KUNDEN CASE STUDY

Sichere Mobilität für den Schienenverkehr

Für die Erfurter Bahn als KRITIS-Organisation steht IT-Sicherheit ganz oben auf der Tagesordnung. Die NIS-2-Richtlinie stellt spezifische Anforderungen an die Netzwerksicherheit. Sophos hilft mit seinem Cybersecurity-Ökosystem dabei, diese Herausforderungen zu stemmen und gleichzeitig ein effektives Management zu gewährleisten.

SOPHOS

ERFURTER BAHN

Erfurter Bahn GmbH

Industrie
Transport/Schienenverkehr

Nutzer
223

Sophos-Partner
IBYKUS AG

Sophos-Lösungen
Firewall
MDR
Endpoint Security
DNS Protection
Access Points
Managed Risk & Response

Die Erfurter Bahn steht seit über 100 Jahren für Mobilität, Verlässlichkeit und Fortschritt. Gegründet im Jahr 1912 als städtische Industriebahn, begann das Unternehmen mit Gütertransporten und entwickelte sich kontinuierlich weiter und expandierte 1998 im Schienenpersonennahverkehr. Heute bietet die Erfurter Bahn in vier Bundesländern einen effizienten, sicheren und pünktlichen Nahverkehr. Gemeinsam mit dem Tochterunternehmen Süd•Thüringen•Bahn beschäftigt sie rund 650 Mitarbeitende und setzt auf eine moderne Fahrzeugflotte, bestehend aus 97 Regio-Shuttle RS 1 der BR 650 und 6 LINT-Fahrzeuge der BR 648 sowie 2 Lokomotiven für den Güterverkehr.

„Dank Sophos konnten wir erfolgreich die Sicherheit eines 24/7-SOC-Supports durch Spezialisten im Hinblick auf die KRITIS-Vorgaben von NIS-2 zeitnah und unproblematisch realisieren."

Daniel Heider
CISO, Erfurter Bahn

Die Herausforderung

Das IT-Team der Erfurter Bahn sichert rund 200 Notebooks sowie 60 Server in einer auf VMware basierenden Virtualisierungsumgebung und setzt dabei auf eine große Bandbreite an VPN-Infrastruktur als Basis für die Fahrzeug-Server-Kommunikation. Zudem müssen verschiedene interne sowie externe Webserver-Anwendungen sowie Mobile-App-Kommunikation mit internen Systemen abgesichert werden.

Die zunehmende Gefahr durch moderne Cyberattacken machte eine Anpassung der IT-Sicherheit neben der NIS-2-Thematik noch einmal dringender. Im Fokus steht daher die Abbildung eines 24/7-SOC-Teams, das sich betriebswirtschaftlich sinnvoll realisieren lässt, sowie eine Verringerung des administrativen Aufwands, um mehr Zeit für die Kernaufgaben zur Verfügung zu haben.

Die Lösung

Da die Erfurter Bahn in Kooperation mit dem IT-Partner Ibykus bereits seit vielen Jahren auf Sophos-Lösungen zum Schutz seiner Endpoints und Netzwerke setzt, wurde auch der Wechsel von traditionellen IT-Sicherheitsarchitekturen hin zu modernen SaaS-Strategien zusammen mit dem Cybersecurity-Spezialisten vorgenommen. Ein weiteres Entscheidungskriterium waren die regelmäßig guten Bewertungen durch Marktforschungsunternehmen sowie positive Testberichte und Experten-Meinungen.

Eine detaillierte Schwachstellenanalyse sowie die Vorgaben der NIS-2-Richtlinie machten schnell klar, dass neben der bestehenden Cybersecurity-Infrastruktur vor allem das Thema Managed Detection & Response zur bestmöglichen Absicherung eines komplexen und hochverfügbaren Netzwerks vorangetrieben werden musste.

Das globale Cybersecurity-Expertenteam von Sophos sorgt rund um die Uhr für die Überwachung der Unternehmensumgebung. Zudem gewährleistet die Integration von Sophos Managed Risk & Response in die existierende Nessus-Lösung vom Sophos-Kooperationspartner Tenable zusätzliche Sicherheit.

Um der Bedrohungslage auch zukünftig gewachsen zu sein und Endgeräte im Bereich IoT und OT besser überwachen zu können, testet das IT-Team der Erfurter Bahn zurzeit Sophos NDR, um gegebenenfalls 2026 eine Erweiterung des MDR-Services mit NDR zu realisieren.

Das Ergebnis

Die Erfurter Bahn profitiert seit der Einführung der MDR-Services stark von der automatisierten Überwachung und Bewertung verschiedener Bedrohungen sowie der Möglichkeit, auf sehr kurzem Weg auf ein Experten-Team zugreifen zu können. So ist das IT-Sicherheitsteam in der Lage, sehr schnell eine Bewertung verdächtiger Log-Einträge oder Alarme im eigenen SIEM erhalten zu können.

Die Managed-Service-Erweiterung ermöglicht es zudem, die Vorgaben der Geschäftsführung im Hinblick auf NIS-2 mit einem 24/7-SOC-Supports durch Spezialisten zu erfüllen und zusätzlich finanziell positive Auswirkungen auf die bestehende Cybersecurity-Versicherung zu generieren.

Last but not least bietet die gesamtheitliche Lösung von Sophos aus administrativer Sicht den großen Vorteil der Verwaltung aller Tools über die Central-Plattform. Aufgrund des zentralen Managements der neuen Gesamtlösung, bei der Endpoint- und Netzwerkschutz Hand in Hand arbeiten, konnte die angestrebte Entlastung der IT-Abteilung nachhaltig durchgesetzt und gleichzeitig eine enorm verbesserte Flexibilität bei gleichzeitiger Erhöhung des Schutzes vor modernen Cyberattacken umgesetzt werden. Bei erfolgreichen Tests ist eine zusätzliche Erweiterung mit Sophos Mobile im Bereich Mobile Device Management vorgesehen.

„IT-Sicherheit ist ein dynamischer Prozess, auf den wir mit dem übergreifenden Sophos-Ökosystem inklusive Managed Services schnell und effektiv reagieren können."

Daniel Heider
CISO, Erfurter Bahn

Der Partner

IBYKUS

IBYKUS AG

1990 in Thüringen gegründet, unterhält die IBYKUS AG mit Hauptsitz in Erfurt heute insgesamt sechs Standorte in Deutschland. Bundesweit arbeitet das Unternehmen mit über 370 Mitarbeitenden daran, sowohl Unternehmen als auch die öffentliche Verwaltung mit verschiedensten Softwarelösungen und intelligenten Technologien einfacher, sicherer und digitaler zu gestalten.

Das Leistungsspektrum reicht von umfassenden E-Government-Lösungen für die Verwaltung europäischer, nationaler und kommunaler Fördermittel bis hin zu innovativen Lösungen zur Prozessdigitalisierung für Unternehmen und Behörden. Die Entwicklung mobiler Anwendungen, IT-Security, IT-Infrastruktur sowie der zuverlässige Betrieb von Lösungen in eigenen BSI-zertifizierten Rechenzentren in Deutschland und eine professionelle Beratung runden das Portfolio ab.

Mehr Informationen unter www.sophos.de

2026-01-26 CCS-DE (NP) CRE-4436

SOPHOS