SBB CFF FFS

SBB uses standardised security services to protect its central rail communication platform

Swiss Federal Railways, or SBB for short, operates with a punctuality of over 95 per cent. This high level of reliability is only possible thanks to secure and fast communication between the control centres and staff working in stations, trains and on the tracks.

The operational communication environment has been continuously expanded and modernised over the course of almost 20 years of cooperation with Frequentis. During this time, IT threat scenarios and the resulting security requirements have also changed fundamentally. Alongside rail transport security, the topic of security, cyber security in particular, is today of significantly greater importance for maintaining smooth operation.

To meet the various challenges in the area of cyber security, the joint team of SBB and Frequentis used a standardised security service catalogue from Frequentis to clearly define the responsibilities for systems, components and the associated processes. This ensures that SBB is optimally positioned to address current security risks in the area of rail communications through effective hazard management.

Customer profile

Swiss Federal Railways is a railway company with over 33,500 employees. Every day, SBB transports around one million passengers and 185,000 tons of goods across its 3,265 km network.

Initial situation

The topic of IT security is becoming increasingly important for providing seamless customer service across all industries and areas of business. Although the communication solutions implemented at SBB's control centre have been continuously expanded and modernised over many years, IT security requirements have also increased at the same time.

Solution

To counter the ever-increasing number of cyber threats, SBB uses a comprehensive security services catalogue from Frequentis to provide even more effective protection of its central operational communication infrastructure, which has continued to grow over many years.

Results

- 28 security services are now used to define and document processes, responsibilities and measures for rail communication
- Protects 2,200 users and 650 end devices from cyber threats
- Provides customised security monitoring and proactive security management
- Supports more efficient implementation of internal and external security requirements

> "The joint development and implementation of security services for our operational communication asset has enabled SBB to further deepen its collaboration with Frequentis."
>
> Zachäus Arnold, Swiss Federal Railways SBB

Faster identification of risks and a reduction of operational risk

Efficient communication thanks to robust infrastructure

Digitalisation is a cornerstone of SBB's innovation strategy. The company uses secure digital networking to further improve its outstanding customer service, which currently boasts over 95 per cent punctuality.

To achieve this level of service, SBB relies on operational railway communication with a Frequentis solution at its core. Using this solution, SBB ensures that control centre employees are able to quickly and safely coordinate operations with the train drivers, the service personnel on the trains and (maintenance) teams out on the track.

The increasing digitalisation of voice communication is placing increasing demands on the network infrastructure, which puts cyber security requirements in the foreground.

Focus on cyber security with standardised security services

Owing to the much-publicised ransomware attacks of late, SBB and Frequentis have placed an even greater focus on the topic of cyber security. The cross-company team analysed the overall situation and developed a flexible security strategy.

SBB uses Frequentis' standardised security service catalogue to systematically assess risks and coordinate appropriate measures. From the available 28 security services, which enable rapid and agile adaptation to dynamically changing security requirements, SBB selected the specific services that supplement existing cyber security at the company. This makes the topic a central element of SBB's trusting and forward-looking cooperation with Frequentis.

Improved security and transparency

Through the security service catalogue, SBB benefits from better protection against security threats. Working together, the team of specialists from SBB and Frequentis drew up a detailed description of tasks in the areas of prevention, intrusion and security monitoring, information security management systems, security risk management and requirements management, based on which they created a cross-company responsibility matrix. This process transparency enabled SBB to safeguard and optimise its capacity to act.

During implementation, the standardised security services were tailored to SBB's requirements. The package includes central security monitoring with intrusion detection and the proactive early detection of threats. This allows unauthorised access attempts to be detected and managed in real time. A flexible configuration with customer-specific thresholds enables intelligent, automated responses to suspicious activity.

For prevention purposes, the Frequentis Security Incident Response Team (SIRT) provides comprehensive information on security threats to the technology stack used and, if necessary, works together with SBB to devise measures to minimise operational risk. This information and the associated processes enable SBB to react more quickly to changing cyber security requirements.

Thanks to Frequentis Security Services, SBB is able to further improve the quality and availability of rail communication systems and optimise operational processes in the area of cyber security. The services currently protect 2,200 users and 650 end devices more effectively against attacks and other threats.

FREQUENTIS AG
Innovationsstraße 1
1100 Vienna, Austria
Tel: +43-1-811 50-0
www.frequentis.com

The information in this publication is for general information purposes only. The technical specifications and requirements are valid at the time of first publication. Typing and printing errors reserved. The liability and warranty of Frequentis for the publication are excluded. All rights reserved. Information from this publication may not be used without the express consent of Frequentis.