Case Study

Wie Axians das IT-Netzwerk gegen Cyberbedrohungen sichert

Über Dalli-Werke GmbH & Co. KG

Mit langjähriger Forschungsexpertise in der Haushalts- und Schönheitspflege entwickelt das traditionsreiche Familienunternehmen Dalli-Werke innovative, leistungsstarke Produkte mit hoher Verbraucherakzeptanz. Dies sichert dem Unternehmen regelmäßig Spitzenergebnisse bei den europäischen Verbrauchertestorganisationen, wie z.B. der Stiftung Warentest und Öko-Test in Deutschland. Um diesen Erfolg in Zeiten umfassender Digitalisierung und Vernetzung nicht durch neuartige Cyberbedrohungen zu gefährden, setzen die Dalli-Werke auf fortschrittliche IT-Sicherheitslösungen der Axians.

Anforderungen

- Erhöhung des Reifegrads der IT-Security
- Proaktive Reaktion auf unbekannte Angriffe
- Steigerung der Detektions- & Response-Rate

Facts

- Konsumgüter
- In Deutschland ansässig
- > 1.300 Mitarbeitende



Herausforderung:

Diverse Sicherheitsvorfälle in der Vergangenheit ließen das Bewusstsein des Unternehmens für die Notwendigkeit einer umfassenden Absicherung gegen kurzfristige und langfristige Angriffe auf die Unternehmensnetzwerke wachsen. Cyberangriffe können für Unternehmen zu erheblichen Nachteilen wie Betriebsausfällen, Geldstrafen, rechtlichen Auseinandersetzungen mit Partnern und Kunden sowie Imageschäden führen. Die Dalli-Werke planten daher, zusätzliche Sicherheitslösungen in ihr Unternehmensnetzwerk zu integrieren und das Expertenwissen im Umgang mit Bedrohungen auszubauen. Eine verbesserte Kommunikation zwischen internen und externen Experten soll dabei helfen, eine robuste Verteidigungslinie aufzubauen und die Unternehmensdaten effektiv zu schützen.

Lösung: Managed SOC

Als Konsumgüterhersteller entschieden sich Dalli-Werke für den Managed Security Service - Managed SOC, um die Aktivitäten innerhalb ihres Unternehmensnetzwerks zu überwachen.

Zunächst analysierte das Axians-Team den Ist-Zustand der IT-Infrastruktur. Demnach waren die Dalli-Werke im Bereich der Prävention mit klassischen IT-Security-Komponenten gut aufgestellt. Jedoch verfügten sie nicht über ein dediziertes Security Monitoring, um den Datenverkehr und die Ereignisse innerhalb des Unternehmensnetzwerks zu überwachen und Auffälligkeiten durch SOC-Analysten zu analysieren.
Daraus ergab sich die Aufgabenstellung, die Kommunikation und Dokumentation des Datenverkehrs durch ein „Security Information and Event Management System" (SIEM) zu unterstützen. Dieses sollte systembezogene Berichte (Logs) automatisch qualifizieren, korrelieren und melden können.

Eine Meldung kann eine Aufnahme oder Alarmierung als Sicherheitsvorfall bedeuten sowie in regelmäßigen Abständen als Report abgerufen oder versendet werden. Das SIEM unterstützt damit den Betrieb aus drei Perspektiven: **Compliance, operatives Geschäft und IT-Sicherheit.**

Erfolgreiche Implementierung des Managed SOC:

Die Dalli-Werke wählten hierfür das Managed SOC. Als einer der führenden IT-Security-Provider in Deutschland, implementierte die Axians im ersten Quartal 2021 die Lösung in weniger als zwei Monaten. Der Kunde schätzte die strategische Beziehung und das Vertrauen in die Ansprechpartner der Axians. Ihn überzeugte die Passgenauigkeit der Lösung zur IT-Architektur des Unternehmens, die Flexibilität hinsichtlich Skalierbarkeit und die Möglichkeit der zukunftsorientierten Erweiterbarkeit sowie die schnelle Umsetzung und gute Zusammenarbeit.

> Axians hat in diesem Projekt durch hohe Flexibilität und eine zügige Umsetzung überzeugt. Dies hat uns in die Lage versetzt, bereits in relativ kurzer Zeit wertvolle und wichtige Ergebnisse zu erhalten.
>
> **Stephan Willems -** Leiter IT-Infrastruktur & IT-Support, Dalli-Werke GmbH & Co. KG

Projektablauf

- Abstimmung und Planung der Kommunikationswege und Installation des Managed SOC
- Anbindung der Log-Quellen und im weiteren Verlauf die Optimierung der Serviceelemente
- Weiterer Ausbau der Services und Entwicklung spezifischer Use-Cases
- Das Managed SOC analysiert und korreliert die Logdateien der Dalli-Werke und reichert Incidents mit externer Sicherheitsinformationen wie Indicators of Compromise (IOCs) an und alarmiert die Analysten bei Anomalien und potenziellen Bedrohungen im SOC. Die Analysten können somit jeden Alarm weiterführend qualifizieren und entsprechende Handlungsempfehlungen einleiten.

Eingesetzte Managed Security Services

- **Incident Response**
- **Incident Monitoring**
- **KPI-Reporting**
- **Threat Intelligence**
- **Use Case Development**

Ergebnis: Next-Level IT-Security

Die IT-Infrastruktur der Dalli-Werke hat sich mit diesem Projekt im Bereich der Detektion und Reaktion von Cyberangriffen durch das Managed SOC verbessert und kann somit proaktiv mit den Spezialisten der Axians auf Cyberangriffe reagieren. Dalli-Werke haben das IT-Sicherheitsniveau spürbar gesteigert.



Axians magellan GmbH · Max-Reichpietsch-Str. 1-5 · 51147 Köln
info-aml@axians.de · www.axians.de/magellan