



CASE STORY

Marc Pauli, Swiss Federal Railways (SBB)



Network perimeter protection and inventory data quality

Initial situation.

The measures to increase network protection were triggered by incidents that had a detrimental effect on live operations. These incidents were due to either virus attacks or incorrect network access.

In a project encompassing network access control (NAC) the client, Telecom SBB, provided clear specifications. This major project basically entailed the implementation of a network authentication system (NAS) for more than 20,000 devices spread across the whole of Switzerland that are not used for railway control (i.e. no control systems, tracks, etc.). The system was expected to recognise and prevent the unauthorised connection of unknown devices to the SBB's IP data network.

Another function that the NAS application was expected to perform was to improve the inventory data quality of devices connected to the SBB network.

Implementation.

The NAC project at SBB Telecom was divided into two phases. The first step, the system building phase, involved setting up the application infrastructure (NAS server platform, application development and interfaces to external systems). In this phase devices could be identified, but not yet authorised.

Phase two revolved around defining and implementing inventory processes for the purpose of recording and updating end-system MAC addresses. Using the inventories obtained in this way, it was possible to authorize the identified devices. The application changeover from «ALLOWED» to «RESTRICTIVE» mode, implemented location by location, took place as part of a pilot project.

Customer benefits.

The goals of «more security», «more transparency» and «high inventory data quality» were clearly achieved. With NAS, SBB now has a system to protect the network perimeter that meets the requirements stipulated by the IT Security Framework. The network authentication system currently prevents virus attacks, unauthorised access and network failures on around 25,000 devices.

In addition, it provides a full picture of the number and type of devices connected to the network, the geographical location of these devices and the associated changes over the course of time. This precise information not only plays its part in access protection, but is also used to update and maintain device inventory data. Alongside powerful reporting and a practical cost allocation basis per network port, another benefit is a process cleanup, which is reflected, for example, in clear processes for new connections.

MARC PAULI «A project of this magnitude requires extensive internal support.»

Interview with Marc Pauli, Plattform Manager Data & Security, Telecom SBB



Question: *What were the requirements that gave rise to the project for the network authentication system?*

M. Pauli: To begin with, the pressure came from the area of network security. Viruses and incorrect access had hindered live operations on various occasions. Bearing this in mind, new security standards were developed – and an extensive network authentication system had to be implemented in order to comply with these standards. The whole undertaking was a complex challenge – a real balancing act, in fact. However, this isn't particularly surprising when you consider that there are now 25,000 devices involved! We had to work on a broad basis right from the start. At the same time, we needed to provide users with protection without hindering their work. Security shouldn't be simply an end in itself, but should also act as an enabler. Security must not have a detrimental effect on benefits, that is to say availability. The trick is therefore to achieve both goals at once – something that is only possible if the project receives broad internal support.

Question: *Were the goals of collaboration with United Security Providers achieved?*

M. Pauli: The demands for security, transparency and inventory data quality were successfully met. The collaboration with United Security Providers proved to be worthwhile in all aspects. We now have a full overview of the number of devices connected to the SBB network as well as the types of device involved. We are also able to track changes made over the course of time to the devices connected to the network. As is so often the case, the appetite comes with eating. The requirements placed on flexible reporting are increasing. We are confident of not only meeting future demands, but also further streamlining network provision processes.

MARC PAULI «**Protection is good, but not at the expense of availability. Security must not undermine benefits. A pragmatic approach is needed.**»



UNITED SECURITY PROVIDERS