Sicherheits-Fundament für die Zukunft

DB Netz AG: Security Consulting zu ESARIS schafft Effizienz und Transparenz

Referenzprojekt:

DB NETZE

„Die Anwendung von Bausteinen der Sicherheitsarchitektur ESARIS hilft, eine moderne Basis für ein operatives IT-Sicherheitsmanagement zu schaffen. Der Kunde erzielt damit unternehmensweit Effizienz und Transparenz."

Dr. Eberhard von Faber, T-Systems

Das größte nationale Schienennetz in Europa managen die über 50.000 Mitarbeiter der DB Netz AG für ihre Kunden und deren Fahrgäste. Denn nicht nur die Deutsche Bahn profitiert von den Leistungen ihrer Tochter, sondern über weitere 400 Eisenbahnverkehrsunternehmen.

Neben Streckenneubauten und der Instandhaltung des Streckennetzes erstellt die DB Netz AG u.a. die Fahrpläne für den operativen Betrieb. Für reibungslose Betriebsabläufe in dieser Größenordnung – täglich nutzen ca. 23.500 Züge die Netz-Infrastruktur und erzeugen so während eines Jahres über eine Milliarde Trassenkilometer – spielt IT eine entscheidende Rolle. Sie dient nicht nur dazu, Signale, Bahnübergänge und Weichen korrekt zu stellen, sondern unterstützt auch in der Koordination des kompletten Bahnverkehrs in Deutschland.

Die DB Netz AG ist in ihrer Funktion ein KRITIS-Unternehmen par excellence – sie sorgt dafür, dass eine einzigartige kritische Infrastruktur in Deutschland dauerhaft verfügbar bleibt. Als KRITIS-Unternehmen liegt die Messlatte für die IT-Sicherheit besonders hoch. Dokumentation und Erfüllungsgrad von Sicherheitsvorgaben sind ein wichtiger Aspekt für das Geschäft der DB Netz AG.

Auf einen Blick

- Drastisch steigende Aufwände für Audits (z.B. KRITIS)
- Ablösung manuell-reaktiver Abläufe für IT Security Management
- Verbesserung der Effizienz
- Nachhaltige Verankerung im Unternehmen
- Security Consulting T-Systems/Deutsche Telekom Security
- Nutzung der ESARIS-Sicherheitsarchitektur
- Entwicklung einer spezifischen Sicherheitstaxonomie
- Entwicklung eines modernen, effizienten IT-Sicherheitsmanagements inklusive Governance
- Zentrale Orchestrierung der IT-Sicherheitsdokumentation
- Kontinuierliche Transparenz
- Entlastung des Security-Teams

T Systems

Let's power higher performance

Die Referenz im Detail

Herausforderung

Die KRITIS-Anforderungen an die DB Netz AG sind nicht neu. Doch in den letzten Jahren hat sich eine zunehmende Fülle von Standards, Anforderungslisten, Arbeitsanleitungen und Security-Konzepten entwickelt, deren Etablierung und Erfüllung Auditoren prüfen. Diese Inhalte und Mitwirkungsleistungen sind über das ganze Unternehmen und seine speziellen Einheiten verteilt. Damit verbinden sich immense Aufwände für das schmal aufgestellte IT-Security-Team des Unternehmens. Um die KRITIS-Anforderungen, aber auch andere Sicherheitsstandards und Zertifizierungen, bedienen zu können, entschloss sich das Team, sein existierendes Managementsystem für Informationssicherheit (ISMS) auf den Prüfstand zu stellen. „Wir wollten umfassende Transparenz erzeugen über die notwendigen Informationen und gleichzeitig eine effiziente Umsetzung des ISMS sicherstellen“, erläutert Dr. Eberhard von Faber von T-Systems. Das Sicherheitsteam wollte eine moderne Basis für das IT-Sicherheitsmanagement legen und im Unternehmen verankern. Denn eine Fülle interner Einheiten muss dauerhaft daran aktiv mitwirken. Wie kann das gelingen?

Lösung

Mit ESARIS (Enterprise Security Architecture for Reliable ICT Services) entdeckten die Verantwortlichen eine passende Sicherheitsarchitektur, um die IT-Sicherheit grundlegend aufzuarbeiten und auf neue Füße zu stellen. Sie wandten sich an T-Systems/Deutsche Telekom Security, um Beratungsleistungen zu erhalten.

ESARIS ist eine Sammlung von Maßnahmen, Standards und Anleitungen zur Absicherung von ICT-Services. ESARIS standardisiert, harmonisiert und verbessert die IT-Sicherheit. ESARIS wurde primär für IT Service Provider entwickelt, bei denen eine hochgradig verteilte Wertschöpfung an der Tagesordnung steht. Dies ist auch bei der DB Netz AG der Fall. Entsprechend können viele Bausteine der Sicherheitsarchitektur ESARIS genutzt werden. Das demonstrierten T-Systems und Deutsche Telekom Security im Rahmen eines mehrmonatigen Beratungsprojektes im Jahr 2021.

In Zusammenarbeit mit den Fachleuten analysierten sie die existierende Situation bzgl. genutzter Werkzeuge, Informationsquellen, vorhandener Dokumentationen etc. Sie spiegelten die Ergebnisse der Analyse an den vorhandenen Blaupausen der ESARIS-Sicherheitsarchitektur. Dabei stellte sich heraus, dass nicht nur originäre IT-Sicherheitsthemen der Enterprise-IT berücksichtigt werden müssen, sondern auch der zunehmend wichtigere Bereich der OT- bzw. IIoT-Sicherheit.

Auf dieser Basis entwickelten die Berater mit dem Sicherheitsteam eine unternehmensspezifische Sicherheits-Taxonomie. Sie legt detailliert dar, welche Themen und Aufgaben bearbeitet werden müssen und wie sie in Verbindung miteinander stehen. Die Taxonomie ermöglicht, einen dauerhaften Überblick zu gewinnen und dient als Steuerungsinstrument. Mit diesem zentralen Werkzeug können die IT-Sicherheitsverantwortlichen der DB Netz AG ihr IT-Security Management effizient orchestrieren. Sie gewinnen eine solide Basis und einen Plan für die nächsten Umsetzungsschritte. Darüber hinaus spielt ein zentrales Dokumentenmanagement eine wichtige Rolle, dessen Grundpfeiler gemeinsam erörtert wurden. Ein Zusammenarbeitsmodell definiert die Mitwirkungsleistungen, hilft, die Zusammenarbeit zu organisieren, und schafft die Grundlage für die Governance innerhalb des Unternehmens.

Kundennutzen

Mit der neuen Basis für das Management der Informationssicherheit kommt die DB Netz AG von einem reaktiven, manuellen Modus in einen geplant-aktiven. Es gelingt ihr die notwendigen Informationen und Mitwirkungsleistungen effizient zu orchestrieren. An die Stelle der aufwändigen reaktiven wiederkehrenden Rechercheaufgaben (z.B. für anstehende Audits) tritt ein systematischer, industrialisierter Ansatz für die Informationssicherheit. Die DB Netz AG wird in die Lage versetzt, eine strukturierte IT-Sicherheitsdokumentation als Vorgabe für die Einheiten im Konzern, als Nachweis der Einhaltung und als Werkzeug für ein umfassendes Sicherheitsmanagement aufzubauen. Das Unternehmen gewinnt ein hohes Maß an Transparenz zu jeder Zeit und verankert die Bedeutung der IT-Sicherheit auch auf der Ebene der Geschäftsführung. IT-Security-Management wird so auch im umfangreichen und schnelllebigen Geschäft sowie in komplexer werdenden Rahmenbedingungen und Regularien beherrschbar. „Silos“ werden aufgelöst, ein unternehmensweiter Blick entsteht.

Weitere Vorteile:

- Zentrale Orchestrierung mit schmalem IT-Security Management Team
- Einfachere Auditierung, geringere Aufwände
- Gestärkte interne Positionierung des Security-Teams
- Sensibilisierung des Mitarbeiterstamms für IT-Sicherheit

Kontakt
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Deutschland
E-Mail: referenzen@t-systems.com
Internet: www.t-systems.com

Herausgeber
T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main
Deutschland

Letzte Änderung : 06/2022 | Konzipiert durch: Creative Factory, TSIN