A security basis for the future

DB Netz AG: Security consulting with ESARIS creates efficiency and transparency

Reference project:

DB NETZE

“Using modules from the ESARIS security architecture helps to provide a modern basis for the operational IT security management. The client achieves company-wide efficiency and transparency.”

Dr. Eberhard von Faber, T-Systems

More than 50,000 employees from DB Netz AG manage Europe’s largest national rail network for their customers and passengers. Not only does Deutsche Bahn profit from its subsidiary’s services, it benefits more than 400 other rail travel companies too.

In addition to building new rail lines and maintaining the rail network, DB Netz AG’s tasks include drawing up the train schedules for operations. IT plays a crucial role in ensuring seam-less operational processes at this kind of scale – around 23,500 trains use the network infrastructure every day and cover more than a billion path kilometers over the course of a year. The IT not only serves to operate signals, level crossings, and track switches correctly, it also helps coordinate all of the rail traffic in Germany.

In its capacity as a company in a critical infrastructure sector, DB Netz AG is outstanding – it ensures that unique critical infrastructure in Germany remains permanently available. When it comes to IT security, the bar is especially high for companies in critical infrastructure sectors. The documentation and degree of fulfill-ment for security requirements are an important aspect of DB Netz AG’s business.

At a glance

- Dramatic increase in effort required for audits (e.g., critical infrastructure sectors)
- Replacement of manual, reactionary workflows for IT security management
- Increased efficiency
- Systems sustainably embedded within the company
- Security Consulting at T-Systems/Deutsche Telekom Security
- Use of the ESARIS security architecture
- Development of a specific security taxonomy
- Development of a modern, efficient IT security management system, including governance
- Centralized orchestration of IT security documentation
- Continual transparency
- Burden on the security team eased

T Systems

Let’s power higher performance

Reference in detail

The challenge

The requirements to be fulfilled by DB Netz AG within the critical infrastructure sector are not new. However, an increasing array of standards, lists of requirements, work instructions, and security concepts have been developed over the past years, and auditors check for their establishment and fulfillment. These contents and obligations are distributed across the entire company and its specialized units. This requires a huge amount of time and effort for the company's streamlined IT team. In order to meet the requirements for critical infrastructure sectors as well as other security standards and certifications, the team decided to review its existing information security management system (ISMS). "We wanted to create full transparency concerning the information needed and simultaneously guarantee the efficient implementa-tion of the ISMS," explains Dr. Eberhard von Faber, T-Systems. The security team wanted to create a modern foundation for IT security management and embed this within the company since there is a plethora of internal units who must be actively involved at all times. How could this be achieved?

The solution

With ESARIS (ESARIS: Enterprise Security Architecture for Reliable ICT Services), the team found themselves a suitable security architecture which they could use to fundamentally rework their IT security and give it a whole new foundation. They turned to T-Systems/Deutsche Telekom Security for advice.

ESARIS is a collection of measures, standards, and instructions for securing ICT services. ESARIS standardizes, harmonizes, and improves IT security. ESARIS was primarily developed for IT service providers whose business involves a highly distributed value creation. This is also the case at DB Netz AG, so many of the building blocks of the ESARIS security architecture can be used accordingly. This was demonstrated by T-Systems and Deutsche Telekom Security as part of a consultation project lasting several months in 2021.

In collaboration with the experts, they analyzed the existing situation with regard to the tools used, sources of information, documentation available, etc. The results of the analyses were then reflected in the existing blueprints of the ESARIS security architecture. This highlighted the fact that not only do original IT security issues associated with enterprise IT needed to be accounted for, but also the increasingly important area of OT/IIOT security.

Using this as a basis, the consultants developed a security taxonomy tailored to the company, together with the security team. It shows in detail the issues and tasks that need to be processed and how they are interconnected. The taxonomy makes it possible to gain a permanent overview and serves as a monitoring tool. This centralized tool allows the IT security team at DB Netz AG to orchestrate its IT security management efficiently. They gain a solid foundation and a plan for the next steps in its implementation. Centralized document management also plays an important role, so its key pillars were discussed jointly by the teams. A collaboration model is used to define the obligations, helps organize the collaboration, and creates the basis for governance within the company.

Customer benefits

With this new foundation for information security management, DB Netz AG is moving away from reactive, manual methods to a planned, active approach. It has managed to orchestrate the necessary information and obligations efficiently. Recurring time-consuming, reactive research tasks (e.g., for upcoming audits) have been replaced by a systematic, industrialized approach to information security. DB Netz AG has been enabled to set up structured IT security documentation as a requirement for units within the group as proof of compliance and as a tool for end-to-end security management.

The company has a high level of transparency and has entrenched the importance of IT security within the company, even at the management level. The IT security management is even manageable in extensive, fast-paced business as well as with increasingly complex framework conditions and regulations. "Silos" have been broken up, and a company-wide view has emerged.

Further advantages:

- Centralized orchestration with a streamlined IT security management team
- Easier auditing with less time and effort required
- Internal position of the security team strengthened
- Greater awareness of IT security throughout the entire workforce

Contact
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
Email: referenzen@t-systems.com
Internet: www.t-systems.com

Published by
T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main
Germany

Last update: 08/2022 | Designed by: Creative Factory, TSIN