HOW INFORMATION SECURITY CAN BE ENSURED IN TUNNEL SYSTEMS

Gerhard Hudecek
ASFINAG Maut Service GmbH, AT

DOI 10.3217/978-3-85125-996-4-41 (CC BY-NC 4.0)

ABSTRACT

Based on Directive (EU) 2016/1148 of the European Parliament, the European Cyber Security Strategy [1] was transposed into Austrian law (NIS Act) at the end of 2018. The aim was to ensure a high level of security of network and information systems. The requirement was to take appropriate and proportionate technical and organisational security precautions and to report security incidents.

ASFINAG, as the Austrian motorway operator, was identified as the operator of elementary services by notice dated 12.11.2019. One of these essential services is tunnel control. By 11.11.2022, proof of NIS conformity had to be provided to a so-called qualified body.

A tunnel system is now equipped with a large number of IT and OT systems and components. These are connected with each other and connected to remote monitoring centres for control and monitoring. This creates a multitude of potential security risks, which can lead to an impairment of the function of safety equipment and to a reduction in the availability of the tunnel.

Until the establishment of the NIS Act (NIS-G) [2], ASFINAG very successfully pursued the strategy "never touch a running system". I.e. it was well planned, well built and well maintained. Software changes were avoided as far as possible. In order to comply with the NIS-G, this strategy had to be completely changed to "keep the system up-2-date", which means very frequent software changes. ASFINAG currently operates 167 tunnel systems, so the NISFIT © programme was developed on how to make these systems "cybersecure". In order to achieve a sufficient level of information security, the following key points must be addressed: A seamless IT asset management in order to know where which systems and components are installed and in operation, as well as to be able to assess potential risks.

Another important element is physical security on site as well as remote access management. Only those persons who are authorised to do so should be allowed secure access. Thirdly, active monitoring of the systems, including regular virus scans and penetration tests, is required. To make all this possible, as well as the requirement to report security incidents within the specified time, a Security Operation Centre (SOC) has been implemented.

In the end, ASFINAG succeeded in proving to the auditing authority in due time that all necessary measures for network and information system security (NIS) had been implemented.

Keywords: Information Security, Cybersecurity.

1. INTRODUCTION

Apart from artificial intelligence, there is hardly any other topic in information technology that is more prominent in the media of all kinds than information security, also often referred to as cybersecurity. The reason for this is the rapid progress of digitalisation, which affects all

areas of life, especially the economy in all its sectors. Every use of hardware and software increases the risk of external attacks, while digitalisation leads to increasing networking, which increases the variety of attack vectors. Attack vectors include phishing emails, malware infections, vulnerabilities in software that enable malware to be executed, but also insecure networks that allow attackers to penetrate hardware and software or spy on data traffic - a colourful bouquet of possibilities.

Cybersecurity affects every system. Pure IT systems - there are constant reports of successful attacks on companies and authorities that have been affected by successfully introduced ransomware with fully encrypted and therefore no longer usable data. But also, OT systems - probably the most famous case is the successful attack on the Iranian nuclear programme back in 2010. Stuxnet was specially developed to attack a monitoring and control system (SCADA system) that uses Siemens Simatic S7 programmable logic controllers.

It is clear from this that all systems that support our lives and processes are potential targets, regardless of the technology used. Such systems are also referred to as critical infrastructure and as such also affect road transport facilities as a whole and tunnels in particular.

2. CRITICAL INFRASTRUCTURE – ESSENTIAL SERVICES

The European Union has defined a cybersecurity strategy based on Directive (EU) 2016/1148 of the European Parliament. The aim was to ensure a high level of security of network and information systems. The requirement is to take appropriate and proportionate technical and organisational security precautions and to report security incidents. At the end of 2018, this directive was also transposed into Austrian law, the so-called NIS Act. As NIS2 is now specifically dealt with, we refer to it here as NIS1.

The Austrian authorities had to determine who is an operator of essential services in Austria and which critical infrastructure is declared as an essential service. Sectors were defined that must achieve a high level of security for network and information systems. These include:

- Energy
- Banking
- Financial market infrastructure
- Health sector
- Drinking water supply and distribution
- Digital infrastructure
- and transport!

In November 2019, ASFINAG, as the operator of all Austrian motorways and highways, was therefore sent a notice in which the following two essential services were defined as particularly worthy of protection:

- Traffic control on highways
- Traffic control in tunnels!

ASFINAG now had 36 months from receipt of the notice to prove that these two essential services meet the high cyber security requirements. The fulfilment of these requirements was checked by an auditor, a so-called qualified body. The fact that 36 months is very short can be explained by the fact that the authority assumed that these services would be operated with

appropriate security precautions anyway and that 36 months is therefore sufficient to provide evidence.

This review of the suitability of the security measures in place was divided into four areas and eleven categories:

Table 1: Categories if security

#	Area	#	Category
A	Governance and ecosystem	1	Governance and Risk management
		2	Dealing with service providers, suppliers and third parties
B	Protection	3	Security Architecture
		4	System Administration
		5	Identity and Access Management
		6	System Maintenance and Operation
		7	Physical Security
C	Defence	8	Incident Detection
		9	Incident Management
D	Resilience	10	Business Continuity
		11	Crisis Management

In contrast to many other standardisations, there are no concrete specifications for NIS1 as to which exact security precautions must be implemented in which way in order for the qualified body, i.e. the auditor, to give a positive assessment. There is no helpful checklist. There are three ratings for the review regarding the effectiveness of measures:

- **effective**, i.e. the auditor determines that the implemented measures are effective

- **partially effective**, i.e. improvements are required

- **not effective** i.e. the implemented measures are not effective > The objective has not been achieved.

The special challenge is that only a **single ineffective** measure in a category leads to the entire category being **not effective**; this applies analogously to partially effective. Consequently, each individual measure must be effective in each category in order to achieve an effective rating in all categories.

3. THE PROGRAMME

Although ASFINAG has placed a special focus on information security for many years, it quickly became clear after the NIS Act and the notice were issued: the goal to provide positive evidence to a qualified body could only be achieved with a concentrated effort, as a whole range of measures had to be implemented. In addition, many of these measures were interdependent and could only be implemented on time and with sufficient quality with overall control, meaning that multi-project management was required. Based on this recognition, the **programme NISFIT © - N**etwork and **I**nformation **S**ystem Security **Fit**ness - was launched.

The aim of the programme was to centrally manage all measures, from the risk analysis of essential services to ensuring all documentation Furthermore to regularly report progress to ASFINAG management, as well as to identify essential obstacles and bring about the necessary decisions via a ASFINAG-Group-wide steering committee.

In order to implement information security to a suitable extent, the following must be considered essential:

- ISMS - Information Security Management System
  Review and revision of emergency concepts, emergency manuals and emergency plans
  Review and revision of the existing crisis handbook
  Creation of information security implementation concepts for each service in the scope
- Process analysis
  Analysing which processes require adjustments in order to be able to establish information security sustainably.
- Scope definition
  Determining what the scope is: Which associated services make up the essential services
- Risk analysis
  Using a GRC tool (Governance, Risk and Compliance)
  Business impact analysis
  Gap analysis of the affected services based on previous modelling
  Project definitions derived from this in order to close the gaps in the services in the scope in a targeted and timely manner.
- Asset management
  Which components make up the services in the scope, both hardware and software. In order to be able to assess a risk or take protective measures in a given case, it must be known what is being used and where.
- Physical access protection
  Premises in which the components from services in scope are installed must be secured against unauthorised access - development of a zone concept.
  Derived from this, project definition for establishing access protection in order to establish physical access protection in a targeted and timely manner.
- Dealing with third parties
  Contractors must be involved. Complete authorisation must be ensured with regard to access and access by third parties.
  It must be made clear to suppliers and service providers that information security is given special attention.
- Remote access
  It must be ensured that networks, systems and services are accessed via controlled and secure channels. This also includes secure file transfer to prevent malware from being introduced into the ecosystem.
- User administration
  Regardless of whether it is your own staff or third parties, every single user must be known and authorised - Physical Identity and Access Management PIAM. The personal handling of information security must be trained in a sustainable manner.
- Protective measures
  Centrally controlled virus protection on all systems, log management, monitoring
- Defence
  The establishment of a Security Information and Event Management (SIEM) and a Security Operation Centre (SOC) is necessary to ensure the highest possible level of protection for the network and services. This is the only way to achieve 24/7 detection and defence against attacks.

It is clearly that many projects and measures must be implemented in parallel in order to be able to successfully provide evidence of information security in accordance with the NIS Act

to the qualified body in time - the need for programme management can be clearly derived from this.

4. IMPLEMENTATION OF THE NISFIT © PROGRAMME

In parallel to the countless measures and projects that secure ASFINAG's overall system externally, both technically and organisationally or procedurally, all tunnel facilities were analysed in depth. It was clear from the beginning that ASFINAG's previous very successful strategy "never touch a running system", that means it was well planned, well built and well maintained, and software changes were avoided as far as possible, would have to be completely changed to "keep the system up-2-date", which force frequent software changes.

First, the so-called target state had to be achieved, following a clear priority: ASFINAG operates almost 90 tunnels that are subject to the STSG (Road Tunnel Safety Act). The control systems of these tunnels, specifically the SCADA systems, and, where applicable, the local control systems (PLC) were comprehensively renewed or brought up to the latest technical standard. This means that the server infrastructure was replaced with Hyper Converged Infrastructure systems, which are high-performance and redundant server infrastructures that enable very high availability and simple manageability with several virtual machines. The applications and databases themselves were migrated to the latest version to achieve the best possible security. The local PLCs whether hardware or software PLCs, were also replaced where necessary or at least upgraded to the latest software version. In addition, centralised virus protection was implemented, and the prerequisites were created to enable regular software updates (patch management) to be carried out with the least possible effort.

These migration projects were not only a technical challenge, but they also had to be tested extensively, as tunnel safety naturally has top priority. Both required full tunnel closures or at least partial closures. The need for very high availability of the tunnel facilities in order to minimise disruption to traffic was no less of a challenge than the technical aspects. This is because, regardless of the establishment of NIS1 compliance, other ASFINAG renovation projects also cause traffic-impairing measures, which required complex and time-consuming coordination with various ASFINAG organisational units.

Clarification works also had to be carried out in advance with the tunnel administration authority to make clear, that these migration projects would not change the functionality approved by the authority during the construction or latest renovation of the tunnel.

A major effort, which was always carried out in advance of the migration works, was checking the installed assets and updating the asset information in the Configuration Management Database (CMDB).

Part of the migration projects was the creation of the so-called information security implementation concepts, which help to ensure that the necessary measures were also implemented in a comprehensible manner.

5. THE PROOF

All measures from the 11 categories were reviewed in 4 partial audits by the so-called qualified body and the reports were sent to the Austrian DSN (Directorate of State Security and Intelligence). The audits were also carried out on site, primarily to be able to check the requirements for property protection and access protection. Ultimately, the measures in all 11 categories were assessed **positive** by the authority.

6. THE CHALLENGES

Protection of buildings was particularly challenging, as the necessary measures went beyond all the partial responsibilities of different organisational units at ASFINAG. In addition, the geographical distribution of the properties - and these are not just the tunnels, but all premises that host components that are in the scope of the essential services - also contributed to the complexity. The realisation of the construction measures was not only costly, but also difficult in terms of time. Here, the programme management raised awareness accordingly and brought about decisions with the necessary consistency.

The time resources and information security expertise of the individual employees responsible for the individual services in the scope had to be supported. These support resources were also procured and provided and managed by the programme management.

7. CONCLUSION

Only by deciding to launch the NISFIT © programme was ASFINAG able to successfully implement all measures on time. In addition, the programme management initiated the long-term safeguarding of the level of information security achieved by making information security part of ASFINAG's day-to-day business in all processes and planning procedures.

Mission accomplished!

8. REFERENCES

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148

[2] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536