enthus

Sichere Basis für die IT

EEW SPC setzt bei der Bedrohungserkennung auf SIEM-as-a-Service von enthus

Die Challenge

- Umfassende Absicherung der IT-Infrastruktur eines produzierenden Unternehmens
- Begrenzte personelle Ressourcen in der IT-Abteilung

Unser Job

- Überprüfung der IT-Sicherheitsstrategie im Rahmen eines Security-Workshops
- Implementierung und Betrieb eines zentralen Log-Servers
- Umsetzung einer individuell angepassten SIEM-as-a-Service-Lösung

Der Businessvorsprung

- Echtzeit-Überwachung der gesamten IT-Infrastruktur auf Anomalien
- Schnellere Reaktionsmöglichkeiten bei Cyber-Angriffen
- Sichere zentrale Speicherung aller Log-Daten für Forensik und Compliance
- Kostenersparnis im Vergleich zu einer selbst betriebenen SIEM-Lösung

EEW SPC

Die EEW Special Pipe Constructions (EEW SPC) GmbH spielt für den Ausbau der weltweiten Offshore-Windindustrie eine tragende Rolle – und das im wahrsten Sinne des Wortes: Das 2008 gegründete Unternehmen ist Vorreiter bei der Herstellung von Monopiles, die als Gründungspfähle für Offshore-Windkraftanlagen dienen.

In seinem Rostocker Werk produziert EEW SPC dickwandige Rohre mit einem Durchmesser von bis zu zwölf Metern, einer Länge von bis zu 120 Metern und einem Stückgewicht von bis zu 2.500 Tonnen. Mit mehr als 2.100 ausgelieferten Monopiles ist das Unternehmen heute Weltmarktführer.

Weitere Informationen finden Sie unter:
www.eewspc.de

EEW SPC liefert starke Fundamente für Offshore-Windkraftanlagen auf der ganzen Welt. Die Basis für die eigene IT-Sicherheit bezieht das Unternehmen von enthus: Mit SIEM-as-a-Service kann EEW SPC Bedrohungen in Echtzeit erkennen, bewerten und abwehren – bevor das Unternehmen Schaden nimmt. Die Sicherheitsspezialisten von enthus arbeiten dabei Hand in Hand mit dem internen IT-Team zusammen.

enthus

> „Der Service von enthus macht professionelles SIEM und zentrales Logging für uns sehr einfach nutzbar. Wir stärken damit unsere Sicherheitsstrategie und sind nun in der Lage, mögliche Angriffe auf unsere IT früher zu erkennen. Das lässt uns heute deutlich ruhiger schlafen.“
>
> **Marco Sieg,** IT-Leiter, EEW Special Pipe Constructions GmbH

IT-Risiken für die Produktion minimieren

Offshore-Windparks werden heute in immer größeren Meerestiefen und mit immer leistungsstärkeren Turbinen geplant. Die Rohrfundamente von EEW SPC müssen daher enormen Kräften standhalten und fest im Meeresboden verankert werden. Nur so können die Windkraftanlagen sicher arbeiten und zuverlässig nachhaltigen Strom für eine klimafreundliche Energieversorgung produzieren.

Hohe Sicherheitsanforderungen gelten heute auch für die IT von EEW SPC. „Als schnell wachsendes Produktionsunternehmen müssen wir unsere digitalen Prozesse so gut wie möglich vor Cyber-Risiken schützen“, sagt Marco Sieg, IT-Leiter des Unternehmens. „Ein Ausfall wichtiger IT-Systeme könnte unsere Produktion sehr schnell lahmlegen.“

Mit einem kleinen IT-Team ist es jedoch nicht einfach, alle aktuellen Bedrohungsszenarien und Entwicklungen im Security-Bereich im Blick zu behalten. EEW SPC beschloss daher, die eigene Sicherheitsstrategie auf den Prüfstand zu stellen. Das Unternehmen vereinbarte einen Workshop mit Security-Spezialisten von enthus, um mögliche Schwachstellen aufzudecken und Expertentipps zur Absicherung der Infrastruktur zu erhalten.

Mit zentralem Logging und SIEM zu höherer Sicherheit

Im Rahmen des enthus Security Checks wurden EEW SPC vor allem zwei Maßnahmen empfohlen: die Einrichtung eines zentralen Log-Server und der Einsatz eines SIEM-Systems (Security Information & Event Management). SIEM-Lösungen überwachen IT-Infrastrukturen auf mögliche Anomalien und können bereits an subtilen Veränderungen erkennen, dass ein Cyberangriff stattgefunden hat. Dadurch gewinnen Unternehmen Zeit, um im Ernstfall schnellstmöglich zu reagieren und den Schaden zu begrenzen.

Die Datenbasis für das SIEM-System liefert ein zentraler Log-Server. Hier laufen die Daten zusammen, die für eine effektive Überwachung und Analyse von IT-Systemen und Netzwerken relevant sind – also zum Beispiel Log-Daten von Netzwerkkomponenten, Firewalls, Servern und Endgeräten. Diese Daten werden auch für die forensische Untersuchung von Sicherheitsvorfällen benötigt. Zentrales Logging erleichtert Unternehmen zudem die Einhaltung von Compliance-Anforderungen.

„Wir haben sehr schnell verstanden, dass wir mit diesen Maßnahmen die Sicherheit unserer IT auf ein neues Niveau heben“, sagt Marco Sieg. „Allerdings war uns auch klar, dass wir die dafür notwendigen Komponenten mit unserem Team nicht alleine implementieren und betreiben können. Deshalb haben wir uns für das SIEM-as-a-Service-Angebot von enthus entschieden, das auch einen zentralen Log-Server beinhaltet.“

enthus

Security-Service entlastet das IT-Team

Nachdem die Entscheidung für den Service gefallen war, startete enthus sehr schnell mit der Umsetzung. Die Spezialisten des IT-Dienstleisters richteten den Log-Server und die SIEM-Lösung auf Basis von Splunk Enterprise Security im Rechenzentrum von EEW SPC ein. Bereits nach wenigen Tagen waren alle wichtigen Datenquellen angebunden.

Im nächsten Schritt ging es nun darum, das „Datenrauschen" zu reduzieren, und zum Beispiel falsch positive Warnmeldungen herauszufiltern. „Dabei konnten wir enorm von der Expertise von enthus profitieren", berichtet Marco Sieg. „Die Spezialisten haben sich von Anfang an auf die für uns relevantesten Anwendungsfälle und Überwachungspunkte konzentriert. Ohne enthus hätten wir Monate gebraucht, um aus der Masse an Daten die richtigen Erkenntnisse zu ziehen."

Mit dem neuen Service erhält EEW SPC einen ganzheitlichen Überblick über die Sicherheitslage der IT-Umgebung und wird automatisch über allen Auffälligkeiten informiert. Das IT-Team bespricht diese mit den Security-Experten von enthus und kann dann bei Bedarf sehr schnell die notwendigen Schritte einleiten. Gerade in der Anfangszeit waren häufig falsch konfigurierte Systeme die Ursache für die Anomalien. Der neue Service hilft dem Unternehmen daher auch kontinuierlich, Fehlerquellen zu reduzieren und die eigene Infrastruktur zu optimieren.

„Die SIEM-Lösung liefert uns viele wertvolle Einblicke in unsere Infrastruktur und eine verlässliche Datenbasis, um in jeder Situation die richtigen Entscheidungen zu treffen", fasst Marco Sieg zusammen. „Entscheidend ist aber natürlich auch, dass wir mit enthus einen Partner an unserer Seite haben, der uns bei der Erkennung und Beseitigung von Bedrohungen kompetent unterstützt."

enthus

Über 500 Enthusiast:innen an 10 Standorten in Deutschland, Österreich und der Schweiz sind bei 170 Millionen Euro Jahresumsatz (2022) leidenschaftliche #erfolgreichmacher für IT und Digitalisierung. Mit innovativen IT-Lösungen, Managed Services & XaaS sowie unseren smarten Lösungen für digitale Geschäftsprozesse wollen wir #yourfirstchoice auf dem Weg ins digitale Zeitalter sein.

Denn Herausforderungen löst man am besten im Schulterschluss – partnerschaftlich und auf Augenhöhe.

Weitere Informationen finden Sie unter: **www.enthus.de**

Interessiert?

Wolfgang Hahl
Mitglied der Geschäftsführung
E-Mail: hallo@enthus.de