REFERENZ RHEINBAHN

CYBERRESILIENZ FÜR DEN ÖPNV DER ZUKUNFT

↳ SOC as a Service von SVA stärkt die Sicherheit kritischer Anlagen bei der Rheinbahn AG.

AUF EINEN BLICK

Aufgabe
24/7-Überwachung der IT- und OT-Infrastruktur zur Erkennung von Cyberangriffen und zur Absicherung kritischer Systeme im öffentlichen Personennahverkehr.

Systeme und Software
– SOC by SVA Basis-Modul
– Managed SIEM Analytics mit Splunk Enterprise Security
– Palo Alto Cortex XSOAR
– Proactive Incident Response Service
...

RHEINBAHN AG

Die Rheinbahn AG ist das bedeutendste kommunale Verkehrsunternehmen im Verkehrsverbund Rhein-Ruhr und zählt bundesweit zu den fünf größten Nahverkehrsbetrieben. Mit über 130 Linien, rund 1.700 Haltestellen und etwa 202 Millionen Fahrgästen pro Jahr verfolgt die Rheinbahn den Anspruch, Menschen und Orte miteinander zu verbinden. Als Betreiber kritischer Anlagen trägt sie eine besondere Verantwortung für die Verfügbarkeit, Sicherheit und Stabilität ihrer Systeme und Prozesse sowie für die Menschen, die den Nahverkehr in Düsseldorf und der Region nutzen.

HERAUSFORDERUNG

Als Betreiber kritischer Anlagen unterliegt die Rheinbahn AG hohen regulatorischen Anforderungen an die Informationssicherheit. Ihr Ziel war es daher, gesetzliche und normative Anforderungen gemäß §31 BSIG vollständig zu erfüllen und gleichzeitig die bestehende Sicherheitsüberwachung deutlich auszubauen. Dabei standen insbesondere die zuverlässige Erkennung von Angriffen auf die IT- und OT-Infrastruktur sowie die kontinuierliche Absicherung des öffentlichen Personennahverkehrs im Fokus.

...

Vorteile
- zentrale Erkennung und Korrelation sicherheitsrelevanter Ereignisse
- höhere Verfügbarkeit kritischer Betriebs- und Verkehrssysteme
- schnelle Reaktion auf Sicherheitsvorfälle durch 24x7 SOC-Betrieb
- Entlastung der internen IT-Teams durch standardisierte Prozesse
- Integration von IT- und OT-Systemen in eine zentrale Sicherheitsarchitektur
- DSGVO-konformer Betrieb und feste deutschsprachige Ansprechpartner
- zukunftssichere Plattform für den weiteren Ausbau der Sicherheitsüberwachung

Vor Projektbeginn existierten zwar bereits zahlreiche Protokoll- und Monitoring-Daten aus unterschiedlichen Systemen, jedoch fehlte eine zentrale Plattform zur Korrelation und Bewertung sicherheitsrelevanter Ereignisse. Die Auswertung erfolgte dezentral, anlassbezogen und ohne einheitliche Standards hinsichtlich des Inhalts und der Qualität der Log-Daten. Perspektivisch war dadurch eine frühzeitige Erkennung komplexer oder systemübergreifender Sicherheitsvorfälle nur eingeschränkt möglich.

Besondere Aufmerksamkeit verlangte dabei die Absicherung der betriebskritischen Systeme der Rheinbahn. Dazu zählen unter anderem Leitstellenkommunikation, Funkanlagen, die Steuerung von Bussen und Bahnen sowie Managementsysteme auf den Betriebshöfen. Zusätzlich sollten auch klassische IT-Systeme wie Active Directory, Firewalls und Netzwerkkomponenten in eine durchgängige 24/7-Überwachung integriert werden. Gleichzeitig musste eine Lösung gefunden werden, die standardisierte Prozesse etabliert, interne Ressourcen entlastet und die Reaktionsfähigkeit im Ernstfall nachhaltig verbessert.

LÖSUNG

Im Rahmen einer öffentlichen Ausschreibung entschied sich die Rheinbahn AG für das Proactive SOC by SVA. Ausschlaggebend waren der Status als sowohl wirtschaftlichste als auch technologisch ausgereifteste Lösung sowie die hohe fachliche Qualität des Servicekonzepts. Bereits in der Marktsondierung und im Vergabeverfahren überzeugte SVA mit umfangreicher Security-Expertise und Erfahrung in der Überwachung von OT-Systemen sowie einem ganzheitlichen Ansatz aus Security Monitoring und Incident Response.

Die implementierte Lösung basiert auf mehreren eng verzahnten Komponenten: Das SOC by SVA Basis-Modul bildet die technische und organisatorische Grundlage für die 24/7-Sicherheitsüberwachung. Sicherheitsrelevante Ereignisse werden zentral verarbeitet, analysiert, über die integrierte SOAR-Plattform *Palo Alto Cortex XSOAR* korreliert und mit Threat-Intelligence-Daten angereichert.

Ergänzend kommt das Security-Detection-Modul *Managed SIEM Analytics* auf Basis von *Splunk Enterprise Security* (ES) zum Einsatz. Diese SIEM-Plattform sammelt und analysiert Log-Daten aus IT- und OT-Systemen, erkennt bekannte Angriffsmuster und identifiziert Anomalien, die auf bisher unbekannte Bedrohungen hindeuten können. Durch bestehende Schnittstellen, beispielsweise zu OPC-UA, können perspektivisch weitere OT-Systeme, wie Steuerungssysteme zur Weichenstellung, integriert werden.

Ein weiterer zentraler Bestandteil ist der *Proactive Incident Response Service* von SVA. Dieser ermöglicht schnelle Unterstützung bei Sicherheitsvorfällen, sowohl remote als auch vor Ort, und ergänzt die Sicherheitsüberwachung durch strukturierte Krisenvorbereitung, Tabletop-Übungen und forensische Analysen. Besonders wertvoll für die Rheinbahn war dabei die enge Verzahnung von SOC- und Incident-Response-Leistungen aus einer Hand.

> Für die Rheinbahn war es wichtig, eine Lösung zu finden, die die hohen Anforderungen des §31 BSIG an uns als Betreiber kritischer Dienstleistungen erfüllt und unsere IT- und OT-Systeme lückenlos überwacht. Mit dem SOC by SVA haben wir eine zentrale Plattform, die regulatorische Sicherheit schafft und Angriffe auf kritische Anlagen frühzeitig erkennt. Die DSGVO-konforme Datenhaltung und feste Ansprechpartner im SOC-Team sind für uns unverzichtbar.

Yannick Beckmann,
Informationssicherheitsbeauftragter,
Rheinbahn AG

FAZIT

Mit dem SOC as a Service von SVA konnte die Rheinbahn AG ihre Cyberresilienz deutlich stärken und die Sicherheitsüberwachung ihrer kritischen Anlagen nachhaltig professionalisieren. Sicherheitsrelevante Ereignisse werden heute zentral korreliert, schneller erkannt und strukturiert bewertet. Dadurch lassen sich potenzielle Störungen frühzeitig behandeln, bevor sie Auswirkungen auf den Fahrbetrieb oder die Fahrgäste haben.

Gleichzeitig wurden klare Prozesse für Incident Management, Eskalation und Krisenkommunikation etabliert. Die Integration in bestehende Notfall- und BCM-Prozesse verbessert die organisatorische Resilienz zusätzlich und sorgt für höhere Prozesssicherheit im täglichen Betrieb.

Auch die internen IT-Teams profitieren erheblich von der neuen Lösung. Durch standardisierte Abläufe, klare Handlungsempfehlungen und eine zentrale Kommunikation über Ticketsysteme werden die Administratoren deutlich entlastet und können sich stärker auf Betrieb und Weiterentwicklung ihrer Systeme konzentrieren.

Die Lösung wird vollständig aus Deutschland betrieben, sämtliche Daten verbleiben im Kundennetzwerk und die Kommunikation erfolgt über feste Ansprechpartner im SVA SOC-Team. Dadurch konnte eine hochverfügbare, DSGVO-konforme Sicherheitsarchitektur geschaffen werden, die sowohl regulatorischen Anforderungen als auch den besonderen Betriebsanforderungen eines modernen Verkehrsunternehmens gerecht wird.

Die Zusammenarbeit mit SVA wurde von Beginn an als äußerst professionell und partnerschaftlich wahrgenommen. Besonders positiv bewertet die Rheinbahn feste Kontaktpersonen, die deutschsprachige Kommunikation sowie die Kombination aus SOC- und Incident-Response-Kompetenz. Darüber hinaus schafft die Plattform eine zukunftsfähige Basis für den weiteren Ausbau der Sicherheitsüberwachung. Perspektivisch sollen zusätzliche Systeme und weitere kritische Anlagen in die Sicherheitsarchitektur integriert werden.

Rheinbahn

KONTAKT

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