UNITED
SECURITY
PROVIDERS

NETZWERKPERIMETER-SCHUTZ UND INVEN-TARDATENQUALITÄT

SWISS FEDERAL RAILWAY

SUCESS STORY

Auslöser für die Massnahmen zum höheren Netzwerkschutz waren Vorfälle, die den produktiven Betrieb beeinträchtigten. Diese waren entweder auf Virenbefall oder fehlerhafte Netzwerkzugriffe zurückzuführen. Beim Vorhaben, das unter den Oberbegriff «Network Access Control» (NAC) fällt, bestanden seitens der Auftraggeberin Telecom SBB klare Vorgaben.

MARC PAULI
PLATTFORMMANAGER
DATA & SECURITY
TELECOM SBB

AUSGANGSLAGE

Grundsätzlich ging es bei dem Grossprojekt um die Einführung eines Netzwerk-Authentifizierungssystems für über 30'000 nicht bahnsteuerungstechnische (d. h. keine Leitsysteme, Gleisanlagen etc.), über die ganze Schweiz verteilte Endgeräte. Mit dem System sollte der unerlaubte Anschluss von unbekannten Endgeräten an das IP-Datennetz der SBB erkannt und verhindert werden. Eine weitere Erwartung an die NAS-Applikation war die Verbesserung der Inventardatenqualität der am SBB-Netzwerk angeschlossenen Endgeräte.

Als Lösung wählten die SBB das USP Network Authentication System® (NAS) von United Security Providers.

> **Marc Pauli: «Ein Projekt dieser Grössenordnung muss intern breit abgestützt sein.»**

DIE UMSETZUNG

Das NAC-Projekt der SBB Telecom gliederte sich in zwei Phasen: In einem ersten Schritt, der Systembauphase, wurde die Applikationsinfrastruktur (NAS-Serverplattform, Applikationsentwicklung und Schnittstellen zu den Umsystemen) aufgebaut. In dieser Phase liessen sich die Endgeräte bereits identifizieren, aber noch nicht autorisieren.

Phase zwei stand im Zeichen der Definition und Einführung der Inventarisierungsprozesse für die Erfassung und Pflege der Endsystem-MAC-Adressen. Auf der Basis der so gewonnenen Inventare konnten die identifizierten Endgeräte auch autorisiert werden. Die nach Lokationen gestaffelte Umschaltung der Applikation vom «ALLOWED» in den «RESTRICTIVE»-Mode erfolgte im Rahmen eines Pilotprojekts.

DER KUNDENNUTZEN

Die Ziele «mehr Sicherheit», mehr Transparenz» und «hohe Qualität der Inventardaten» wurden eindeutig erreicht.

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

swiss made software

Mit NAS verfügt die SBB nun über ein System zum Schutz des Netzwerkperimeters, das den Vorgaben des IT-Security-Frameworks entspricht. Das Netzwerk-Authentifizierungssystem beugt Virenvorfällen, unberechtigtem Zugriff und Netzwerkausfällen vor – bei gegenwärtig rund 25'000 Endgeräten.

Ferner liefert es ein vollständiges Bild über die Anzahl, Art und den geografischen Ort der am Netzwerk angeschlossenen Geräte sowie die damit verbundenen Veränderungen im Zeitverlauf. Diese exakten Informationen erfüllen nicht nur ihre Aufgabe beim Zugriffsschutz, sondern dienen auch der Aktualisierung und Instandhaltung der Geräteinventardaten.

Neben dem aussagekräftigen Reporting und einer praktischen Verrechnungsbasis pro Netzwerk-Port ergab sich als weiterer Nutzen eine Prozessbereinigung, die sich zum Beispiel in klaren Abläufen bei Neuanschlüssen äussert.

INTERVIEW

AUS WELCHEN BEDÜRFNISSEN HERAUS WURDE DAS PROJEKT FÜR DAS NETZWERK-AUTHENTIFIZIERUNGSSYSTEM GEBOREN?

Der Druck kam ursprünglich aus der Ecke Netzwerksicherheit. Viren und fehlerhafte Zugriffe hatten verschiedentlich den produktiven Betrieb behindert. Entsprechend wurden neue Sicherheitsvorgaben entwickelt. Um dem gerecht zu werden, musste ein umfassendes Netzwerk-Authentifizierungssystem eingeführt werden.

> **Marc Pauli: «Schützen ja, aber nicht auf Kosten der Verfügbarkeit. Sicherheit darf den Nutzen nicht untergraben. Pragmatisches Vorgehen ist gefragt.»**

Das Ganze war eine vielschichtige Herausforderung, ja ein eigentlicher Balanceakt – was nicht weiter überrascht, wenn wir von heute rund 25'000 Endgeräten reden! Wir mussten von Anfang an in die Breite gehen. Gleichzeitig ging es darum zu schützen, aber nicht zu verhindern. Security soll kein reiner Selbstzweck sein, sondern fungiert auch als Enabler. Der Nutzen, das heisst die Verfügbarkeit, darf nicht unter der Sicherheit leiden. Die Kunst dabei ist also ein Sowohl-als-auch. Das geht nur, wenn das ganze Projekt intern auf breiter Front unterstützt wird.

WURDEN DIE ZIELE IN DER ZUSAMMENARBEIT MIT UNITED SECURITY PROVIDERS ERREICHT?

Die Forderungen nach Sicherheit, Transparenz und Inventardatenqualität wurden erfolgreich umgesetzt. Die Zusammenarbeit mit United Security Providers hat sich auf der ganzen Linie bewährt. Heute sind wir komplett im Bild darüber, wie viele Endgeräte am SBB-Netzwerk angeschlossen sind beziehungsweise um welche Art Endgerät es sich handelt. Auch wissen wir Bescheid über die Veränderungen der am Netz angeschlossenen Geräte im Zeitverlauf.

Wie so oft kommt auch hier der Appetit beim Essen. Die Anforderungen an ein flexibles Reporting steigen. Wir sind zuversichtlich, nicht nur zukünftigen Ansprüchen gerecht zu werden, sondern auch die Netzwerkbereitstellungsprozesse weiter zu straffen.

UNITED SECURITY PROVIDERS

ZERO TRUST UNIVERSE

Besuchsadressen
Hauptsitz | Stauffacherstrasse 65/15, 3014 Bern
Baslerpark | Baslerstrasse 60, 8048 Zürich

+41 31 959 02 02
info@united-security-providers.ch
united-security-providers.ch