CASE STUDY

SentinelOne

Keine halben Sachen: Die ESA Elektroschaltanlagen Grimma GmbH ersetzt AV-Lösung mit der All-in-One-Plattform von SentinelOne

Eine kontinuierliche Überprüfung und Aktualisierung bestehender Prozesse hat für die ESA Elektroschaltanlagen Grimma GmbH oberste Priorität und ist ein Garant für die gleichbleibend hohe Qualität – dies betrifft die Bereiche Entwicklung und Fertigung ebenso wie die IT-Sicherheit. Im Rahmen einer wirtschaftlichen und IT-strategischen Überprüfung ihrer Endpunktsicherheit hat die IT-Abteilung deshalb entschieden, dass es Zeit ist, die traditionelle Antiviren-Lösung durch eine Endpoint-Security-Plattform abzulösen. Die Sicherheit im Unternehmen konnte durch diese Entscheidung nur gewinnen.

Der Kunde: Die ESA Elektroschaltanlagen Grimma GmbH

Mit ca. 350 Mitarbeitern und einer Produktionsfläche von 9.700 qm ist die ESA Elektroschaltanlagen Grimma GmbH eines der großen inhabergeführten, mittelständischen Unternehmen im Landkreis Leipzig. Als ausgewiesener Spezialist für die Entwicklung und Herstellung von Niederspannungsschaltanlagen, elektrischen Weichenheizungsanlagen für den Schienenverkehr, sicherer Stromversorgung in Krankenhäusern und Komplettlösungen im Bereich der Produktionsanlagen-Automatisierung, genießt das Unternehmen auch international einen ausgezeichneten Ruf, weshalb das Unternehmen neben den Standorten Grimma und Leipzig auch Vertriebsbüros in China und in den USA betreibt.

ESA GRIMMA
ESA ELEKTROSCHALTANLAGEN GRIMMA GmbH

HERAUSFORDERUNG

- Lückenlose und effektive Cybersicherheit
- Maximale Performance bei minimalen Hardware-Ressourcen
- Kurze Reaktionszeit und Reduzierung des administrativen Aufwands

LÖSUNG

- Endpoint-Security-Plattform von SentinelOne
- Umsetzung durch GORDION, Troisdorf

VORTEILE

- Effective Malware-Abwehr mit hohem Grad an Automatisierung
- Geringer Verwaltungsaufwand für die IT-Abteilung
- Nahtlose Integration in das bestehende Security-Konzept

Die Ausgangslage: Erhöhtes Sicherheitsbewusstsein zum Schutz der Produktion

Die Gewährleistung einer lückenlosen und effektiven Cybersicherheit ist für Unternehmen heute eine der größten Herausforderungen. Tatsache ist: Je größer IT-Infrastrukturen werden – sprich, je mehr Geräte internetfähig sind – desto höher wird der Aufwand, diese Geräte sicherheitstechnisch auf dem neuesten Stand zu halten. Die Anzahl der Sicherheitslücken in den einzelnen Systemen steigt – und parallel damit das Bedrohungspotential hinsichtlich Cyberangriffen.

Bei der ESA Grimma GmbH bildet die Basis der unternehmensweiten IT-Sicherheit ein mehrstufiges Schutzkonzept bestehend aus Endpunktsicherheit, Firewall und Mail-Security-Systemen von Fortinet, die mit Server-Security-Produkten ergänzt werden.

Der Wunsch: Kurze Reaktionszeiten und eine Minimierung des administrativen Aufwands

Als die Lizenzierung ihres bisherigen Antiviren-Produktes auslief, nutzte die IT-Abteilung der ESA Grimma GmbH diese Gelegenheit für eine grundlegende wirtschaftliche und IT-strategische Überprüfung ihrer unternehmensweiten Endpunktsicherheit. Da die Kommunikation der vorhergehenden AV-Lösung mit dem vom Unternehmen eingesetzten Network-Access-Control-System mit einer Reaktionszeit von mehr als einer Minute deutlich zu lange dauerte, stand schnell fest, dass eine neue, schnellere Lösung zum Einsatz kommen sollte. Bezüglich der Anforderungen an das neue Produkt war sich das Team dabei umgehend einig: So sollte die neue Lösung hoch performant sein, möglichst wenig Hardware-Ressourcen benötigen und gleichzeitig möglichst einfach zu verwalten sein, um den administrativen Aufwand für die Mitarbeiter soweit es geht zu minimieren.

„Als unser Endpunktschutz noch aus einer traditionellen AV-Lösung bestand, konnten wir nie ausschließen, dass trotz Eingangsprüfung von externen Datenträgern Schadsoftware unsere IT-Infrastruktur befällt. Diese Bedrohung ist seit dem Einsatz von SentinelOne so nicht mehr existent.“

Marco Sackersdorff
IT-Administrator bei
ESA Grimma GmbH

Die Entscheidung: Die Endpoint-Security-Lösung, die alles kann

Bei der Evaluierung möglicher Endpunkt-Security-Produkte wurde das Unternehmen dann von ihrem langjährigen IT-Consultant und Systemintegrator GORDION Data Systems Technology GmbH unterstützt. Nach eingehender Analyse verschiedener Technologien und interner Beratung mit der Geschäftsführung fiel die Entscheidung schließlich auf die Endpunktsicherheits-Plattform von SentinelOne. „Wir konnten das Produkt im Vorfeld auf insgesamt 50 PCs testen und haben dabei schnell festgestellt, dass SentinelOne die sicherste, benutzerfreundlichste und performanteste Endpoint Protection-Lösung ist, die derzeit zur Auswahl steht,“ so Marco Sackersdorff, IT-Systemadministrator bei der ESA Grimma GmbH. „Der Großteil der Implementierung konnte dann in nur wenigen Wochen und ohne größere Störungen abgeschlossen werden. Alles in allem also ein gelungener Prozess, bei dem uns das Support-Team von SentinelOne und Gordion jederzeit zur Seite stand und alle offenen Fragen kompetent und verständlich beantwortet hat.“

Das Ergebnis: Auch dateilose Schadsoftware im Griff

Die Vorteile der SentinelOne-Technologie wurden dabei schnell sichtbar. So minimiert die EPP-Plattform nicht nur den allgemeinen administrativen Aufwand, sie macht auch zusätzliche Virenprüfungen nach einem Malwarefund unnötig, was die IT-Abteilung ein weiteres Mal entlastet. Ein Segen ist dabei der hohe Grad der Automatisierung der Lösung, welcher eine unvergleichlich effektive Malware-Eindämmung ermöglicht: So werden etwa befallene Systemen ganz automatisch vom Netzwerk getrennt, was das Risiko einer unkontrollierten Weiterverbreitung von Schadsoftware verhindert.

Dass das Niveau der Endpunktsicherheit bei der ESA Grimma GmbH heute so hoch ist wie nie zuvor, liegt aber auch an SentinelOnes dynamischen Verhaltensanalyse-Techniken, die auf maschinellem Lernen beruhen. Diese identifizieren bösartigen Code allein anhand seines Laufzeitverhaltens, weshalb auch dateilose oder speicherbasierte Schadsoftware-Varianten, die Pattern-basierte Antiviren-Systemen problemlos umgehen können, entdeckt und blockiert werden.

Das Fazit: Goodbye AV, hello Security

Das bisher vom Unternehmen eingesetzte AV-Produkt wurde letztlich hinfällig und konnte vollständig durch die neue Lösung ersetzt werden. Alle anderen Sicherheitssysteme bleiben im Einsatz und bilden zusammen mit der SentinelOne-EPP nun einen mehrschichtigen, robusten Schutzwall, der sowohl Cybersicherheit als auch Nutzerfreundlichkeit bei ESA Grimma auf eine neue Stufe gehoben hat. So profitieren die IT-Mitarbeiter von einer nie dagewesenen Transparenz über das gesamte Netzwerk hinaus, die es ihnen ermöglicht, den Modus Operandi der Angreifer schnell zu durchschauen und in Echtzeit darauf zu reagieren.