CYBER-SICHERE VERSORGUNG IN WÜRZBURG

Würzburger Versorgungs- und Verkehrs-GmbH etabliert SIEM-Lösung mit Splunk.

AUF EINEN BLICK

AUFGABE

Aufbau einer Splunk Enterprise-Lösung als SIEM für die IT-Infrastruktur der WVV sowie zugehörige kritische Infrastrukturen

SYSTEME UND SOFTWARE

> Splunk Enterprise

VORTEILE

> Automatische Erkennung von Ereignismustern und Echtzeit-Interaktion mit Suchergebnissen

> Etablierung eines zentralen, aktuellen Standardsystems, jederzeit erweiterbar um neue Anwendungen

> Bedrohungen mit verlässlichen Informationen und leistungsfähigen Analysen erkennen und bekämpfen

WÜRZBURGER VERSORGUNGS- UND VERKEHRS-GMBH (WVV)

Die Würzburger Versorgungs- und Verkehrs-GmbH (WVV) ist ein deutsches Infrastrukturunternehmen und Energieversorger mit Sitz in Würzburg. Die Gesellschaft befindet sich vollständig im Besitz der Stadt Würzburg und versorgt die Stadt und viele Randgemeinden mit Strom, Erdgas, Fernwärme und Trinkwasser.

HERAUSFORDERUNG

Das IT-Sicherheitsgesetz verlangt von Betreibern kritischer Infrastrukturen (KRITIS), wie der WVV, dass sie ihre Netze besser schützen und Angriffe melden. Entsprechend wurde hier 2018 die ISO 27001 Zertifizierung durchgeführt und es musste als Schutzmaßnahme ein Security Information & Event Management (SIEM) System als Teil der Cyber-Sicherheitsstrategie etabliert werden.

LÖSUNG

Nach ersten Beratungsgesprächen mit SVA-Experten war klar, dass die Lösung auf Splunk basieren sollte. Wichtig war zunächst die Definition eines SIEM-Rahmenwerks inklusive der Prozesse und relevanten Playbooks unter Berücksichtigung der bestehenden IT-Organisation sowie der IT-Governance der WVV. Dies erfolgte in drei Schritten:

1. Fachliche Konzeption unter Einbeziehung grundsätzlicher Basisanforderungen an das SIEM sowie fachlicher Grundausbau und Erarbeitung eines Konzeptes zur Operationalisierung
2. Technische Konzeption und Implementierung der technischen SIEM-Lösung
3. Ausbau des SIEM-Konzeptes für die Beschreibung weiterer Use Cases und Anbindung weiterer Anwendungen

PLATTFORM FÜR OPERATIONAL INTELLIGENCE

Mit Splunk Enterprise steht der WVV eine Lösung zur Verfügung, die Maschinendaten aus beliebigen Quellen überwacht und analysiert, um Operational Intelligence bereitzustellen. Mit intuitiven Analysefunktionen, Machine Learning, standardisierten Anwendungen und offenen APIs ist die Plattform flexibel und kann von spezifischen Anwendungsfällen auf ein unternehmensweites Analyse-Backbone skaliert werden. Dabei können nun folgende Aufgaben unterstützt werden:

> Echtzeit-Monitoring des Sicherheitsniveaus mit einem klaren, grafisch aufbereiteten Bild, individuell anpassbar und mit Drilldowns zu den zugrundeliegenden Ereignissen
> Sicherheitsspezifische Sicht auf die Daten, um die Erkennungsmöglichkeiten zu vergrößern und die Reaktion bei Vorfällen zu optimieren
> Ad-hoc-Suchen und statische, dynamische und visuelle Korrelationen, um böswillige Aktivitäten aufzuspüren
> Mehrstufige Sicherheitsverletzungs- und Untersuchungsanalysen, um die dynamischen Aktivitäten im Zusammenhang mit komplexen Bedrohungen nachzuverfolgen

Splunk ES kann als Software verteilt werden, als Cloud-Service, in einer öffentlichen oder privaten Cloud oder in einer Hybridumgebung aus lokaler Software und Cloud-Verteilung. Bei der WVV setzt man auf eine Kombination aus Hybridumgebung aus lokaler Software und Cloud-Verteilung.

Durch die Etablierung eines zentralen, aktuellen Standardsystems wird bei Fehleranalyse Zeit durch die zentrale Log-Sammlung gespart. Probleme können so auf Log-Ebene analysiert und zentral mit anderen Systemen gegengeprüft werden. Splunk bietet außerdem Visualisierungen von Log-Daten anhand von Dashboards an. Somit ist ein Einblick in die aktuellen Geschehnisse eines Systems deutlich einfacher.

Insgesamt werden nun bei der WVV mehr als 40 heterogene Systeme mit sehr hohem Schutzbedarf einschließlich SAP eingebunden und überwacht - jederzeit erweiterbar um neue Anwendungen. Es können dort nun mögliche Angriffe erkannt und es kann proaktiv reagiert werden. Eventuelle Schäden durch Cyberangriffe können durch Präventivmaßnahmen oder frühzeitige Erkennung vermieden werden. Die BSI-Vorgaben zum Mindeststandard zur Protokollierung und Detektion von Cyber-Angriffen sind somit voll erfüllt.

Mit dem sicheren, in Echtzeit operierenden Meldesystem hat SVA die passende Lösung für die Anforderungen der WVV und im Rahmen KRITIS identifiziert und das Schutzniveau der Infrastruktur und des Rechenzentrums am Standort Würzburg wurde merklich erhöht. Innerhalb eines knappen Zeitfensters wurden alle Komponenten der SIEM-Struktur in einem problemlosen Projektdurchlauf von SVA implementiert und ganzheitlich in enger Zusammenarbeit mit der IT der WVV vor Ort gelöst.

KONTAKT
SVA System Vertrieb Alexander GmbH
Borsigstraße 26
65205 Wiesbaden
Tel. +49 6122 536-0
Fax +49 6122 536-399
mail@sva.de
www.sva.de