durchgängiges Sicherheitskonzept, das bestehende Investitionen schützt und gleichzeitig ein deutlich höheres Schutzniveau ermöglicht.

AUFGABE / ZIEL

- Schutz vor Ransomware und modernen Cyberangriffen
- Automatisierte 24/7-Reaktion auf Sicherheitsvorfälle
- Entlastung des IT-Teams bei begrenzten Ressourcen

LÖSUNG

- Integration in die bestehende EDR-Umgebung
- Machine-Learning-basierte Analyse von Systemverhalten
- Automatisierte Eindämmung von Angriffen

NUTZEN

- Reduzierte Angriffsfläche und verbesserte Sicherheitslage
- Automatisierter 24/7-Schutz ohne manuelle Eingriffe
- Spürbare Entlastung der IT-Abteilung
- Vermeidung von Produktionsausfällen und Sicherheitsvorfällen
- Unterstützung bei Compliance und Audits

REFERENZ

MOLL Batterien

Von der Lernphase zur aktiven Angriffserkennung

Die Implementierung erfolgte innerhalb von vier Tagen und begann mit einer rund sechswöchigen Lernphase. In dieser Zeit analysierte das System das Verhalten der IT-Umgebung und lernte, echte Anomalien von normalem Betrieb zu unterscheiden.

Nach Abschluss dieser Phase wurde der sogenannte Kill-Switch aktiviert. Seit diesem Zeitpunkt erkennt die Lösung verdächtige Aktivitäten in Echtzeit und greift automatisiert ein, indem sie betroffene Systeme isoliert und die Ausbreitung eines Angriffs verhindert.

Die Integration verlief reibungslos, der laufende Betrieb wurde zu keinem Zeitpunkt beeinträchtigt. Die Lösung ist seit April 2025 im produktiven Einsatz.

Mehr Sicherheit bei weniger Aufwand

Mit der Einführung des automatisierten Ransomware-Schutzes konnte MOLL Batterien die Cybersicherheit signifikant verbessern und gleichzeitig den operativen Aufwand deutlich reduzieren. Bedrohungen wie Phishing, Malware, Zero-Day-Angriffe und Ransomware werden frühzeitig erkannt und blockiert, bevor sie operative Prozesse erreichen. Das Risiko von Produktionsausfällen, Reputationsschäden und Haftungsrisiken sinkt dadurch spürbar. Sicherheitsvorfälle werden automatisiert bewertet und behandelt, ohne manuelle Analyse oder Eskalation.

Das IT-Team kann sich auf strategische Projekte konzentrieren, während gleichzeitig die Reaktionsgeschwindigkeit steigt.

Auch auf geschäftlicher Ebene zeigt sich der Mehrwert deutlich: Produktionsausfälle lassen sich vermeiden, sensible Daten werden geschützt und potenzielle Reputationsschäden reduziert. Gleichzeitig werden hohe Kosten durch Sicherheitsvorfälle oder externe Maßnahmen vermieden, wodurch die IT-Kosten besser planbar sind.

Zusätzlich werden mehrere Sicherheitsfunktionen in einer Plattform gebündelt, was Komplexität sowie Lizenz- und Wartungsaufwand in der bestehenden Sicherheitsarchitektur reduziert. Darüber hinaus unterstützt die Ransomware-Lösung die Einhaltung regulatorischer Anforderungen und erleichtert die Vorbereitung auf Audits durch nachvollziehbare Prozesse und eine transparente Dokumentation.

Zukunftssichere IT durch automatisierten Ransomware-Schutz

Das Projekt zeigt, wie sich auch mit begrenzten Ressourcen ein hohes Sicherheitsniveau erreichen lässt. Durch die gezielte Ergänzung bestehender Systeme und den Einsatz automatisierter Schutzmechanismen konnte MOLL Batterien eine leistungsfähige und zukunftssichere Sicherheitsarchitektur aufbauen.

Axians agierte dabei nicht nur als Implementierungspartner, sondern als strategischer Berater, der gemeinsam mit MOLL Batterien eine passgenaue Lösung entwickelt hat. Das Ergebnis ist ein skalierbarer Ansatz, der sich auf produzierende Unternehmen übertragen lässt, die ihre Cybersicherheit stärken möchten, ohne zusätzliche organisatorische Komplexität aufzubauen.

KUNDENINFO

Unternehmen: MOLL Batterien GmbH

Branche: Automotive, Elektro & Aerospace

Sitz: Bad Staffelstein, Deutschland

Größe: Rund 240 Mitarbeitende in Bad Staffelstein, spezialisiert auf Batteriesysteme für die Automobilindustrie.

Internet: www.moll-batterien.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