CSC

ICT Solutions for Brilliant Minds

Adapting to the NIS 2 directive

20th SIG-NOC, 2024-05-08

Urpo Kaila urpo.kaila@csc.fi

Head of Security

Agenda

- Introduction
- NIS 2 recap
- Cyber security compliance
- Compliance requirements for CSC and Funet
- Typical pitfalls
- ISO 27001 and NIS 2
- Compliance and NRENs’
- Discussion

What was cyber security all about?

- Cyber security is about **protecting assets against risks with security controls**
  - such assets are systems, data, services, and reputation.
- Assets can (and must) **be protected** to prevail their
  - **Confidentiality** – the prevention of intentional or unintentional disclosure
  - **Integrity** – the prevention of unauthorized modification and protection of consistency
  - **Availability** – the protection of reliable and timely access
- Think big on scope of security
  - Network security, information security, corporate security, cyber security

NIS 2 recap

- NIS 2 is a legislative act that aims to achieve a high common level of cybersecurity across the European Union.
  - The full name is directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148
- Member States must
  - ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures
    - to manage the risks posed to the security of network and information systems
    - to prevent or minimise the impact of incidents on recipients
      - of their services and on other services
    - The measures must be based on an all-hazards approach

Cyber Security Compliance (1/2)

- What does compliance mean?
  - In this context: " conformity in fulfilling official requirements"
- For conformity to make sense, explicit compliance criteria or at least documented well known best practices should be available
- To ensure compliance it should be verified by a trusted third party
  - Accredited auditors
  - Audit methodology and procedures
  - It is not compliance if somebody just claims thar 'We are 100% secure"
- A certification can be issued as a proof if no non-conformities has been found
- Certification does not ensure that no cyber security issues exists

Cyber Security Compliance (2/2)

- What requirements does NIS 2 contain?
- Essential measures:
  - Asset management
  - Risk management
  - Data and information security
  - Employee management
  - IT governance
  - Managing suppliers and IT services
  - Incident handling and reporting
  - Business continuity
  - Security policies
  - Regular performance evaluation

Compliance requirements for CSC and Funet

- Other security cyber security compliance requirements affecting CSC and Funet
  - Security and procurement agreements
  - National Security Auditing Criteria "Katakri"
  - Assessment criteria for information security in public administration "Julkri"
  - ISO 27001
  - Act on Secondary Use of Health and Social Data
  - Regulation by Finnish Transport and Communications Agency
  - CER, DER,…

Typical pitfalls in security compliance

- “My job is a personal issue, nobody should meddle with that”
- “ Outsiders cannot understand what we are doing”
- “The customers/management/funding party should just trust us”
- “Only we understand security”
- “Security is only about our technology”
- ”We don’t trust anybody outside our own team”
- “Security is not part of the deal”

ISO 27001 and NIS 2

- Fortunately there is a strong overlapping between NIS 2 requirements and ISO 27001

NIS 2	ISO 27001:2022 Appendix A
Asset management	A.5.9
Risk management	A.5.1
Data and information security	A.5.1
Employee management	A 5.15-A5.19, A.6.1-A.6.8
IT governance	A.5.36
Managing suppliers and IT services	A.5.19 -A.5.21
Incident handling and reporting	A.5.24-A5.27
Business continuity	A.5.29-A5.30, A.8.13-A.8.14
Security policies	A.5.1
Regular performance evaluation	A.5.35-A.5.36

Examples

Compliance and NRENs'

- NREN's are mission critical providers for higher education and for research infrastructures'
- The European risk landscape has changed to a clearly darker mode
- NREN's has a good track record on availability
- Few NREN's has achieved ISO 27001 certification
  - See "Typical pitfalls"
  - Customers cannot choose their NREN
- Discussion

Discussion

Urpo Kaila

security@csc.fi
urpo.kaila@cscfi
security@csc.fi

040-5174601

facebook.com/CSCfi

twitter.com/CSCfi

youtube.com/CSCfi

linkedin.com/company/csc---it-center-for-science

github.com/CSCfi