Implementation of the NIS Directive in Austria…

…from the point of view of the Operational NIS Authority in the Ministry of Unrestrictedal Affairs

Gernot Goluch, II/.BVT/5-NIS
Wien, 27. Juni 2019

Overview

- **NIS Directive**
  - EU Directive on security of network and information systems
- Cybersecurity Act
  - EU legal act on cyber security
- NIS-Law & NIS-Regulation
  - Implementation of NIS Directive into Austrian law

NIS Directive

- **Background**
  - IT systems play a central role in society
  - Reliability and security are crucial to economic and social activities and the proper functioning of the internal market
- **Directive (EU) 2016/1148 of 6th July 2016**
  - Directive on measures to ensure a high common level on security of network and information systems in the European Union
  - 1. legal act on cybersecurity in the EU

Overview

- NIS Directive
  - EU Directive on security of network and information systems
- **Cybersecurity Act**
  - EU legal act on cyber security
- NIS-Law & NIS-Regulation
  - Implementation of NIS Directive into Austrian law

Cybersecurity Act

- **Permanent mandate** for the European Union Agency for Network and Information Security **(ENISA)** with increased funding
- Among other things, ENISA will serve as an independent **center of competence** and should also contribute to **capacity building** within the EU
- Establish an EU-wide **European certification framework** for cybersecurity of **products, processes and services**
- The framework should consider security characteristics such as **"Security by Design"**

Overview

- NIS Directive
  - EU Directive on security of network and information systems
- Cybersecurity Act
  - EU legal act on cyber security
- **NIS-Law & NIS-Regulation**
  - Implementation of NIS Directive into Austrian law

NIS-Law – Objectives and Goals

- Establish measures to achieve a high level of security of network and information systems
  - In particular by:
    - National strategy for the security of network and information systems
    - Establishment of national organizational and coordination structures
    - **Security requirements and reporting requirements**
    - Tasks and requirements for computer emergency teams
    - Data protection
    - Sanctions

NIS – Regulations (BKA)

- Essential elements are specified in regulations
  - Terminology regarding essential services
  - Terminology regarding security incidents
  - Definition of subsectors and areas
  - Definition of essential services
  - Determination of parameters and thresholds
  - Definition of reporting thresholds
  - Definition of *lex specialis* provisions
  - Requirements on certification authorities (Qualified Bodies)

Addressees

- Addressees of the NIS-Law are
  - Providers of digital services
  - **Operators of essential services**
  - Public administration facilities
- Addressees are essential for the proper functioning of the community
- Obligations
  - Taking security precautions
  - Reporting security incidents
- Computer emergency teams / Qualified Bodies

Operators of Essential Services

- The Office of the Federal Chancellor determines
  - for each sector, those operators with a branch in Austria,
  - who provide an essential service

1. Energy
2. Transport
3. Banking sector
4. Financial market infrastructure
5. Healthcare
6. Drinking water supply
7. Digital infrastructure

NIS-Law & NIS-Regulations – Status Quo

- NIS-Law entered into force already
- NIS-Regulations aligned
- Preparatory measures for notifications
- New NIS Fact Sheets
- National computer emergency team **CERT.at**
- Reporting web portal
- Work on sector-specific security standards

NIS-Regulations & Investigation Proceedings – Status Quo

- After coming into force of **NIS-Regulations**
  - **Identification** of **operators of essential services** in all sectors of NIS-Law by the Office of the Federal Chancellor by **notification**
- Investigation proceedings
  - **Preparation of notification**
  - **Letter of information**
  - Transnational consultation

Requirements on Qualified Bodies (QuaSteV-Regulation)

- **Coordinated** with the Office of the Federal Chancellor
- Can only be issued **after the entry into force** of the **NIS-Regulations**
- **Timely** submission is expected
- After the entry into force of **QuaSteV-Regulation**
  - **Approval procedure for Qualified Bodies**

Security Measures – Framework

Security Measures for Operators of Essential Services

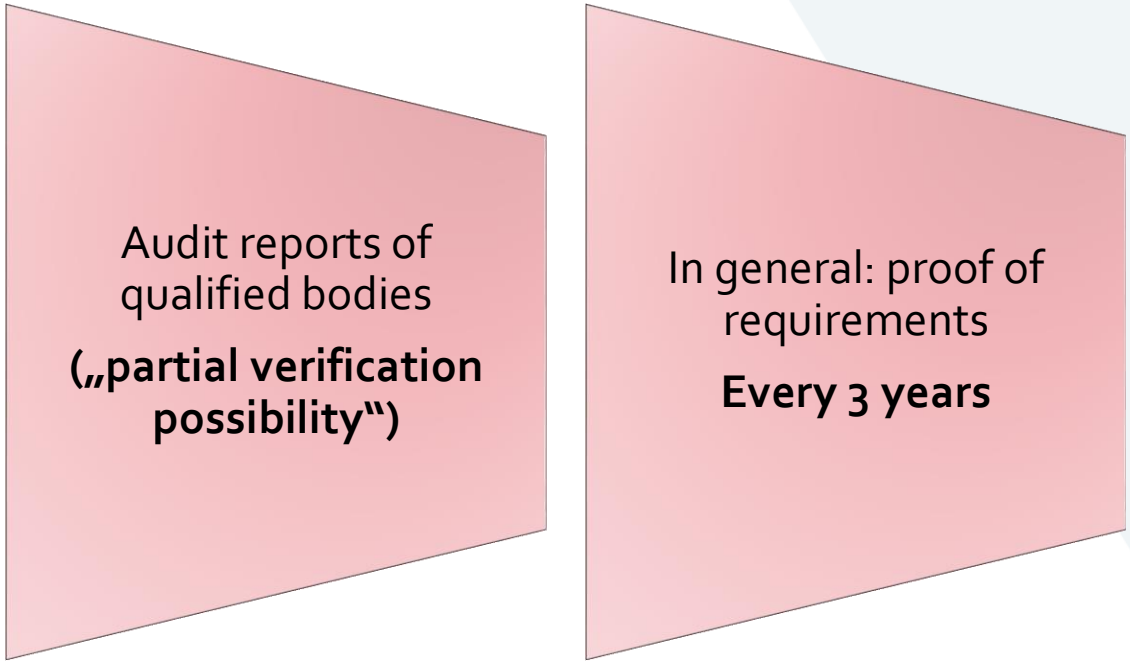
NIS Fact Sheet 08/2018

- NIS Fact Sheet 08/2018 – Mapping table, example:

2.2.1 Governance und Ökosystem

#	Kategorie	Sicherheits-maßnahme	Ö. Informations-sicherheits-handbuch Version 4.0.1	BSI IT-Grundschutz[5]	ISO 27001:2013	ISA/IEC 62443 3-3	CIS CSC Version 6.0	CIS CSC Version 7.0	NIST CYBER SECURITY FRAMEWORK
1	Governance und Risikomanagement	Risikoanalyse	4 Risikoanalyse	*BSI-Standard 100-2, Kapitel 3, 4, 5, BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz*	8.2 Information security risk assessment 8.3 Information security risk treatment	SR 5.1, 5.2, 5.3	1, 2, 4, 13, 14, 17	1, 2, 3, 13, 14, 17	ID.GV-4 ID.RA-1,2,3,4,5,6 D.RM-1,2,3 PR.AT-2

Check Cycle of Security Measures for Operators of Essential Services



Thank you for your Attention!

Mag. Gernot Goluch
II/.BVT/5-NIS
nis@bvt.gv.at