SUCCESS STORY

ERFOLGE DER TECHNOLOGIE-PARTNERSCHAFT
MIT DER EBM-PAPST GROUP

sure[secure]

ebmpapst

WEBSITE

https://www.ebmpapst.com/

REGION

Standorte in Europa

BRANCHE

Produzierendes Unternehmen

MITARBEITER

Rund 15.115

01 DIE AUSGANGSSITUATION

Die ebm-papst Unternehmensgruppe, Weltmarktführer bei Ventilatoren und Motoren mit Sitz in Mulfingen, hat im Jahr 2018 beschlossen, die Aktivitäten im Bereich der Informationssicherheit zu intensivieren und gesellschaftsübergreifend neu zu koordinieren. Zielsetzung dabei war, das Niveau der Informationssicherheit innerhalb der Unternehmensgruppe zu erhöhen und die zentrale IT-Sicherheitsrichtlinie zu überarbeiten.

Die verschiedenen IT-Security-Insellösungen innerhalb der Unternehmensgruppe boten vor Projektstart zwar punktuell Schutz, besaßen jedoch keine Möglichkeit untereinander zu kommunizieren. Daher wurde beschlossen, eine Softwarelösung am Markt zu suchen, bei der sich die unterschiedlichen Softwarekomponenten automatisiert austauschen.

Bei der Qualifizierung der für ebm-papst optimalen Lösung unterstütze die suresecure GmbH in beratender Funktion. Nach erfolgter Marktanalyse konnte sich das Softwarehaus Trend Micro mit dem Produkt „Connected Threat Defense“ durchsetzen. Es wurde mit ebm-papst ein Projektplan mit 3-jähriger Laufzeit erarbeitet, um die IT-Sicherheit in der gesamten Gruppe zu erhöhen.

02 DIE HERAUSFORDERUNG

Bevor die erste Phase des Projektes in die Implementierungsphase gehen konnte, lastete eine durch einen Virusangriff verursachte IT-Störung eine Vielzahl an Systemen kurzzeitig stark aus.

Auch hier konnte die suresecure sofort unterstützen und zur Lösung beitragen. Eine große Herausforderung in jedem Incident Response-Prozess ist es, die erhobenen Informationen korrekt und effizient zu verarbeiten. Nicht selten wird falschen Fährten nachgegangen oder benötige Informationen stehen erst Stunden später zur Verfügung, weil diese aus den verschiedensten Systemen zusammengetragen werden müssen.

03 DIE LÖSUNG

Die Antwort auf diese Herausforderung war Splunk. Für jede aufkommende Frage wurde ein Dashboard erstellt, damit Informationen in Echtzeit korreliert und somit gängige Fragen sofort beantwortet werden konnten. Um auch automatisiert den Angriff eindämmen zu können, wurde zusätzlich die Connected Threat Defense von Trend Micro implementiert.

04 ERREICHTE ERFOLGE

Ein ganzheitliches IT-Security-Konzept der suresecure adressiert diese Herausforderungen zielgerichtet und ermöglichte bereits erhebliche Verbesserungen in der IT-Infrastruktur der ebm-papst Unternehmensgruppe.

Erhöhung der Schutzmechanismen durch:

- Machine Learning
- Sandboxing
- Behavior Monitoring
- Intrusion Prevention
- Visibilität im Netzwerk
- Einführung eines SIEM
- Network Intrusion Detection Systeme
- Automatisierte Reaktion
- Connected Threat Defense
- Unterstützung von APIs
- Unterstützung von IOCs

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de