Issued:	Entry into force:	Validity:
08/04/2025	08/04/2025	until further notice

Legal basis:
Act on Cybersecurity Risk Management (124/2025), sections 9 and 18
Act amending the Act on Information Management in Public Administration (125/2025), section 18 c

Revision details:

Finnish Transport and Communications Agency Traficom recommendation on cybersecurity risk management measures for NIS supervisory authorities

Contents

I Background and purpose of the recommendation

Recommendation for authorities

The National Cyber Security Centre Finland at the Finnish Transport and Communications Agency Traficom (later 'the Finnish Transport and Communications Agency') has drawn up this recommendation for supervisory authorities to support the monitoring of the cybersecurity risk management measures described in the NIS2 Directive. The recommendation is based on the Act on Cybersecurity Risk Management (124/2025) (later also 'the Cybersecurity Act') and amendments (125/2025) to the Act on Information Management in Public Administration (906/2019) (later also 'the Information Management Act').

The purpose of the recommendation is to offer information to the authorities on what kinds of measures the statutory requirements may entail. The recommendation also describes different methods that the supervisory authority may use in its guidance and supervisory tasks based on its discretion and case-specific assessment. The authority may also make use of external information security inspection bodies or other information security professionals. The use of external assistance can be needed e.g. in situations where an inspection would require special technical expertise or extensive technological capabilities that the supervisory authority does not itself possess. These include situations where the supervisory authority does not have the necessary tools or competence for performing scans or configuration reviews.

For the sake of clarity, the Finnish Transport and Communications Agency states that the recommendation is not binding on the authorities or entities and is only intended to guide, assist and support. Legally binding obligations are laid down in acts, implementing acts of the Commission and any further technical regulations issued by supervisory authorities, which may account for sector-specific special characteristics. Each supervisory authority is competent to decide what kinds of measures meet the regulated requirements in each sector. In turn, an entity within the scope of application of the regulation must ensure that the operations of its organisation comply with the regulated obligations.

The Finnish Transport and Communications Agency states that complying with the recommendation and the standards or general frameworks mentioned in the recommendation or using the Cybermeter tool created by the Finnish Transport and Communications Agency does not guarantee that the entity meets the regulated requirements as a whole. The assessment criteria and standards used in the recommendation are not harmonised as such with the requirements of the Cybersecurity Act or the Information Management Act. For example, an item in a standard may contain requirements that are not included in legislation, so they are not directly comparable. This means that the assessment criteria and standards are used as additional information sources and examples; there is no obligation to use them, but they help to demonstrate compliance.

The recommendation was only created to translate into concrete terms the options for verifying the measures that are set out in section 9 of the Cybersecurity Act and section 18c, subsections 1–12 of the Information Management Act and specified in their rationales. However, the Finnish Transport and Communications Agency notes that other provisions closely associated with risk management measures, such as provisions on sector-specific risk assessments, risk management activities carried out by entities in which the principle of proportionality is accounted for, and management accountability in the Cybersecurity Act and Information Management Act are also background factors.

The recommendations issued can also support the cybersecurity risk management planning of other entities than the ones referred to in section 3 of the Cybersecurity Act. In particular, the recommendations on the baseline information security practices in chapter 11 are drawn up in a way that also allows entities outside the scope of application of the NIS regulation to follow them and assess the maturity level of their organisation’s cybersecurity and improve it.

The Finnish Transport and Communications Agency has drawn up this recommendation for the supervisory authorities of cybersecurity risk management measures as a part of the authority cooperation and coordination task of the single point of contact.

Legal basis

The recommendation is based on the so-called NIS2 Directive, Cybersecurity Directive, i.e. 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.

Article 21 of the NIS2 Directive issues provisions on cybersecurity risk management measures. According to Article 21(1), Member States shall 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 which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. According to Article 21(2), these measures shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents. The points of Article 21(2) list factors that this approach must at least include.

The NIS2 Directive has been nationally implemented with the new Cybersecurity Act and amendments to the Information Management Act.

The scope of application of the Cybersecurity Act covers entities from different sectors specified in section 3 of the Act. Section 9 of the Act lays down provisions on cybersecurity risk management measures. According to section 9, subsection 1, entities must take proportionate technical, operational or organisational management measures in accordance with the cybersecurity risk management procedure in order to manage the risks posed to the security of networks and information systems and prevent or minimise harmful impact. According to the provisions of section 9, subsection 2, the cybersecurity risk management procedure and the management measures that are based on it must take into account and keep up to date at least the factors mentioned in paragraphs 1−12 of the subsection. This recommendation discusses the practices applicable to these 12 paragraphs as separate chapters.

In terms of public administration entities, requirements concerning cybersecurity risk management measures have been implemented with the Act on Information Management in Public Administration. Section 3 of the Act provides more detailed provisions on what kinds of public administration entities are subject to the requirements. In the Information Management Act, the requirements for cybersecurity risk management measures are laid down in chapter 4 a, section 18 c. The contents of the requirements are the same as in the Cybersecurity Act.

Under section 18 of the Cybersecurity Act, the National Cybersecurity Centre Finland at the Finnish Transport and Communications Agency acts as the single point of contact as referred to in Article 8(3) of the NIS2 Directive. According to section 18, subsection 2, the task of the single point of contact is also to promote cooperation and coordination between the supervisory authorities in implementing their tasks under the Act. According to the rationale for the provision, the single point of contact can promote cooperation and information exchange between the supervisory authorities and issue recommendations for the supervisory authorities on the coordination of the requirements and supervision under the Act.

The above-mentioned nationally implementing regulation does not issue stricter requirements than the NIS2 Directive. Instead, the Directive has been implemented based on the principle of minimum harmonisation.

Preparation and maintenance of the recommendation

In drawing up this recommendation, the Finnish Transport and Communications Agency has examined in parallel the Cybersecurity Act and the Information Management Act, the NIS2 Directive and Implementing Regulation 2024/2690 and its accessory documents prepared in cooperation by Member States, the Commission and ENISA, as well as several sets of information security criteria and assessment tools, such as ISO/IEC 27001, IEC 62443, NIST CSF, Julkri and Cybermeter. With the help of the above-mentioned and the Agency’s experience gained from various information security tasks, the objective has been to define common cybersecurity practices that can be applied to the cybersecurity risk management measures specified in the Act and their supervision.

During the preparation of the recommendation, discussions have been held with authorities supervising operations in accordance with so called NIS Directive (EU) 2016/1148 and new supervisory authorities under the NIS2 Directive. The purpose of these discussions has been to chart the scope of entities falling under the supervision of different authorities and the capabilities of authorities to conduct supervision in accordance with the new regulation. In particular, the discussions covered questions on the competence and resources required for supervision and the procurement of external assistance. The authorities especially hoped to receive assistance in the supervision of technical cybersecurity, in terms of both carrying out the supervision and assessing the results. This recommendation aims to provide answers to these questions and it has been supplemented during the preparation process e.g. based on discussions conducted with the authorities.

The Finnish Transport and Communications Agency requested statements on the draft recommendation on cybersecurity risk management measures referred to in the NIS2 Directive for supervisory authorities. The recommendation was circulated for comments in Finnish on the lausuntopalvelu.fi service for eight weeks between 5 April 2024 and 31 May 2024 (comment request journal number: Traficom/18410/09.00.02/2023). The request for comments was particularly targeted to the supervisory authorities under the Cybersecurity Act, but anyone wishing to do so could leave a comment.

Sixteen comments on the recommendation were received in total.

A summary of the comment feedback has been prepared with the most pertinent feedback. The comment summary is available on the Finnish Transport and Communications Agency's website[1].

As a result of the comment feedback, the recommendation was adjusted with changes, clarifications and additional information.

According to the statements received, the draft recommendation was generally found to be supportive of the supervisory authorities and entities. It was felt that the recommendation translates the practical implementation of the risk management obligations imposed by the legislation into concrete terms. As a basic premise, the content of the draft recommendation was regarded as being comprehensive and having a clear structure, as it is consistent with the structure of the Government proposal for an Act on Cybersecurity Risk Management for the corresponding parts. Parties issuing statements found that the presentation in table format supported the comprehensibility of the recommendation. They welcomed the fact that each individual measure of the recommendation was explained and contains a clear reference to the relevant frameworks.

[1] https://kyberturvallisuuskeskus.fi/sites/default/files/media/file/Summary%20of%20statements%20on%20the%20Traficoms%20draft%20recommendation%20on%20cybersecurity%20risk%20management%20measures%20referred%20to%20in%20the%20NIS2%20Directive%20for%20NIS%20supervisory%20authorities.pdf

On the other hand, examination of each risk management measure individually and separately from other requirements was also found challenging, as this can guide entities to manage each risk with the same intensity. Parties issuing statements would also like to see more attention being paid to the possibility of the measures offsetting each other. The recommendation was additionally felt to be too long, which is why a summary of the management measures was called for.

The recommendation consciously strives to present each risk management measure as an independent entity and to set out its content, which results in partial overlap between the example implementations. The explanation paragraph included in each individual risk management measure discussed in the recommendation was regarded as serving as a summary.

The terminology of the recommendation was clarified, and the references used in the recommendation were specified. The introductory text of the recommendation was complemented, and detail was added to it insofar as the feedback received concerned a risk-based approach, the principle of proportionality, management accountability and the relationship between the recommendation and any further technical regulations to be issued by the authorities. In addition, the instructions for reading the recommendation were supplemented with a more specific definition of entities with a higher level of maturity.

Perceiving the correspondence between the risk management measures included in the recommendation and the frameworks used in it (standards and sets of assessment criteria) was experienced as a challenge. While a cross-reference document drawn up by the Finnish Transport and Communications Agency was appended to the recommendation as a response to this feedback, the introduction of the recommendation was supplemented to avoid a possible misunderstanding of it constituting harmonised standards that would directly meet the requirements of the Act.

Comments on the risk management measures included in the recommendation were provided in both general statements and those specific to individual measures. The recommendation was primarily updated in keeping with the amended Government proposal for an Act on Cybersecurity Risk Management, after which the feedback received on cybersecurity measures during the consultation was taken into account as far as possible by modifying the recommendation or adding detail to it. The observations concerning sector-specific standards and guidelines were added to the recommendation as proposed.

According to the feedback received, organising the consultation before Parliament had finished debating the Cybersecurity Act was considered problematic, a fact of which the Finnish Transport and Communications Agency was also aware. The Finnish Transport and Communications Agency requested comments on the draft recommendation despite the challenging timing of the consultation, as even if the draft was incomplete, it was deemed to translate the implementation of the risk management measures into more concrete terms and to support especially those supervisory authorities and entities who are new to the scope of this legislation.

The recommendation is valid from 08.04.2025 onwards until further notice. The recommendation will be updated if necessary based on feedback from stakeholders and practical experiences.

Impact assessment

Impact on the information society and security

The objective of the new regulation on cybersecurity risk management, and thereby of this recommendation, is to improve the security and reliability of society reliant on networks and information systems. Discussions held during the preparation and the application of the recommendation can be used to assess and promote in concrete terms the maturity level and state of cybersecurity in different sectors. The recommendation aims to increase and strengthen the overall reliability and security of networks and services used in different sectors of society. The recommendation is expected to promote and strengthen cybersecurity in society.

One section of the new regulation are the baseline information security practices (in the NIS2 Directive, basic cyber hygiene practices). Section 11 of the recommendation provides recommendations for baseline information security practices that can be utilised by all entities of society regardless of whether the entity falls within the scope of regulated obligations. In this respect, in particular, the recommendation aims to improve society’s cybersecurity.

Impact on the authorities

The objective of the recommendation is to make guidance, advice and supervision related to national regulation more consistent and harmonised on the level of society as a whole. The recommendation provides authorities with tools for drawing up proactive material for entities, for issuing advice and guidance and applying the requirements, as well as for drawing up potential regulations on cybersecurity risk management measures. The purpose of the recommendation is to support the authorities so that they do not need to create all methods and practices from scratch. The expertise and resources of supervisory authorities vary e.g. because the tasks imposed by national regulation are new for some authorities. Due to the differences in sectors, however, the recommendation cannot cover sector-specific special characteristics.

The recommendation should have positive impacts on the operations of supervisory authorities and, for its part, it provides a support for the cooperation between different supervisory authorities. If the recommendation is widely adopted, the supervisory procedures of the supervisory authorities will be harmonised across different sectors. This will also promote the transparency of authority duties and the predictability and consistency of supervisory operations among entities.

The preparation of the recommendation has aimed for technological neutrality and universal solutions. However, it is difficult to predict future technologies, which can cause the need to update the recommendation later. Keeping the recommendation up to date may prove to be challenging due to the speed of technological development.

Due to the wide scope and technical nature of the recommended matters, lighter informative guidance, such as authority advice in individual situations, occasional training events or frequently asked questions on authority websites, is estimated to be less effective than a recommendation. The recommendation can help reduce the need for entity-specific guidance.

Impact on entities

The recommendation aims to ensure that cybersecurity risks are assessed comprehensively as a part of an entity's risk management and that changes in the operating environment and their impact on operations are better identified in the future. Furthermore, the recommendation enables the proportional assessment of risk management measures in relation to the risk and supports in the implementation of risk management. By implementing the measures described in the recommendation, entities are better able to recover from cyber incidents and can thus produce more secure and reliable services to society as a whole.

The recommendation also takes acquisitions and supply chains into account from the perspective of risk management. Implementing the measures described in the recommendation enables an entity to form a better situational picture of the potential risks posed. In terms of procurement, in particular, the recommendation aims to offer tools for identifying and managing cyber risks related to procurement.

Good risk management can offer many benefits to the entity. If the recommendation helps an entity manage cybersecurity risks, it can reduce its burden in acquiring required or voluntary sector-specific certifications. In the long term, a continuously maintained and appropriate risk management system supports the entities' business operations and helps them identify business development opportunities. Following the recommendation can prevent a cyber risk from being realised, meaning that no financial resources are taken up by incident response and recovery. With the help of the recommendation, an entity can also learn to assess the meaning of residual risk and prepare for it. Furthermore, the entity can better define the division of responsibility related to residual risk.

Definitions

The definitions presented here are largely based on the definitions of the Cybersecurity Act and the related government proposal and the definitions of the TEPA Term Bank.[2] A reference is provided for each definition. This section

[2] Finnish Terminology Centre's collection of special language dictionaries https://termipankki.fi/tepa/en/

particularly contains definitions used in the recommendation that are not included in section 2 Definitions of the Cybersecurity Act.

Entity refers to a legal or natural person who carries out operations referred to in Annex I or II of the Cybersecurity Act or is of the entity type referred to in Annex I or II and meets or exceeds the definition of a medium-sized entity or is an entity regardless of its size, or meets the special criticality criteria. (Cyber Security Act, section 3)

Significant incident refers to an incident that has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned, or an incident that has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage. (Cyber Security Act, government proposal rationale)

Risk management policy refers to an organisation's top-level planning that systematically identifies, assesses and treats risks posed to the organisation or its operation, sets objectives and monitors their implementation. [Similar principles can also be referred to as a risk management policy.] (Cyber Security Act, government proposal rationale)

Risk management procedure/process refers to a risk management process that regularly identifies, analyses, assesses and treats risks posed to networks and information systems and their physical environment. The effectiveness of the management measures of risks treated as a part of the risk management procedure is assessed with appropriate metrics. (Cyber Security Act, government proposal rationale)

Risk management measures refer to the measures taken by entities in order to manage and prevent the risks posed to the security of networks and information systems and prevent or minimise harmful impact. (Cyber Security Act, government proposal rationale)

Information security policy refers to an entity's view of the objectives, principles and implementation of network and information system information security throughout their lifecycle. The ISO/IEC 27001 standard also refers to similar principles as the information security policy. (Cyber Security Act, government proposal rationale)

Information security procedures/processes refer to different processes and technical procedures that implement the information security policy related to networks and information systems. (Cyber Security Act, government proposal rationale)

Information security practices refer to operating methods related to information security and cybersecurity that implement the information security procedures in practice. (Cyber Security Act, government proposal rationale)

Verification refers to the procedure of aiming to ensure the legitimacy, authenticity or origin of a target. Verification can take place on different levels, it can be strong or weak, and it can be performed on a desired assurance level. (TEPA Term Bank)[3]

In this recommendation, verification or authentication can also be used in the context of access control, in which case the definition of the term is discussed separately.

Configuration refers to the configuration of software or a device. (TEPA Term Bank)

Hardening refers to a configuration where only the functions, equipment and services that are essential for operating requirements and data processing have been taken into use. (Katakri)[4]

Segmentation refers to network separation by restricting a network environment into manageable entities. (Katakri)

Zero trust refers to a principle where no information network, device, user or application is automatically guaranteed certain rights or access to information or information systems. According to the principle, each action in an information system always requires identification, and activities are monitored continuously and automatically. (Katakri)

A backup is a recording that is intended to be used if the original recording is lost due to a fault or damage or some other similar issue. (TEPA Term Bank)

A backup/redundant system is a system that can be taken into use when the use of the normal system is disrupted or prevented. The backup system does not need to be identical to the normal system as long as it provides operational readiness that is similar enough to the normal system. (TEPA Term Bank)

[3] Finnish Terminology Centre’s collection of special language dictionaries https://termipankki.fi/tepa/en/
[4] https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

II Reading instructions for the recommendation

Each of the following chapters focuses on one cybersecurity risk management measure listed in section 9, subsection 2 of the Cybersecurity Act and section 18 c, subsection 1 of the Information Management Act. The measures are presented in the same order as in the Acts. In implementing the measures and their supervision, orders deviating from this recommendation may be justified. Furthermore, it can be reasonable to focus supervision on the supervisory measures that are most important for the supervised sector or entity.

Each of the presented cybersecurity risk management measures is further divided into more specific recommendations that are presented in the form of a list. After the list of recommendations, more detailed grounds for each recommendation are provided in table form.

Each risk management measure presented in a table is followed by an extended instruction for entities from whom the supervisory authority expects a higher level of maturity. The recommendation lists and tables are otherwise in the same order.

The instructions for entities with an elevated cyber risk is primarily based on Implementing Regulation (EU) 2024/2690 adopted by the Commission on the basis of Article 21, paragraph 5 of the NIS2 Directive, which established technical and methodological requirements for cybersecurity risk management measures for

- DNS service providers
- TLD name registries
- cloud computing service providers
- data centre service providers
- content delivery network providers
- managed service providers
- managed security service providers
- providers of online market places
- providers of online search engines
- providers of social networking services platforms, and
- trust service providers.

The requirements of a higher level of maturity may also be justified for other actors within the scope of the Cybersecurity Act and the Information Management Act on the basis of the entity’s risk assessment and sector-specific special characteristics. Such entities could include large organisations with their own software development. In the future, the Commission may also adopt other implementing regulations concerning essential and important entities to lay down requirements for risk management measures.

Example implementations

- The example implementations describe how the recommendation described in the table or parts thereof can be implemented and what kinds of implementations the supervisory authority may encounter in connection with supervision.
- The list of example implementations is not exhaustive, but in particular aims to provide examples for situations where there is no prior experience of the implementation of matters described in the recommendation. The scope of implementations should, however, be proportional to the risk and other operational requirements related to the operations.
- The required measures can vary significantly based on the entity size, sector and the threats facing the entity. However, the example implementations aim to take into account various kinds of entities and their varying needs as far as possible.

Verification

Verification describes examples of how the supervisory authority can verify the implementation of an entity’s cybersecurity risk management measures. The verification examples are divided into three categories based on the technical difficulty level of the measures. Supervision in accordance with different categories provides certainty of different levels on the status of the entity’s cybersecurity at the time of review. Measures from different categories can also be selected in accordance with the available resources.

1. Category 1 mainly describes supervision based on documentation or self-evaluation. A review based on documentation or self-evaluation rarely provides an in-depth view of the actual status of cybersecurity. It is therefore recommended that at least some matters from categories 2 or 3 are included. By using the category 1 implementation examples, however, the supervisory authority can gain a broad understanding of the overall status of the sector relatively lightly by targeting a similar supervision or self-evaluation to a large number of entities.
2. Category 2 describes a more in-depth review of the current state of the entity’s measures. However, the category focuses on technically light measures, such as interviews, configuration reviews or other similar evidence. Category 2 reviews can typically make use of more technical evidence provided by the entity.
3. Category 3 describes technically advanced measures that usually require preparation and different competences, such as the use of different programs and tools and the ability to interpret technical data. These can include various scanning that, in addition to the authority, can be carried out by the entity itself or a third party.

It is recommended that supervision also use methods from different categories e.g. based on sector-specific risks or vulnerabilities caused by the nature of the sector. The scopes and technologies of networks and information systems can vary considerably and there are a great number of related details that impact cybersecurity. It is also typical that self-evaluation and documentation review do not provide a realistic image of the cybersecurity of a network and information system. Self-evaluation is naturally also dependent on the experience of the self-evaluator and on the time available. Other verification means can complement the image of the system's status received through self-evaluation.

The supervisory authority must consider what measures it deems necessary for its supervisory operations in each case. In addition to the authority receiving information and evidence from the entity, the authority itself can carry out inspections and other observation or make use of external inspection bodies, such as accredited information security inspection bodies or other competent information security professionals. In some cases, supervision can also require cooperation with another supervisory authority in Finland or in another Member State.

Explanations

Explanations offer some practical grounds for why the measure indicated by the heading has been included in legislation and the recommendation and what its objective is.

Explanations offer tools for discussions between the supervisory authority and the entity on the grounds for the requirements. Explanations help the supervisory authority to interpret whether the measures taken by the entity protect against the threat perspectives mentioned in the explanations.

Some sections do not include explanations. In such cases it is considered that presenting separate explanations does not provide additional value to the example implementations or supervisory methods already presented in the table.

References

References offer examples of widely known standards, frameworks and guidelines related to the recommendation in question. The supervisory authority can look for more information or descriptions of commonly used implementations from these sources.

The list acts as an example and aims to highlight specific sections of standards and frameworks that particularly serve the aims of each recommendation. Different sectors may also use other relevant standards and frameworks.

Tools

Tools mention assessment means and metrics in addition to tools and software that a supervisory authority can utilise in its supervisory measures. An entity can also use tools to measure its own maturity level and improve its operations.

1 Cybersecurity risk management policy and assessing the effectiveness of risk management measures

These recommendations are based on Article 21(2)(f) and partly (a) of the NIS2 Directive. The national implementation of these points is laid down in section 9, subsection 2, paragraph 1 of the Cybersecurity Act and in section 18 c, subsection 1, paragraph 1 of the Information Management Act.

1. **Cybersecurity risk management procedure**: An entity should have in use a cybersecurity risk management procedure that regularly identifies, analyses, assesses and treats risks posed to networks and information systems and their physical environment. When assessing the effectiveness of policies and measures, the nature of risk management should be factored in as a continuous part of an organisation's activities, which would require including the assessment of the effectiveness of policies and measures in management measures. The cybersecurity risk management policies and procedure should be based on up-to-date best practices and standards adopted in the sector. (See sections 1.1 and 1.1.1.)

2. **All-hazards approach**: Risk management should adhere to an all-hazards approach and ensure that the company's governance and risk management processes take information security risks and cybersecurity risks into account. (See section 1.2.)

3. **Identifying needs and activities**: The starting point for risk management should be to identify needs related to confidentiality, integrity, availability and authenticity and, as its target, the key services, systems, processes and persons in terms of activities. Identification relates to section 5 on asset management. (See section 1.3.)

4. **Cyber threat identification**: Risk management would require identifying threats to the entity and assessing their likelihoods and impacts. (See sections 1.4 and 1.4.1.)

5. **Risk treatment**: Risk treatment should aim to address risks in such a way that their likelihood or impact is minimised, eliminated or outsourced and that the residual risks generated as a result of risk treatment are justifiably accepted. (See section 1.5.)

6. **Risk management effectiveness assessment and metrics**: The effectiveness of risk management should be assessed regularly with appropriate metrics so that the functioning of selected measures can be measured and improved if necessary. The assessment could be carried out as a self-evaluation or with the help of independent information security service providers. Risk management should involve assessing the effectiveness of risk management measures in relation to threats to the entity, and their foreseeable impacts. (See sections 1.6 and 1.6.1.)

1.1 Cybersecurity risk management procedure

Example implementations

- Entities use a cybersecurity risk management procedure for protecting networks and information systems and their physical environment from incidents and their impact. The cybersecurity risk management procedure is a key part of the entity's overall risk management. The risk management procedure is usually a part of the organisation's management system and supports the organisation's business strategy. Top management has approved the risk management procedure and the roles, responsibilities and authorisations important for cybersecurity and risk management, see section 6.1 Human resources security procedures.
- The entity has documented the risk management procedure and prepared risk assessments and made them available. The documentation indicates the policies and the selected documentation method. The procedure includes a description of the risk management process, the assessment and development of the procedure, and practices for assessing and measuring the effectiveness of risk management measures and continuous improvement. The documentation indicates management commitment, roles and responsibilities important for risk management, risk owners and persons responsible for management measures.
- In its risk management process, the entity has described the risk management process and included all stages required by risk management, such as risk identification, analysis and impact assessment as well as procedures for risk treatment, including procedures for selecting the management measure, residual risk treatment and management review. See section 1.5 Risk treatment.
- The risk management policies and measures are appropriate for the entity's needs, and they have been developed continuously and as the operating environment changes. As a part of the management measures, their effectiveness should also be assessed to ensure that the selected risk management measures are up to date. See section 1.6 on effectiveness assessment.
- The risk management procedure should be based on risk management methods and tools in accordance with generally known standards or best practices adopted in the sector.
- It is recommended that the risk management procedure also include sector-specific policies and rules, standards and sector-specific regulation.
- The entity has carried out risk management regularly and in particular when changes or significant incidents occur in the operations or the operating environment.

Verification

1. The supervisory authority verifies that the entity has a documented cybersecurity risk management procedure, risk lists and instructions as well as potential assessment of change impacts. The documents are available to staff. The procedure and documentation indicate the different stages of the risk management process, such as risk identification, analysis, assessment and treatment as well as implemented risk management measures. The procedure indicates how cybersecurity risk management is implemented and documented as a part of the organisation's operations, how risk management takes into account the risks to networks and information systems and their physical environment as well as how the entity has included the assessment of the effectiveness of policies and measures into its risk management measures. The procedure also indicates how management accountability is implemented in the risk management procedure and any roles and authorisations related to risk management (see section 6.1). The risk management procedure indicates the regularity and continuity of risk management that can also be assessed by reviewing the procedure revision history. If the procedure is based on some standard or framework, this is clearly evident from the documentation. The documentation indicates what standard or framework has been used and how it has been applied (which parts are adopted and which are not).
2. By interviewing the entity's personnel, the supervisory authority verifies how the cybersecurity risk management procedure is maintained and developed. The interviews show that risk management is applied to networks and information systems and the risks of their physical environment. The implementation of the risk management procedure is verified by interviewing personnel on the risk management procedure and the organisation's cybersecurity risk reporting practices. Where applicable, the personnel are able to carry out risk management as a part of their daily work. The personnel know how to report risks and incidents they detect (see section 9).

Explanations

The risks posed to the security of the networks and information systems used in the entity's activities or service provision should be identified, assessed and managed regularly and as a fixed part of the organisation's risk management. The risk management procedure should be assessed regularly and whenever changes occur in the operating environment. Risk management proportionate to the operations prevents and minimises the impacts of incidents on operations, operational continuity, service recipients and other services.

References

ISO/IEC 27001:2022 (6.1, 6.2, 8.2, 8.3)

ISO/IEC 27005:2022 (5.1, 5.2, 6.3, 6.5, 7, 8, 9, 10.4)

ISO 31000:2018

IEC 62443-2-1:2010 (4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.11, 4.2.3.12, 4.2.3.13, 4.3.2.6.3, 4.3.2.6.5, 4.3.2.6.6, 4.3.3.2.6, 4.3.4.2)
IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1, ORG 2.4, Annex B)
IEC 62443-2-4:2015 (SP 02.01, SP 03.01)
IEC 62443-2-4:2024 (SP.03.01)
NIST CSF 1.1 (ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, ID.GV-4, ID.RM-1, ID.RM-2, ID.RM-3)
NIST CSF 2.0 (ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-03, GV.RM-01, GV.RM-02, GV.RM-03, GV.PO-01, GV.PO-02)
NIST SP 800-30 rev 1 (2.1, 2.2, 2.4, 3.1, 3.2, 3.3)
NIST SP 800-37 rev 2 (2.1, 2.2, 3.1, E)
COSO Enterprise Risk Management Framework
Government’s risk management handbook for central government administration
NIS CG Reference document (3.3.1 Risk management framework)
NIS CG Implementing guidance (2.1 Risk management framework)
Tools
Julkri (HAL-06)
Kybermittari (CRITICAL-2, RISK-1, RISK-2, RISK-3, RISK-4, RISK-5, THIRD-PARTIES-2, ARCHITECTURE-1, PROGRAM-1, PROGRAM-2)

1.1.1 Risk management procedure – extended instructions

Example implementation

This recommendation is intended for the supervision of entities from whom the supervisory authority expects a higher level of maturity.

- In addition to section 1.1, the entity has created and maintained a set of risk treatment criteria appropriate for its operations. The treatment criteria define procedures applicable to the entity for the definition of different risk levels and their treatment.
- The risk treatment criteria can contain practices for the selection of risk treatment methods that can include retaining the risk and impact minimisation, elimination and outsourcing.
- The risk treatment criteria should indicate the entity’s risk tolerance and practices for accepting residual risk.

Verification

1. The supervisory authority verifies that the entity has defined and adequately documented a set of risk treatment criteria.
2. The supervisory authority ensures that the implementation of the risk treatment criteria is assessed by reviewing risk treatment and the recording of residual risks. In addition, the application of the criteria can be verified by interviewing personnel on their application.

Explanations

Criteria defined as a part of the risk management procedure help the organisation produce comparable risk assessments.

References

ISO/IEC 27001:2022 (6.1.2)

ISO/IEC 27005:2022 (6.4, 8.1)

ISO 31000:2018 (6.3.2, 6.3.4)

IEC 62443-2-1:2024 (ORG 2.1)

NIST CSF 1.1 (ID.RM-2, ID.RM-3)

NIST CSF 2.0 (GV.RM-02, GV.RM-03, GV.RM-06)

NIS CG Reference document (3.3.1 Risk management framework)

NIS CG Implementing guidance (2.1 Risk management framework)

Tools

Julkri (HAL-06)

Kybermittari (CRITICAL-2, RISK-3, RISK-4)

1.2 All-hazards approach

Example implementation

- As a part of the entity’s governance and risk management procedure, the entity has assessed risks posed to networks and information systems and their physical environment using an all-hazards approach.
- The entity has assessed the impacts of an insider threat, external threat or physical threat on the confidentiality, integrity, authenticity and availability of information or services and takes them into account in its risk management

procedure. Other such threats can include telecommunication or power failure, theft, malicious act, fire, adverse weather conditions, natural phenomena and disasters.

- In addition, the assessments can include the impact of development and maintenance measures, such as interruptions caused by application and system updates. See section 3.
- The entity has taken risks caused by other parties into account in its risk assessment, such as changes in suppliers and disruptions in supply chains. See sections 3.2 Security of the object of acquisition and 4.2 Supply chain risk management.
- The risk assessment also covers risks related to personnel and access control. See sections 6 Human resources security and cybersecurity training and 7 Access control and authentication procedures.
- Measures for ensuring the physical environment, premises security and the necessary resources are specified in section 12 Measures for ensuring the physical environment and premises security of networks and information systems and the necessary resources. With regard to the physical environment, potential considerations include the impact of possible construction work on the functioning of networks and information systems.

Verification

1. The supervisory authority reviews that the entity has observed all essential hazards in its cybersecurity risk management procedure and risk assessments. The procedure indicates that the company's governance and risk management processes take cybersecurity risks into account. The entity's risk assessment indicates that the risks posed to networks and information systems are extensive and include e.g. physical, technical and personal risks.

Explanations

The all-hazards approach aims to take into account all reasonably foreseeable threat factors posed to networks and information systems. The more significant the network or information system is to the entity, the more comprehensively its threats should be assessed. This approach can promote the entity's preparedness for different types of threats and ensure that too many threats related to a specific category are not missed.

References

ISO/IEC 27001:2022 (6.1.1)

ISO/IEC 27005:2022 (7.2)

ISO 31000:2018 (6.3.3)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1)

IEC/TR 62443-3-1:2013 (4.2.3.7)

NIST CSF 1.1 (ID.RA-5)

NIST CSF 2.0 (ID.RA-05)

NIS CG Reference document (2.2 All Hazard approach)

NIS CG Implementing guidance (2.1 Risk management framework)

Tools

Julkri (FYY-01)

Kybermittari (CRITICAL-2, RISK-1, RISK-2)

1.3 Identifying needs and activities

Example implementation

- The entity has identified the services, systems, processes and persons essential to its activities and included their security needs into risk management. This section is specified in section 5 Asset management and identifying activities important for its security.
- The entity has identified, documented and carried out risk assessment for networks and information systems, including individual devices, services or information systems whose disruption would interrupt entire operations (single point of failure, SPOF).
- A set of risk treatment criteria (see section 1.1.1) is available to support risk impact assessment.
- The entity has identified its operating environment and the security needs related to the confidentiality, integrity, authenticity and availability of data and services based on it. See section 2.3 Selection of security procedures.
- It is recommended that the entity have descriptions of the external and internal operating environment that indicate risk management requirements created by essential stakeholders and the entity itself.

Verification

1. The supervisory authority verifies from documentation that the entity has identified the most critical assets to its operations (essential services, systems, processes and persons) and contained in its risk management procedure their special features and needs for the confidentiality, integrity and availability of data and services. The identified critical activities and assets and their security needs should be evident from the risk management procedure and asset management.

Explanations

The identification of critical needs and activities and the risks posed to them helps in the selection of proportionate security measures and the approval of residual risk.

References

ISO/IEC 27001:2022 (4.1, 4.2, 6.2)

ISO/IEC 27002:2022 (5.9, 5.12)

ISO/IEC 27005:2022 (6.1, 6.2, 6.4, 7.2, 10.1)

ISO 31000:2018 (6.3.2)

IEC 62443-2-1:2010 (4.2.3.4, 4.2.3.6)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.4)

NIST CSF 1.1 (ID.RA-1)

NIST CSF 2.0 (ID.RA-01, GV.OC-02, GV.OC-03)

NIST SP 800-30 rev 1 (2.3, 3.1, 3.2)

NIST SP 800-37 rev 2 (2.3, 2.5, 3.2)

NIS CG Reference document (3.4.1 Asset classification)

NIS CG Implementing guidance (2.1 Risk management framework)

NIS CG Implementing guidance (12.1 Asset Classification)

Tools

Julkri (HAL-04)

Kybermittari (CRITICAL-1, CRITICAL-2, ASSET-1, ASSET-2, THIRD-PARTIES-1, ARCHITECTURE-1)

1.4 Cyber threat identification

Example implementation

- As a part of its cybersecurity risk management, the entity has monitored threats to the security of networks and information systems identified in section 1.3, including cyber threat information and vulnerabilities, and assessed their likelihood and impact as a part of risk assessment. In its threat analysis, the entity includes internal and external threats, negligent acts and accidents.
- The entity has assessed the likelihood of the cyber threat and the impact of its implementation. The assessment of likelihood has taken into account e.g. how

often the threat in question usually occurs, whether the threat has been implemented before in the organisation and whether a similar threat has been implemented in the sector. The assessment of likelihood should also contain threat potential, such as the attacker's ambition, motive, capability and the availability of automated malware.

- In order to assess impacts, the entity can have organised simulations and scenario exercises against threats posed to its operations to assess its preparedness and risk management capability in different imaginary situations.

Verification

1. The supervisory authority verifies that the entity can produce documentation of identified cyber threats posed to the networks and information systems and that they are taken into account as a part of cybersecurity risk management. The entity's threat analysis shows the entity's assessment of the impacts and likelihoods of threats.

Explanations

Threat identification and systematic threat analysis offer a way of identifying the most common threats and vulnerabilities to the system that pose a risk to the reliability, integrity and availability of the network or information system. Threat analysis accumulates understanding of the impacts of the threat and the likelihood of the exploitation of any vulnerabilities.

References

ISO/IEC 27002:2022 (5.7)

ISO/IEC 27005:2022 (7.2, 7.3, 9.1)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1, Annex B)

NIST CSF 1.1 (ID.RA-2, ID.RA-3)

NIST CSF 2.0 (ID.RA-02, ID.RA-03)

NIST SP 800-30 rev 1 (3.2, D, E, G)

NIS CG Implementing guidance (2.1 Risk management framework)

NIS CG Implementing guidance (2.2 Compliance monitoring)

Tools

Kybermittari (THREAT-1, THREAT-2)

Situational picture products of the National Cybersecurity Centre Finland, such as the weekly review and Cyber Weather

Cyber exercises and simulations

1.4.1 Threat analysis – extended instructions

Example implementation

This recommendation is intended for the supervision of entities from whom the supervisory authority expects a higher level of maturity.

- In addition to section 1.4, for the purposes of threat analysis, the entity has gathered threat information and vulnerability information from several different sources and analysed the likelihood of cyber threats and their impact on its operations. In its risk assessment, the entity has included risks to networks and information systems identified through threat analysis.
- The entity has monitored the state of the art of the threat environment and activities related to cybersecurity as well as developed and maintained the cybersecurity of its networks and information systems in accordance with its risk assessment.
- Threat modelling has been used to identify and document the critical data, interfaces, external dependencies and data flows of networks and information systems. Threat modelling can be carried out by using modelling methods deemed appropriate, such as STRIDE and DREAD.

Verification

1. The supervisory authority reviews the threat analyses carried out by the entity. They should show that the analysis has been based on a systematic method and that it is continuous, regular and consistent. The threat analysis has contained the collection and analysis of threat information and the charting and analysis of the entity's threat environment. The entity may have used a well-known threat modelling method, such as STRIDE or DREAD, in identifying the threats posed to the system.
2. The supervisory authority verifies the systematic nature of threat analysis by interviewing personnel on the threat analysis practices. The interviews verify that the scope of threat information gathering, the frequency of analyses, potential threats identified in the entity's threat environment and the measures agreed on the basis of threat analyses are sufficient in relation to the entity's needs.

Explanations

Threat analysis is a preparedness tool. Regularly performed threat analysis can detect changes in the threat environment and identify new threats posed to the system. Threat analysis can also exclude threats, the possible impact of which on the operating environment is small.

References

ISO/IEC 27002:2022 (5.7)

ISO/IEC 27005:2022 (7.2, 7.3, 9.1)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1)

NIST CSF 1.1 (ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6)

NIST CSF 2.0 (ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, DE.AE-04, DE.AE-07)

NIST SP 800-30 rev 1 (3.2, D, E, G)

NIS CG Implementing guidance (2.1 Risk management framework)

NIS CG Implementing guidance (2.2 Compliance monitoring)

Tools

Kybermittari (THREAT-1, THREAT-2, SITUATION-3)

Threat modelling methods: STRIDE[5], DREAD[6]

1.5 Risk treatment

Example implementation

- The entity has treated the identified risks and the significance of each risk based on the assessment. The risk treatment may include different response methods, such as risk retention, acceptance and impact minimisation, elimination and outsourcing. The entity can use a set of risk treatment criteria (see section 1.1.1) to support its risk treatment.
- The entity has defined an owner for the risk, responsible for the implementation of the selected risk management measures. If necessary, the risk owner could determine when a measure should be implemented and monitor the implementation of management measures and their effectiveness.
- The entity has identified and prioritised appropriate cybersecurity risk management measures, taking into account the risk assessment results and results from assessing the effectiveness of management measures. Where applicable, the entity may also have assessed the impact of a risk management measure and the change in operations caused by it as well as carry out a specifying risk assessment, if necessary.
- The entity has also documented the risk management measures and provided clear justification for accepting residual risks.

[5] https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

[6] https://learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers

- The entity’s top management or the risk owner has accepted the results and residual risks of the risk assessment and treatment.
- It is recommended that the risk assessment and risk management measures are reviewed and inspected regularly and whenever significant changes or significant incidents occur.
- Risk management measures have been incorporated into the operations and trained to the personnel. This is specified in sections 2.2 Personnel engagement and 6 Human resources security and cybersecurity training.

Verification

1. The supervisory authority verifies the treatment of cybersecurity risks by reviewing the risk assessment. The entity is able to produce results on the assessment and treatment of cybersecurity risks. The documents indicate the results of risk assessment, the treatment of risks and the agreed management measures in addition to any roles and responsibilities. The objective of risk management has been to treat risks in a way that their likelihood or impact is e.g. minimised, eliminated or outsourced. The documents also show residual risks, the treatment of residual risks and the justifications for their acceptance.

   In order to get evidence of the regularity of risk treatment, the supervisory authority should verify event information related to the treatment of risks. The supervisory authority can verify the entity’s risk management history e.g. by monitoring the number of risks and their effectiveness over a particular period of time. In particular, if key risks have been the target of mitigating measures, the number of risks or their effectiveness can reduce over time. If the risks or their effectiveness have not changed even after a long time, the functioning of the risk management procedure and whether correct criteria are used for measuring risks should be investigated.

Explanations

In treating risks, the effectiveness of risk management measures in relation to residual risk is assessed: is the residual risk level tolerable or are more mitigating measures needed. The aim of risk treatment is to implement such a combination of risk management measures that achieves a satisfactory balance between requirements, costs and the residual risk to security. The risk-bearing capacity and willingness defines the acceptable residual risk level.

References

ISO/IEC 27001:2022 (6.1.3, 8.1, 8.2, 8.3, 9.3)

ISO/IEC 27005:2022 (8)

ISO 31000:2018 (6.5)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1, ORG 2.4, Annex B)

NIST CSF 1.1 (ID.RA-4, ID.RA-5, ID.RA-6, ID.RM-2, ID.RM-3)
NIST CSF 2.0 (ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-2, GV.RM-3)
NIST SP 800-30 rev 1 (3.4, H)
NIST SP 800-37 rev 2 (3.3, 3.4, 3.5, 3.6)
NIS CG Reference document (3.3.1 Risk management framework)
NIS CG Implementing guidance (2.1 Risk management framework)
Tools
Julkri (HAL-06)
Kybermittari (CRITICAL-2, RISK-3, RISK-4, RISK-5, WORKFORCE-4)

1.6 Risk management effectiveness assessment and metrics

Example implementation

- As a part of its risk management, the entity has assessed the effectiveness of measures of treated risks with appropriate metrics and developed the metrics as its business and operational environment change and develop.
- The metrics can be based on a business strategy policy and the measures and procedures used in the organisation.
- The effectiveness assessment of network and information system risk management measures also takes into account sector-specific policies and rules, standards and sector-specific regulation.
- With the help of the metrics, the entity has assessed whether the listed risks are still significant, whether the impact or likelihood of the risk is still on the same level and whether the targeted measures are up to date. The assessment of the effectiveness of measures takes into account the threats posed to the entity and their foreseeable impacts, such as the most typical consequences caused by threat factors and their typical impact.
- The effectiveness of risk management is assessed regularly and whenever significant incidents or changes occur.
- As a result of risk management effectiveness assessment and measurement, the entity has modified its risk management measures to correspond with the changed situation.
- The network and information system cyber security management implemented by the entity and its implementation have been reviewed and assessed independently. The entity has created processes for independent reviews, and the management should plan and implement them regularly.
- Persons carrying out the review are independent of the entity's operations and have the appropriate competence and experience to carry out the

assessment. The review may have been carried out as a self-evaluation or by a managed security service provider.
- The assessment results have been reported to management. The corrective measures are implemented and the residual risks accepted in accordance with the entity's risk criteria.

Verification

1. The supervisory authority reviews the metrics defined by the entity. The metrics should be applicable to the effectiveness assessment of risk management measures so that the functionality of selected measures can be measured and improved, if necessary. The plans must indicate the entity's review processes and plans. The entity is able to present reports of reviews and assessments.
2. The supervisory authority interviews the entity's personnel and assesses the use and functionality of the metrics in practice. As necessary, the metrics should act as a management tool on the cybersecurity risk management situation. The supervisory authority interviews the entity on risk treatment. The interviews should indicate the start of risk management measures based on the metrics. The entity can also be requested to present its risk treatment documentation that should show the history of measures.

Explanations

Risk management measures should be able to create additional value, which is why they must be assessed regularly. The continuously changing threat environment and technology create the greatest challenges to keeping the selected measures up to date. For this reason, risk management and effectiveness assessment should be carried out throughout a risk's lifecycle. Independent assessment ensures the effectiveness and up-to-dateness of an organisation's risk management.

References

ISO/IEC 27001:2022 (6.1.1, 6.1.3, 6.2, 9.1, 9.2, 9.3, 10.1)

ISO/IEC 27002:2022 (5.31, 5.35, 5.36, 8.34)

ISO/IEC 27005:2022 (8.3, 8.6, 9.2, 10.1, 10.5 10.6, 10.8)

ISO 31000:2018 (6.6)

IEC 62443-2-1:2010 (4.4.2.3, 4.4.3)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1, ORG 2.4, Annex B)

IEC 62443-3-3:2013 (SR 3.9)

NIST CSF 1.1 (ID.RM-1)

NIST CSF 2.0 (ID.IM-01)

NIST SP 800-30 rev 1 (3.4)

NIST SP 800-37 rev 2 (3.6, 3.7)

NIS CG Reference document (3.3.2 Policies and procedures to assess the effectiveness of security measures)

NIS CG Reference document (3.3.4 Independent review of information and network security)

NIS CG Implementing guidance (2.2 Compliance monitoring)

NIS CG Implementing guidance (2.3 Independent review of information and network security)

NIS CG Implementing guidance (7. Policies and procedures to assess the effectiveness of security measures)

Tools

Kybermittari (CRITICAL-2, RISK-4, RISK-5, PROGRAM-2)

1.6.1 Risk management effectiveness assessment and metrics – extended instructions

Example implementation

This recommendation is intended for the supervision of entities from whom the supervisory authority expects a higher level of maturity.

- In addition to section 1.6, the entity has drawn up a policy for assessing the effectiveness of cyber security risk management measures.
- The entity has introduced a reporting system to monitor the implementation of the cybersecurity risk management measures of the NIS2 Directive and their effectiveness. The reporting system has been prepared to match the size and organisational structure of the entity, the operating environment and the threat environment.
- In order to measure the effectiveness of risk management measures, the entity may have defined matters such as the following:
  - risk management measures to be monitored and measured and their higher-level objectives.
  - monitoring processes and methods
  - when the monitoring and measuring should be carried out
  - who monitors and measures
  - when the results of monitoring and measurements should be analysed and assessed and
  - who analyses and assesses these results.

- The entity has included cyber security audits and information security testing of networks and information systems into its risk management effectiveness procedures.
- The entity has assessed the implementation of the risk management procedure in its organisation.

Verification

1. The supervisory authority reviews the policy and reporting system drawn up by the entity for the effectiveness assessment of cybersecurity risk management measures. The reporting system indicates the risk management plan implemented by the organisation, including any responsible persons. It can also indicate the implementation, effectiveness and up-to-datedness of the cybersecurity risk management measures.

Explanations

The reporting system can help the entity monitor the implementation of the NIS2 Directive’s cybersecurity risk management measures in its organisation.

References

ISO/IEC 27001:2022 (6.1.1, 6.2, 9.1, 9.2)

ISO/IEC 27002:2022 (5.31, 5.35, 5.36)

ISO/IEC 27005:2022 (8.3, 8.6, 9.2, 10.1, 10.5 10.6, 10.8)

IEC 62443-2-1:2010 (4.4.2.3, 4.4.4)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1, ORG 2.4)

IEC/TR 62443-3-1:2013

NIST CSF 1.1 (PR.IP-8)

NIST CSF 2.0 (ID.IM-03)

NIS CG Reference document (3.3.2 Policies and procedures to assess the effectiveness of security measures)

NIS CG Reference document (3.3.3 Compliance monitoring)

NIS CG Implementing guidance (2.2 Compliance monitoring)

NIS CG Implementing guidance (7. Policies and procedures to assess the effectiveness of security measures)

Tools

Kybermittari (CRITICAL-2, RISK-4, RISK-5, PROGRAM-1, PROGRAM-2)

2 Information security policy of networks and information systems

These recommendations are based on Article 21(2)(a) of the NIS2 Directive. The national implementation of this point is laid down in section 9, subsection 2, paragraph 2 of the Cybersecurity Act and in section 18 c, subsection 1, paragraph 2 of the Information Management Act.

1. **Information security policies and procedures**: These can concern administrative, personnel, equipment, software, network and dataset security and the security of operations and the physical environment. The ISO/IEC 27001 standard also refers to similar principles as the information security policy. The entity should for example have written information security policies and procedures for networks and information systems. If such are applied, they should be proportionate to the entity's needs and maintained up to date. (See sections 2.1 and 2.1.1.)

2. **Engaging the personnel**: In addition, one objective of risk management could be that the entity's personnel should know the adopted security procedures and commit to complying with them. (See section 2.2.)

3. **Selection of security procedures**: The selection of appropriate procedures could take into account e.g. business needs and identified cybersecurity risks. (See section 2.3.)

2.1 Information security policies and procedures

Example implementation
• The entity has drawn up written information security policies and procedures for networks and information systems. In connection with standards, these are sometimes referred to as the information security policy. The entity's top management has approved the information security policies and procedures and monitors their implementation. • The information security policies and procedures indicate the security objectives of networks and information systems, the entity's commitment to comply with the applicable cyber security requirements and commitment to the continuous improvement of policies and procedures. • The information security policies and procedures are put into practice among personnel and any third parties, such as subcontractors, suppliers and service providers (see section 2.2). • In drawing up the information security policies and procedures, the entity may have used as support generally accepted standards, cybersecurity frameworks or the sector's best practices on information security policy. • Information security policies and procedures concern administrative, personnel, equipment, software, network and dataset security and the security of operations and the physical environment. • In its information security policy for networks and information systems, the entity has included the applicable cybersecurity measures of the NIS2

Directive, such as access control, asset management, secure device configuration, network security, backup management, cryptography, management of disruptions, vulnerability management and physical security.

- As a part of its information security policies and procedures, the entity has presented the roles, responsibilities and authorisations related to security (see section 6.1).
- In selecting information security policies and procedures, the entity has taken business needs and the identified cybersecurity risks into account. The policies and procedures are suitable for the entity and proportionate to the risk posed to the operations.
- Information security policies and procedures for networks and information systems have been kept up to date with regular reviews. Regular reviews have been held at previously agreed times (e.g. once a year) or whenever significant changes or significant incidents have occurred.
- The practical applicability of policies and procedures has been assessed with reviews and they have been adapted to correspond to the entity’s needs. The entity may also have acknowledged the change in the operating environment and threat environment as well as development in cybersecurity technologies.

Verification

1. The supervisory authority verifies that the entity can present documents on the information security policies and procedures for networks and information systems. Information security policies and procedures are sufficiently comprehensive and include all sections applicable to the entity’s needs. The documents clearly indicate the entity’s cybersecurity objectives, principles and implementation.

   To verify the proportionality of policies and procedures, documents should indicate the link between policies and business operations and the cybersecurity risk management implemented by the entity.

   The policies and procedures are up to date and they have been maintained. This can be verified by inspecting the update history of the documents. The update history indicates that the documents have been reviewed regularly and updated as necessary as well as after significant changes or incidents. The entity can present plans and documentation on the reviews of the policies and procedures.
2. The supervisory authority assesses the entity’s information security policies and the proportionality and up-to-dateness of its procedures by interviewing the entity’s personnel on how aware they are of the policies and procedures and how they are implemented and complied with in practice.

Explanations

Information security policies and procedures act as the foundation for an organisation’s security culture and the management and implementation of network and information system security, including people, processes and technologies. Up-to-date and proportionate policies and procedures support everyday work and enable the implementation of the organisation's security objectives.

References

ISO/IEC 27001:2022 (4.1, 4.2, 5.2, 5.3)

ISO/IEC 27002:2022 (5.1, 5.36)

IEC 62443-2-1:2010 (4.3.2.2.1, 4.3.2.2.2, 4.3.2.6)

IEC 62443-2-1:2024 (ORG 1.1, ORG 1.3, ORG 1.6, ORG 2.4)

IEC 62443-2-4:2015 (SP 01)

IEC 62443-2-4:2024 (SP.01.05, SP.01.06, SP.01.07, SP.03.01)

NIST SP 800-53 Rev. 5

NIST CSF 1.1 (ID.GV-1, ID.GV-3, ID.BE-3)

NIST CSF 2.0 (GV.OC-01, GV.OC-03, GV.PO-01, GV.PO-02)

NIS CG Reference document (3.2.1 Network and information security policy)

NIS CG Implementing guidance (1.1 Policy on the security of network and information systems)

Tools

Julkri (HAL-01)

Kybermittari (CRITICAL-2, PROGRAM-1, PROGRAM-2, General management measures)

2.1.1 Information security policy and procedures – extended instructions

Example implementation

This recommendation is intended for the supervision of entities from whom the supervisory authority expects a higher level of maturity.

- In addition to section 2.1, the entity has, if necessary, prepared separate policies for each area. Policies may have been drawn up on matters such as vulnerability management, supply chain security, security testing, the effectiveness assessment of risk management measures, encryption, access management, use of administrator accounts and elevated privileges, management of information and assets, and the use of external storage media.
- As a part of its information security policies and procedures, the entity may have drawn up more specific procedures and instructions for different areas,

such as access control, asset management, secure device configuration, network security, backup management, cryptography, management of disruptions, vulnerability management and physical security.

- The need for more detailed procedures and instructions can arise e.g. from the size of the area or the frequency of the need for updates. As a part of its asset management, for example, the entity may have the need to instruct on the secure transfer of devices, software and data to external premises as regards critical assets.

Verification

1. The supervisory authority reviews the sector-specific policies and detailed instructions on security drawn up by the entity.

Explanations

References

ISO/IEC 27002:2022 (5.1, 5.37)

IEC 62443-2-1:2024 (ORG 1.1, ORG 1.3, ORG 1.6, ORG 2.4)

NIST CSF 1.1 (ID.GV-4)

NIST CSF 2.0 (GV.OC-4)

NIS CG Implementing guidance (1.1 Policy on the security of network and information systems)

Tools

Kybermittari (CRITICAL-2, PROGRAM-1, General management measures)

2.2 Engaging the personnel

Example implementation

- The entity’s management has ensured that the entire personnel and any third parties comply with the information security policies and procedures for networks and information systems (see section 2.1) and the detailed procedures and instructions drawn up for other areas (see section 2.1.1).
- The entity has regularly communicated its information security policies and procedures to personnel and third parties.

- The information security policies and procedures are included in trainings organised by the entity. More information on training in sections 6.5 Personnel training and 11.1 Fundamental information security practices.
- The entity has operating models in case of activities in violation of the information security policies and procedures. This section is specified in section 6.1 Human resources security.

Verification

1. The supervisory authority reviews the practices of communicating or training information security policies and procedures to the personnel. This can be e.g. a webpage, training material or similar presented by the entity and available to the entire personnel. The supervisory authority may also inspect a procedure drawn up by the entity for committing personnel to complying with the cybersecurity procedures. For example, this can mean monitoring the training on information security policy.
2. The supervisory authority verifies with interviews that the personnel is familiar with the information security policies and procedures. The interviews indicate that personnel operate in compliance with the shared policies and procedures. Personnel are aware of where to find the written material.

Explanations

The adoption of information security policies and procedures comes down to the competent personnel. Training helps every member of personnel understand the significance of their task in the overall security of the organisation.

References

ISO/IEC 27001:2022 (5.2, 7.3, 7.4)

ISO/IEC 27002:2022 (5.4, 6.3)

IEC 62443-2-1:2024 (ORG 1.1, ORG 1.4, ORG 1.5, ORG 1.6)

NIST CSF 1.1 (ID.GV-2, ID.AM-6, DE.DP-1, PR.AT-5)

NIST CSF 2.0 (GV.RR-02, PR.AT-02)

NIS CG Reference document (3.2.2 Roles, responsibilities and authorities)

NIS CG Implementing guidance (1.2 Roles, responsibilities and authorities)

Tools

Julkri (HAL-02, HAL-03, HAL-12, HAL-13)

Kybermittari (CRITICAL-2, WORKFORCE-1, WORKFORCE-2 WORKFORCE-3, WORKFORCE-4, General management measures)

2.3 Selection of security procedures

Example implementation

- In selecting network and information system security procedures, the entity has taken into account its business needs and identified cybersecurity risks (see section 2.1). The business needs have included e.g. the requirements of key stakeholders, sector-specific regulations and the entity's standards and certifications.
- The security procedures have been selected on the basis of identified security needs. In order to select proportionate security procedures, the entity has listed its assets, carried out a risk assessment and classified the assets in accordance with their security needs (e.g. confidentiality, integrity, authenticity and availability). If necessary, the entity may also have included authenticity, non-repudiation and authentication. The asset list and asset classification are specified in section 5.2.
- The entity has updated and developed the security procedures regularly and in connection with significant changes, such as changes in the operating environment or threat environment or after incidents.

Verification

1. The supervisory authority reviews the documented information security policies and procedures. Among other things, the documents include requirements posed by the entity's business operations and sector-specific regulation. The selection of security procedures indicates the entity's business needs, standards and certifications included in its management system, sector-specific regulation and the needs of its key stakeholders. The selection of procedures also indicates the identified cybersecurity risks, and they are clearly linked to risk assessment, selection of risk management measures, their effectiveness assessment and metrics as well as asset management and its listing and classification.

Explanations

References

ISO/IEC 27002:2022 (5.12, 5.36)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.1)

NIST CSF 1.1 (ID.GV-1, ID.GV-3, ID.GV-4)

NIST CSF 2.0 (GV.OC-01, GV.PO-01)

NIS CG Reference document (3.2.1 Network and information security policy)

NIS CG Implementing guidance (1.1 Policy on the security of network and information systems)
Tools
Julkri (HAL-05) Kybermittari (ASSET-1, ASSET-2, PROGRAM-1, PROGRAM-2, ARCHITECTURE-1)

3 Security in network and information systems acquisition, development and maintenance and the necessary procedures for vulnerability handling and disclosure

These recommendations are based on Article 21(2)(e) of the NIS2 Directive. The national implementation of this point is laid down in section 9, subsection 2, paragraph 3 of the Cybersecurity Act and in section 18 c, subsection 1, paragraph 3 of the Information Management Act.

1. **Network and information system security throughout their lifecycle**: The entity should aim to maintain a sufficient level of security of networks and information systems throughout their lifecycle. (See sections 3.1 and 3.1.1.)

2. **Security in object acquisition**: Acquired systems and other acquisitions should be sufficiently secure based on the needs of the operations, for example in terms of integrity, availability and confidentiality. System acquisition could pay attention to the ability to protect itself against the most common types of attacks. (See section 3.2.)

3. **System hardening**: The secure configuration, i.e. settings of systems, could be specified, documented and maintained throughout their lifecycle, and special attention could be paid to this matter during updates in particular. (See sections 3.3 and 3.3.1.)

4. **Change and update management**: In terms of configuration and software updates, the aim could be to have them be documented, planned in accordance with change management processes, comprehensive and timely in terms of the characteristics of the target and the criticality of updates. For example, the making of unauthorised or malicious changes could be blocked. (See sections 3.4 and 3.4.1.)

5. **Security testing**: The most critical targets in terms of security could be identified separately, and their security could be ensured e.g. by conducting regular reviews of processes or technical testing. (See section 3.5.)

6. **Vulnerability handling and disclosure**: The entity could for example focus on having a reporting channel for discovered vulnerabilities, accompanied by predefined procedures and practices for processing the reports. (See section 3.6.)

7. **Security of supplied services**: The entity could for example ensure that the secure configuration of these networks and information systems is possible and that appropriate security updates are produced for them. (See section 3.7.)

8. **Structural security of networks**: In terms of networks, the secure structure of the network should be ensured. For example, targets critical

to activities should be identified and protected as necessary with up-to-date technical means, e.g. by segmentation. (See section 3.8.)

9. **Malicious traffic protections**: It should be possible to detect and prevent any malicious traffic. (See section 3.9.)

3.1 Network and information system security throughout their lifecycle

Example implementation

This section extends section 11.3 on baseline information security practices.

- The entity has procedures in place for the protection of networks and information systems throughout their lifecycle. The lifecycle approach must take into account both design, commissioning, operation and decommissioning. Asset lifecycles are specified in section 5.3 Using the asset list.

Verification

1. The supervisory authority verifies by reviewing documentation that the entity protects its networks and information systems. The documentation indicates how they are protected throughout their lifecycle. In terms of the lifecycle, the design, commissioning, operation and decommissioning are taken into account. The adoption of protections can be verified e.g. by using an asset catalogue and changes made to it as well as other evidence supplied by the entity, such as screenshots and interviews. Among others, the reviewed protections include sections 3.3 System hardening, 3.4 Change and update management, 3.8 Structural security of networks and, where applicable, 11 Baseline information security practices.
2. By reviewing configurations and status information supplied by the entity (e.g. DNS, DHCP log data and records, other hardware, network device configuration management or versions) and by comparing them to documentation, the supervisory authority can verify that the procedures have been executed. The information should show that there are no decommissioned devices in the environment or devices whose commissioning process has not been followed through without a justified reason. Special attention should be paid to devices that are not necessarily directly visible in the information of the network and information system. These can typically include virtual machines and services, such as interfaces, in external cloud services, and these may need to be checked from the user interface of the service in question. If the entity uses cloud services or other virtual platforms, the review should cover them as well.
3. The supervisory authority can expand the above-mentioned review with active scanning or data traffic recording.

Explanations

The erosion of security over time can cause vulnerabilities that are not identified. It is common that devices, virtual machines and applications are not removed after they are no longer needed. Targets that are not properly maintained often cause severe vulnerabilities.

References

IEC 62443-2-1:2024 (NET 1.1, NET 1.2, COMP 1.1, CM 1.1, CM 1.3, CM 1.4, ORG 2.3)

NIST CSF 1.1 (PR.AC-5, PR.DS-3)

NIST CSF 2.0 (PR.IR-01)

NIST SP 800-30 rev 1 (F)

NIST SP 800-37 rev 2

NIS CG Implementing guidance (6.1 Security in acquisition of ICT services, ICT systems or ICT products)

Tools

Julkri (HAL-05.1, TEK-17.2)

Kybermittari (ASSET-1, ASSET-2, ASSET-3, ASSET-4)

3.1.1 Secure product development – extended instructions

Example implementation

This recommendation is intended for the supervision of entities from whom the supervisory authority expects a higher level of maturity.

- The entity has produced its applications and systems in accordance with secure development practices, for example by using practices defined by SDLC (secure/software development life cycle) or SSDLC (secure software development life cycle). The practices apply to all stages of the development cycle (definition, design, development, implementation, testing, commissioning and maintenance).
- Cybersecurity requirements have been analysed in the definition and planning stages.
- The measures of secure product development have been defined. This includes secure architectural choices (e.g. zero-trust), secure programming practices, use of secure supply chains, choice of secure components.
- The entity has defined security requirements for the development environment.

- Security testing processes have been defined and implemented. One option for security testing is an automatic workflow (DevSecOps), which includes various security tests, such as static application security testing (SAST), dynamic application security testing (DAST), review practices, security scans and penetration testing.
- The security requirements of the data used in testing have been taken into account in the operations. Any confidential data is protected at least to a similar extent as in production systems, or it has been sanitised, anonymised or pseudonymised.

Verification

1. The supervisory authority reviews the entity's documentation on how the entity implements secure product development. Secure product development measures depend heavily on the product's properties, and verification is proportionate to these properties. Product development often utilises well-known good practices, such as SDLC or SSDLC. Documentation indicates how the entity ensures the cyber security of the products it delivers, for example in the definition, design, development, implementation and testing stages.
2. The supervisory authority verifies the development practices, for example by reviewing the entity's development infrastructure. The development infrastructure usually includes different platforms for development, testing, quality assurance and pre-production, and so on. In addition, security testing is usually carried out on the product during development. Any source code and configurations have been created securely, for example by importing external libraries according to specified procedures, and the source code has been created with procedures that allow only identified and authorized users to make changes. If the development also covers equipment, the related supply chains should be reviewed and the security of the equipment tested.

Explanations

Product testing is a way to ensure that a product is as secure as possible. It ensures that weak implementations are not delivered forward and that delivered products are compatible with the Cybersecurity Act. Testing is also a way to discover vulnerabilities before the attacker. In addition, comprehensive testing and processing the test results can provide a realistic image of the state of security and shine a light on possible weaknesses, which allows compensating for them with appropriate measures.

References

ISO/IEC 27002:2022 (8.25, 8.28, 8.31)

IEC 62443-2-1:2010 (4.3.4.3)

IEC 62443-2-1:2024 (ORG 2.3)

IEC 62443-4-1:2018

NIST CSF 1.1 (PR.IP-2)

NIST CSF 2.0 (ID.AM-08)

OWASP Application Security Verification Standard

OWASP Top Ten

NIS CG Reference document (3.9.7 Secure development life cycle)

NIS CG Implementing guidance (6.2. Secure development life cycle)

Tools

Julkri (TEK-14)

Kybermittari (ARCHITECTURE-4, THIRD-PARTIES-2)

3.2 Security in object acquisition

Example implementation

- The entity must ensure that services, systems, products and resources acquired from a third party are sufficiently secure in relation to the needs of the operations in terms of integrity, availability and confidentiality, among other factors, and can protect themselves against the most common types of attacks.
- The entity must ensure that a product or service can be securely configured and that security updates are available for the object throughout its intended lifecycle if configuration and updating are essential for the object.
- If the object of acquisition is e.g. a service or resource, the security, quality and availability of the object throughout its lifecycle must be ensured. In particular, the entity must prepare for any changes in relation to the service supplier so that the service or resource can be transferred or returned to be managed by the entity itself, if necessary. If necessary, the entity also needs to prepare for changes in ownership.
- Entities can try to ensure the security of acquisitions e.g. by contractual means, studying the product’s properties, requiring certifications, ensuring the reliability of the supplier and preparing for risks. The security requirements are defined already during the initial stages of acquisition, and the requirements are provided to the suppliers and included in the contract.
- The entity has ensured that the acquired object has documentation that covers its content and its secure configuration and use.
- The security of the acquired object is ensured throughout its lifecycle. This can include e.g. updates to the contract, updates to maintenance and regular security inspections.
- In addition to the acquisition process, the object of acquisition can also be ensured with acceptance tests (factory acceptance test, site acceptance test).

- The entity has also taken security-related aspects into account during the acquisition process. More information on secure data processing in section 11.8.

Verification

1. The supervisory authority verifies that the entity has practices in place for ensuring the security of acquired objects (see the example implementations above). The security of acquisition objects should particularly be ensured in case of objects whose cyber security weaknesses e.g. vulnerabilities could cause risks to the entity's operations. Ensuring the security of the acquired object usually requires a comprehensive acquisition process that takes security matters into account. The entity has ensured that the secure configuration of acquired objects is possible and that security updates are produced for them for a sufficiently long period of time. Furthermore, the objects of acquisition should be able to protect themselves at least against the most common types of attacks.

   The security of the objects of acquisition can be approached e.g. through the acquisition process. The acquired object can be e.g. a device, service or resource. A typical method of ensuring security can include e.g. various testing and investigating methods in connection with acquisition, measures related to the object lifecycle management and preparations for various threats and changes in the threat environment with security agreements. In other words, it should be ensured that the entity's acquisition process supports security needs, is complied with and is taken into account in risk assessment. The implementation of the acquisition process can be verified e.g. by studying acquisition documents, conducting interviews and examining the current state of acquired objects. Acquisition should pay particular attention to the special needs of the entity. These can include e.g. geographical requirements, needs related to resources and service promises, possibility of transferring services, the security features of products and services and service updates and lifecycle.

Explanations

In addition to financial risk, failed acquisitions can also entail cybersecurity risks. For example, an unsecured product or service can compromise the rest of the information system and network. If the acquisition has been carried out with insufficient arrangements, the likelihood of many threats increases, such as vendor lock-in, threats caused by changes in ownership, loss of skills and loss of the object of acquisition.

References

ISO/IEC 27002:2022 (5.21, 5.23)

IEC 62443-2-1:2010 (4.3.4.3.1, 4.3.4.3.4)

IEC 62443-2-1:2024 (ORG 1.6, ORG 2.3)

IEC 62443-2-4:2015

IEC 62443-3-3:2013 (SR 3.4, 3.5)

NIST CSF 1.1 (ID.SC-1, ID.SC-3, ID.SC-4)

NIST CSF 2.0 (GV.SC-01, GV.SC-05, GV.SC-07)

NIST SP 800-161 rev 1 (3.1)

NIS CG Reference document (3.9.6 Security in acquisition of ICT services, ICT systems or ICT products)

NIS CG Implementing guidance (6.1 Security in acquisition of ICT services, ICT systems or ICT products)

Tools

Julkri (HAL-16, HAL-16.1)

KYBERMITTARI (THIRD-PARTIES-1, THIRD-PARTIES-2, ARCHITECTURE-3, ARCHITECTURE-4)

Recommendation on information security in procurement issued by the Information Management Board for a target audience of information management units and public authorities: https://urn.fi/URN:ISBN:978-952-367-645-9

3.3 System hardening

Example implementation

This section extends section 11.10 on fundamental information security practices.

- The entity has defined the processes and tools for creating secure configuration for devices, applications, services and networks and maintaining it throughout their lifecycle.
- As a part of risk assessment, at least those objects whose functioning is essential due to security, operating capability, security of supply or other risk management reasons are defined.
- A configuration that promotes their cyber security has been created for these objects. Safe configuration means e.g. removing clear high-risk features, turning off or removing extraneous services, components and ports, changing default values such as default passwords and adopting security functions.
- If a secure configuration cannot be produced to the object or it is a heightened security risk to the network and information system, it is protected by other risk management means.
- Security parameters related to configuration, such as passwords, have been stored securely and they are available and can be changed easily.

Verification

1. The supervisory authority verifies that the entity defines, documents and maintains the secure configuration of systems. The verification of secure configuration can use existing documentation and configuration files. These show that the entity consistently removes extraneous settings, changes unsafe default settings and enables possible security features. In addition, the supervisory authority reviews the entity's configuration practices in connection with changes, such as updates. Typical types of hardening include changing default passwords, removing extraneous services and features (e.g. extra control connections), removing extraneous devices and components, switching to secure traffic protocols (e.g. from unencrypted into encrypted) and enabling security settings (e.g. firewall, malware scanning, automatic updates).
2. The supervisory authority reviews the hardening practices by getting to know the configurations of different devices, software and services with the entity's assistance. The authority may also request screenshots of configurations and make use of interviews. In case of a great number of targets, a comprehensive sampling that includes a variety of target types should be used. The targets that are key for operations and security should be selected for this purpose.

Explanations

References

ISO/IEC 27002:2022 (8.9, 8.20, 8.21)

IEC 62443-2-1:2024 (NET 1.1, ORG 1.1, CM 1.1, CM 1.2, CM 1.3, CM 1.4, COMP 1.1)

IEC 62443-2-4:2015 (SP 06.02)

IEC 62443-2-4:2024 (SP.03.02, SP.03.05, SP.03.08, SP.03.09, SP.06.03, SP.07.04, SP.08.02, SP.09.02 RE(4), SP.09.03, SP.09.04, SP.09.07, SP.09.09, SP.10.02)

IEC 62443-3-3:2013 (SR 7.6)

NIST CSF 1.1 (PR.IP-1, PR.IP-3)

NIST CSF 2.0 (ID.RA-07, PR.PS-01)

NIS CG Reference document (3.9.1 Configuration management)

NIS CG Implementing guidance (6.3. configuration management)

Tools

Attack surface mapping Hyöky.fi

Julkri (TEK-10)

Kybermittari: ASSET-1, ASSET-3, ASSET-4, ARCHITECTURE-3

3.3.1 System hardening of the network and information system is implemented systematically and comprehensively – extended instructions

Example implementation

This recommendation is intended for the supervision of entities from whom the supervisory authority expects a higher level of maturity.

- Secure configuration complies with known configuration or hardening references, among others. Configurations are defined comprehensively for the different targets in the information system.
- Secure configurations have been imported into systems in a controlled manner. This can mean e.g. a centralised configuration management system.

Verification

1. The supervisory authority verifies that the entity has selected hardening references for the hardening of its devices and services, if necessary. Furthermore, the entity has documented any deviations from these. Hardening references are offered e.g. by CIS, DISA and software suppliers. The features used often cause deviations from the reference implementations. The reference selections and deviations made can be written specifications that can be reviewed. The implementation of hardening can be reviewed e.g. by inspecting the configurations of devices, applications and services. If a centralised configuration management system is used, the configurations imported to targets can be checked from there. Configuration management system logs can be used to inspect the functioning and comprehensiveness of the configuration system.

Explanations

Hardening is one of the most efficient ways of reducing the attack surface of an individual application or device. Even simple hardening can achieve visible results, but in reality, extensive products in particular have huge numbers of features whose removal or configuration change can bring benefits. The use of existing hardening and configuration instructions may be appropriate for this purpose.

References

ISO/IEC 27002:2022 (8.9, 8.20, 8.21)

IEC 62443-2-1:2024 (NET 1.1, ORG 1.1, CM 1.1, CM 1.2, CM 1.3, CM 1.4)

IEC 62443-2-4:2015 (SP 06.02)

IEC 62443-2-4:2024 (SP.03.02, SP.03.05, SP.03.08, SP.03.09, SP.06.03, SP.07.04, SP.08.02, SP.09.02 RE(4), SP.09.03, SP.09.04, SP.09.07, SP.09.09, SP.10.02)

IEC 62443-3-3:2013 (SR 7.6)

NIST CSF 1.1 (PR.IP-1, PR.IP-3)

NIST CSF 2.0 (ID.RA-07, PR.PS-01, PR.PS-03)

NIS CG Reference document (3.9.1 Configuration management)

NIS CG Implementing guidance (6.3. configuration management)

Tools

CIS Benchmark

DISA STIG

Attack surface mapping Hyöky.fi

Julkri (TEK-10)

Kybermittari (ASSET-3, ASSET-4, ARCHITECTURE-3)

3.4 Change and update management

Example implementation

This section extends section 11.9 on baseline information security practices.

- The entity has documented its change management procedure and the related process. The change management process can contain a description of the approval of changes, a description of the speed of changes to ensure their timeliness and a description of replacement measures if a change cannot be implemented.
- Changes, fixes and maintenance to the network and information system have been implemented in accordance with the change management procedure. The change management procedure is based on the entity’s policies concerning security.
- The change management procedure describes the methods and obligations related to making emergency changes, including e.g. documentation requirements and measures of ensuring security.

- Changes made via remote management have used approved procedures that prevent unauthorised changes.

Verification

1. The supervisory authority verifies the entity's documentation in terms of change management. The entity has a written description e.g. of how configuration and software updates and changes are taken into different parts of the system comprehensively and in a timely fashion based on the criticality of the update and characteristics of the system. The procedure should describe the change management process describing e.g. how changes are approved, how they can be traced after the fact and how quickly a change must be taken into the target systems. Any replacement measures must also be described if the change cannot be implemented. Change management can be implemented lightly based on risk management, depending also on the size of the entity's network and information system. If necessary, change management also includes a description of how the functionality and security of changes is ensured, particularly if the system has particularly high requirements for availability and confidentiality. Change management should also describe the methods complied with in connection with emergency changes.
2. The supervisory authority verifies the implementation of change management e.g. by utilising change-related events, tickets and log entries. Interviews can also be used. The implementation of the change management procedures can also be verified by comparing configuration and version data and the change log to the running configuration and version at different targets.

   The supervisory authority verifies the implementation of updating practices e.g. by requesting data (event log, screenshots and similar) of the updates that have taken place.
3. The supervisory authority verifies the implementation of updating practices e.g. by making use of scanning. Any exceptions are investigated with the entity's assistance or from documentation.

Explanations

Change and update management can prevent the exploitation of many vulnerabilities. Rapid reaction to the need for updates on the outer edges of networks and information systems in particular is an important defence. However, updates in themselves do not always produce a perfect end result. For example, the network and information system may contain some other product where the same vulnerability remains without an up-to-date patch. In such cases, knowledge of the products and replacement measures targeted based on that knowledge, such as various restrictions and control, may be of help. Product acquisition and supply chain management can also be important. Sometimes a vulnerability e.g. in a library being used is not known to the supplier for some reason or another, in which case the supplier does not react to the need for it to be fixed. Such situations should be taken into account in the case of security-critical products in particular. For example, an organisation can keep records on the dependencies of its critical products (software bill of materials, SBOM) and react as necessary to detected deficiencies by updating end products.

References

ISO/IEC 27001:2022 (6.2, 6.3, 8.1)

ISO/IEC 27002:2022 (7.13, 8.19, 8.32)

IEC 62443-2-1:2010 (4.3.4.3.2, 4.3.4.3.3, 4.3.4.3.5)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.4, AVAIL 1.2, CM 1.4)

IEC 62443-2-4:2024 (SP.11.01, SP.11.02, SP.11.06)

IEC 62443-3-3:2013 (SR 3.4)

NIST CSF 1.1 (PR.AC-3)

NIST CSF 2.0 (PR.AA-03, PR.AA-05, PR.IR-01)

NIS CG Reference document (3.9.2 Change management and maintenance)

NIS CG Implementing guidance (6.4. Change management, repairs and maintenance)

Tools

Attack surface mapping Hyöky.fi

Julkri (TEK-17)

Kybermittari (ASSET-3, ASSET-4, ARCHITECTURE-3l,

ARCHITECTURE-5h)

3.4.1 Change and update management is systematic – extended instructions

Example implementation

This recommendation is intended for the supervision of entities from whom the supervisory authority expects a higher level of maturity.

- The entity has procedures in place regarding changes made to the networks and information systems. The procedures take lifecycle stages from design to decommissioning into account.
- The procedures cover planned and unplanned changes and development, if possible.
- The entity has channels for monitoring vulnerabilities affecting its network and information system. The channel can be a national CSIRT function (CERT-FI) and the notification channels of service or device suppliers.

- The security updates critical to the cybersecurity of the entity's network and information system have been installed without delay. If this is not possible, replacement measures have been adopted immediately.
- Records have been made of emergency changes to indicate the reason for bypassing normal procedure. If the testing required under normal circumstances has been bypassed in connection with an emergency change, testing has been carried out after the fact as extensively as possible.
- The changes have been tested and inspected before being introduced into production systems whenever possible.
- If necessary, a security impact analysis has been carried out on the change, which can also be implemented in a separate testing system.
- Changes are imported into systems in an organised manner. Changes can be imported e.g. with the RFC process where responsibilities and procedures are specified.
- The change management procedures can contain the following stages among others: risk analysis, classification and prioritisation and definition of tests to be performed, roll-back, change documentation and approval.
- Changes, maintenance and fixes have been carried out and recorded with the tools specified.

Verification

1. The supervisory authority reviews the entity's documentation describing change management to ensure that the overall management of changes and updates is controlled, systematic and organised. The entity has specified the channels to be monitored in order to detect necessary security updates and needs for changes as well as procedures for analysing these updates and changes and, if necessary, taking them to the necessary targets without delay. In particular, changes affecting cybersecurity are tested in terms of functionality and cybersecurity e.g. in a test system or otherwise before they are applied to the target. The supervisory authority reviews that there is a systematic manner available for approving, implementing and recording changes. Change management documentation also describes how changes and updates made via remote management are controlled. This applies in particular to changes performed by third parties.
2. In order to review the implementation of change management, the supervisory authority may use the extended methods described in point 2 of Verification in section 3.4 so that change management corresponds with the documentation. There must be responsible persons for different measures who know and follow the process.

Explanations

References

ISO/IEC 27001:2022 (6.2, 6.3, 8.1)

ISO/IEC 27002:2022 (7.13, 8.31, 8.32)

IEC 62443-2-1:2010 (4.3.4.3.2, 4.3.4.3.3, 4.3.4.3.5, 4.3.4.3.7)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.3, ORG 2.4, AVAIL 1.2, CM 1.4)

IEC 62443-2-4:2015 (SP 11)

IEC 62443-2-4:2024 (SP.02.01, SP.03.01, SP.03.02, SP.03.05, SP.03.09, SP.07.04, SP.08.02, SP.08.04, SP.09.09. SP.10.02, SP.11.02, SP.11.06)

IEC 62443-3-3:2013 (SR 3.4)

NIST CSF 1.1 (PR.AC-3, ID.AM-1)

NIST CSF 2.0 (PR.AA-03, PR.AA-05, PR.IR-01, PR.PS-03, ID.IM-01, ID.IM-02)

NIS CG Reference document (3.9.2 Change management and maintenance)

NIS CG Reference document (3.9.5 Security patch management)

NIS CG Implementing guidance (6.4. Change management, repairs and maintenance)

NIS CG Implementing guidance (6.6. Security patch management)

Tools

Attack surface mapping Hyöky.fi

Julkri (TEK-17)

Kybermittari (ASSET-4, THREAT-1, THREAT-2)

3.5 Security testing

Example implementation

- The entity has policies, procedures and operating methods in place for testing its security to the extent required by operations, needs and following a risk-based approach; see section 1.6 Risk management effectiveness assessment and metrics. As needed, this covers both technical and e.g. process and procedure testing. Tests can target individual systems or the entire organisation.
- Security tests may include vulnerability scans and information security audits.
- Security testing is organised, responsible persons have been allocated to it and it is carried out regularly. Testing is performed e.g. at regular intervals, in connection with adopting new systems, in connection with significant changes and after incidents.

- The content of security testing is defined. The definitions can include e.g. a description of testing methods, targets to be tested and ancillary components. Comprehensive documentation is produced of the testing to show e.g. the methods used, timestamp and evidence.
- Findings made during the testing have been processed. On a case-by-case basis, this can mean e.g. changing the process, managing the impact of a vulnerability and reassessing or accepting the residual risk.

Verification

1. The supervisory authority reviews the entity's policy and practices for testing its own security as is necessary based on the entity's operations, needs and risk assessment. Implementing section 1.6 may be sufficient for some entities, particularly if the role of the network and information system in their operations is very small and the risk level is moderate. Testing measures can include regular events where specified measures are performed. These include e.g. tests performed on certain processes or the technical environment. In terms of technical testing, the generated testing reports can be reviewed.
2. Furthermore, the supervisory authority can verify the effectiveness of testing by reviewing the methods used in handling the incidents discovered.

Explanations

Security testing performed by the entity help identify any weaknesses in networks, information systems and processes. Regular testing can prevent an attacker from abusing weaknesses if the entity finds and fixes them first. It is typical that errors occasionally occur in a process and services or open ports that are not updated remain in the system. In such cases, security testing may produce the impact fixing the process.

References

ISO/IEC 27002:2022 (8.29, 8.33, 8.34)

IEC 62443-2-1:2010 (4.3.4.3.1)

IEC 62443-2-1:2024 (ORG 2.3, ORG 2.4, CM 1.4, DATA 1.1, EVENT 1.4)

IEC 62443-2-4:2015 (SP 02.02, RE 3)

IEC 62443-2-4:2024 (SP.02.01, SP.02.02, SP.03.02, SP.03.05, SP.03.09, SP.03.10, SP.06.03, SP.07.04, SP.08.02, SP.08.03, SP.09.09, SP.10.02, SP.11.02, SP.11.06)

IEC 62443-3-3:2013 (SR 3.5, 3.6, 3.7)

NIST CSF 1.1 (DE.CM-8, DE.DP-3, RS.MI-3)

NIST CSF 2.0 (ID.IM-02, ID.RA-01, ID.RA-06)

NIS CG Reference document (3.9.4 Security testing)

NIS CG Implementing guidance (6.5. Security testing)

Tools

Julkri (TEK-03.3, TEK-17)

Kybermittari (THREAT-1, THIRD-PARTIES-2, ARCHITECTURE-4)

3.6 Vulnerability handling and disclosure

Example implementation

- The entity has reporting channels for reporting vulnerabilities found in the services it provides. The entity has procedures and practices for processing vulnerability reports concerning the services it provides.
- The entity also has procedures and practices for using internal and external communication channels for sharing information about vulnerabilities and their possible management methods if necessary.
- The entity has procedures and practices for processing the vulnerability data of the services it uses. (see section 3.4.1)
- The entity has included the reporting of vulnerabilities to CSIRT in its policies and practices in accordance with the national coordinated vulnerability disclosure (CVD) process[7].

Verification

1. The supervisory authority reviews the entity's documentation on how vulnerabilities found in the products can be notified to the entity and how the vulnerabilities are handled. Furthermore, the documentation shows how the detected vulnerabilities are disclosed further if necessary to parties such as the national CSIRT and service users. This includes e.g. the communication channel, communication methods and person responsible.

Explanations

References

[7] https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/coordinated-vulnerability-disclosure-cvd

ISO/IEC 27002:2022 (8.8)

IEC 62443-2-1:2024 (EVENT 1.9, ORG 2.4)

IEC 62443-2-4:2015 (SP 02.02 RE(2), SP 03.03)

IEC 62443-2-4:2024 (SP.03.01, SP.03.03, SP.08.01)

NIST CSF 1.1 (ID.RA-1, ID.RA-5, PR.IP-12, RS.AN-5, RS.MI-3)

NIST CSF 2.0 (ID.RA-01, ID.RA-05, ID.RA-06, ID.RA-08, PR.PS-02)

NIS CG Reference document (3.9.3 Vulnerability handling and disclosure)

NIS CG Implementing guidance (6.10. Vulnerability handling and disclosure)

Tools

Kybermittari (THREAT-2, THIRD-PARTIES-2)

Traficom news article: Vulnerabilities – how to report them correctly[8]

3.7 Security of supplied services

Example implementation

- If the entity produces network and information system services or systems, it has been ensured as needed that the cyber security of these services complies with section 3.2 Security of the object of acquisition. Also see section 4.2 Supply chain risk management.
- The entity has a channel for reporting vulnerabilities found in the services and systems it produces. See section 3.6 Vulnerability handling and disclosure.
- The entity has maintained a materials list of its services and systems (e.g. SBOM, software bill of materials; HWBOM, hardware bill of materials) so that dependencies and their vulnerabilities can be identified.

Verification

1. The supervisory authority reviews the supplier's descriptions of how the security of the services produced by the entity has been ensured to meet the needs described in section 3.2. while also taking section 4.2 into account. The content of the description is highly dependent on the nature of the services and systems, and the requirements on descriptions must be made proportionate to them. The entity has an easily accessible channel for reporting any security issues as well as procedures for processing the reports and taking their findings into the end product (see section 3.6). In relation to

[8] https://www.kyberturvallisuuskeskus.fi/en/news/vulnerabilities-how-report-them-correctly

services and systems, the entity must have sufficient documentation indicating e.g. dependencies of external suppliers or service providers as a part of the implementation of sections 4.2 and 3.2. This can be implemented by the entity maintaining content information, such as materials lists of services and systems (SBOM, HWBOM)

2. The supervisory authority complements the review e.g. with interviews and by testing the vulnerability reporting channel with the entity's assistance. Furthermore, the supervisory authority may use any scanning or testing of services and systems and material produced as a result of these.

Explanations

References

ISO/IEC 27002:2022 (8.25, 8.31)

IEC 62443-2-1:2010 (4.3.4.3)

IEC 62443-2-1:2024 (ORG 2.3)

IEC 62443-2-4:2024 (SP 02.01)

NIST CSF 1.1 (PR.IP-2)

NIST CSF 2.0 (ID.AM-08)

NIS CG Reference document (3.9.6 Security in acquisition of ICT services, ICT systems or ICT products)

NIS CG Implementing guidance (6.1 Security in acquisition of ICT services, ICT systems or ICT products)

NIS CG Implementing guidance (6.10. Vulnerability handling and disclosure)

Tools

Julkri (TEK-14)

Kybermittari (THREAT-1, THIRD-PARTIES-2, ARCHITECTURE-4)

3.8 Structural security of networks

Example implementation

This section extends sections 11.3 and 11.4 on baseline information security practices.

- The entity's network is protected from unauthorised access. Traffic is only permitted to the necessary addresses and ports with the required protocols.
- The entity has restricted the access to its services based on the principle of least privilege, e.g. by restricting access to services in public networks (interfaces, voice services, file sharing, management services) based on identities, user groups, IP addresses, ports or protocols. The principle of least privilege is maintained throughout the lifecycle of the network with the help of change management.
- The remote connections of service providers are also secured. Particular care has been taken in remote management, and the use of remote management access has been defined in detail.
- Furthermore, the entity can limit the service provider's access if necessary based on need and time.
- The network only uses devices controlled by the entity, and connecting any other devices to the network is primarily prohibited.
- If necessary, the mutual communication channels of systems can be protected with methods based on e.g. logical or physical separation or encryption.
- The entity has segmented its network so that different services and systems are separated into their own areas. This can be based e.g. on the criticality, vulnerability, confidentiality, needs or uses of the services or systems. Management and maintenance systems and similar have been separated into different segments where possible. In particular, segmentation has taken industrial automation devices (operational technology OT and industrial control systems ICS) and their separation from IT systems into account.
- The entity has separated the systems that are very vulnerable or critical or whose compromise may lead to the compromise of the entire network or system. Such systems include e.g. management networks and management workstations.
- Traffic between the segments is restricted so that only necessary traffic is allowed.
- The entity has separated its systems and networks from the systems and networks of its suppliers and service providers.
- Separation can be implemented with many different technologies, such as physical or logical separation using one or several of the following: virtual local area network VLAN, virtual extensible local area network VXLAN, firewall, network access control NAC, intrusion detection/prevention system IDS/IPS, virtual private network VPN.
- The entity may have also been able to utilise micro-segmentation and the zero trust principle in network separation.
- There are up-to-date network descriptions and diagrams of the entity's network and information system.

Verification

1. In reviewing the structural security of networks, the supervisory authority makes use of documentation, e.g. network descriptions, information system descriptions, operating methods and other instructions. For example, network descriptions show how different connections from untrusted networks are restricted e.g. to run through individual points. These points commonly include e.g. firewalls, encryption devices and remote access points. Furthermore, the entity may have divided its information systems and networks into separate sections e.g. based on roles, security needs, uses or criticality.
2. The supervisory authority verifies the structure of the network with interviews and configuration reviews. Only essential traffic is enabled in edge devices and between different parts of the internal network. This can be verified e.g. from firewall or routing rules, in cooperation with the entity, if necessary. In some cases, filtering can also be carried out on the device or application level at the target itself (e.g. service or terminal device). Firewall and remote access points have denied all unnecessary traffic by default. Similar functionality can also be achieved by other means, such as static routing and encryption. Segmentation can often be verified using the above-mentioned methods or by inspecting the configuration of the network's active devices. One of the most common methods is to divide the different segments into different virtual local area networks (VLAN), but other technologies may also be in use. It may be beneficial to make use of the entity's personnel in these configuration reviews.

   The supervisory authority requests the entity to verify the network protections e.g. by presenting the sections of configurations that indicate the implementation of the principle of least privilege.
3. The structural protection of the network can also be verified with different scanning applications and by making use of data traffic recordings carried out by the entity. The entity may have performed the scanning itself or used a third party whose results are reviewed by the supervisory authority.

   Scanning tools can be used e.g. by charting the visibility of different sections of the network from its other sections. This should include performing scans across the different sections of the network. Special care should also be used in scanning that reviews visibility from untrusted networks to the entity's networks. In addition to scanning, the generation of different data traffic packets can be used. Contact attempts from different sources can be made to the services of the tested target, e.g. via a browser and other software. The inspection of network security can also make use of data traffic recordings that enable the review of communications between different devices to see that unauthorised devices do not communicate with each other.

Explanations

Network protection prevents a large share of malicious traffic from unsafe networks. The segmentation of the network and information system is a key method for slowing down the advance of the attacker in the network and information system after it has gained initial access to its target.

References
ISO/IEC 27002:2022 (8.16, 8.20, 8.22)
IEC 62443-2-1:2010 (4.2.3.5, 4.3.3.4)
IEC 62443-2-1:2024 (NET 1.1, NET 1.3, NET 1.5, NET 1.6, NET 2.2, NET 3.2, NET 3.3, USER 1.16)
IEC 62443-2-4:2015 (SP 02.03)
IEC 62443-2-4:2024 (SP.03.02, SP.03.03, SP.03.07, SP.05.05, SP.07.03, SP.07.04)
IEC 62443-3-3:2013 (SR 1.11, 1.12, 1.13, 2.5, 2.6, 2.7, 3.1, 3.8, 5.1, 5.2, 5.4, 7.7)
NIST CSF 1.1 (PR.AC-3, PR.AC-5)
NIST CSF 2.0 (PR.AA-03, PR.AA-05, PR.IR-01)
NIS CG Reference document (3.9.8 Network security)
NIS CG Reference document (3.9.9 Network segmentation)
NIS CG Implementing guidance (6.7. Network security)
NIS CG Implementing guidance (6.8. Network segmentation)

Tools
Attack surface mapping Hyöky.fi
Julkri (TEK-01)
Kybermittari (ARCHITECTURE-2)
Scanning: nmap, Nessus, OpenVAS, Rapid7
Data traffic recording: Wireshark, tcpdump, netflow, sFlow
Attempted contact: ping, hping3, nc, ssh, Python Scapy library

3.9 Malicious traffic protections

Example implementation
This section extends sections 11.3 and 11.5 on baseline information security practices. • The entity has a way of detecting malicious traffic and preventing unauthorised applications and their execution where possible.

- The entity uses a solution preventing malicious or undesired traffic from untrusted networks, such as a firewall (separate device or software) or an access control list (ACL).
- Based on the entity's risk management, intrusion detection or prevention systems (intrusion detection system IDS, intrusion prevention system IPS, endpoint detection and response EDR, extended detection and response XDR) and services restricting denial-of-service attacks (e.g. packet washers) may also be used.
- The entity has technical controls or at least written practices for software installation and malware protection (e.g. phishing emails, unknown external storage media, pirate applications, malicious roaming).
- The entity should manage the installation and running of software and the use of storage media automatically (e.g. Windows Defender Application Control WDAC, AppLocker, AppArmor, SELinux).
- The entity uses malware protection, such as antivirus software for terminal devices (e.g. Anti-Virus AV, EDR, XDR), IDS/IPS, or a proxy server. Malware protection can also be implemented centrally in the email service (anti-phishing, anti-malware, DomainKeys Identified Mail DKIM, Domain-based Message Authentication, Reporting and Conformance DMARC, etc.)
- Applications detecting malicious traffic are updated sufficiently often to be able to identify new malware. This can mean daily or otherwise regular updating of identifiers and heuristic data.
- In addition, connecting unauthorised external media to the systems is prevented.
- Malware detection and prevention can also target e.g. email and web traffic.
- Malware detection and blocking the execution of unauthorised applications should apply to all devices, including mobile devices. If this cannot be implemented, other replacement solutions must be used.

Verification

1. The supervisory authority verifies that the entity comprehensively detects and prevents malicious traffic. In particular, malicious traffic produced by malware of an attacker is blocked in points where the entity's network and information system connects to untrusted networks or functionally important network sections. Essential targets typically include e.g. firewalls, remote access points (e.g. VPN gateway), wireless network infrastructure, communication systems, such as email and SMS, and often services provided externally, such as web services and interfaces. The progress of malicious traffic has also been prevented by preventing the execution and installation of unauthorised and malicious applications. This can be carried out e.g. by applications that identify and prevent malware, applications that block unknown external devices and applications and rules that prevent the execution and installation of unauthorised software. In certain cases, solutions based on procedures and practices may also be used, e.g. if the system risk level is particularly low and technical solutions are not possible or otherwise proportionate.

2. The supervisory authority verifies from configurations that protections that detect and prevent malicious traffic are enabled. Furthermore, the functioning of the systems should be reviewed e.g. with the help of log data. If malicious traffic is being prevented with organisational solutions based on procedures and practices, the related awareness and competence can be verified with interviews.
3. With the entity’s and the service provider’s assistance and permission, the supervisory authority tests the functioning of the protections that detect and prevent malicious traffic. However, these tests cannot compromise the entity’s or service provider’s network or information system. Testing can be carried out e.g. by attempting to bypass email protections by different means, such as using fake addresses, aiming to run a harmless but unauthorised software in different targets and by targeting harmless but forbidden inputs on the services.

Explanations

The majority of successful attacks are based on malware that can include e.g. viruses, worms and trojans. Software can also contain malicious features, such as backdoors, that enable an attacker to access the system. It is important that software are installed from secure sources and that the aim is to prevent malicious applications. Restricting the abilities of applications may also work. This may be enough to block some of the functions of a malicious software.

References

ISO/IEC 27002:2022 (5.32, 8.7, 8.19)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.2, COMP 2.1, COMP 2.2, COMP 2.3, CM 1.4, NET 1.8)

IEC 62443-2-4:2024 (SP.10.01, SP.10.02, SP.10.03, SP.10.05)

IEC 62443-3-3:2013 (SR 3.2, 3.3)

NIST CSF 1.1 (DE.CM-4, DE.CM-5, DE.CM-7)

NIST CSF 2.0 (DE.CM-01, DE.CM-03, DE.CM-09)

NIS CG Reference document (3.9.10 Protection against malicious and unauthorized software)

NIS CG Implementing guidance (6.9. Protection against malicious and unauthorized software)

NIS CG Implementing guidance (12.3. Removable media policy)

Tools

Attack surface mapping Hyöky.fi

Julkri (TEK-11)

Kybermittari (SITUATION-2, ARCHITECTURE-3)

Prevention of malicious traffic: for email e.g. Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF), web application firewall (WAF), proxy server, intrusion detection/prevention system (IDS/IPS)

Prevention of the execution of unauthorised applications: SELinux, AppArmor, Windows Defender Application Control WDAC, AppLocker

4 Product security, overall quality of suppliers' services, resilience, cyber security risk management measures and cyber security practices of supply chains, their direct suppliers and service providers

These recommendations are based on Article 21(2)(d) and Article 21(3) of the NIS2 Directive. The national implementation of these points is laid down in section 9, subsection 2, paragraph 4 of the Cybersecurity Act and in section 18 c, subsection 1, paragraph 4 of the Information Management Act.

1. **List of suppliers and service providers**: The entity should have up-to-date information on all direct suppliers and service providers that affect operations and service provision. (See section 4.1.)

2. **Supply chain risk management**: In its risk management, the entity should take the impact of a supply chain disruption to its own operations into account and prepare for any supply disruptions. The entity should take security-related aspects into account in relation to direct device or service suppliers in its supply chain. In considering the risk management measures, the entity should take into account the typical vulnerabilities of direct suppliers and service providers, the overall quality and resilience of products and services used by the entity, cybersecurity risk management measures included in the products and services as well as the cybersecurity practices of suppliers and service providers. These could for example include various security-related requirements in terms of availability, maintainability and contracts. The NIS Cooperation Group, European Commission and ENISA carry out risk assessments of certain supply chains in accordance with Article 22 of the NIS2 Directive. To the extent that such risk assessments have been carried out, the supervisory authority could issue an order to require entities to take the results of the risk assessment into account. (See section 4.2.)

4.1 List of suppliers and service providers

Example implementation
• The entity has maintained a directory of its direct device and service suppliers and, if necessary, other suppliers impacting cybersecurity. • The directory contains the contact information of suppliers. The entity has taken particular care in maintaining data of suppliers who have access to critical activities or who maintain critical activities. • The directory describes the services, systems and products produced by the supplier. Furthermore, the directory should contain contract-related matters, such as the length of the contract period and lifecycle matters.
Verification

1. The supervisory authority reviews that the entity has an exhaustive list of its direct device and service suppliers. The list contains e.g. contact information and the services, systems and products supplied by the supplier.

Explanations

References

ISO/IEC 27002:2022 (5.22)

IEC 62443-2-1:2024 (ORG 1.6, CM 1.1)

IEC 62443-2-4:2024 (SP.06.02)

NIST CSF 1.1 (ID.SC-2, ID.SC-3)

NIST CSF 2.0 (GV.SC-03, GV.SC-05, GV.SC-07)

NIS CG Reference document (8.2 Directory of suppliers and service providers)

NIS CG Implementing guidance (5.2 Directory of suppliers and service providers)

Tools

Kybermittari (CRITICAL-1, THIRD-PARTIES-1)

4.2 Supply chain risk management

Example implementation

- The entity has identified the impact of any supply chain disruptions to its own operations as regards suppliers identified in section 4.1. The entity has defined the necessary preparatory measures in case of supply disruptions and prepared information security policies concerning supply chain security. Continuity and recovery planning is specified in section 10.1.
- The entity has included its direct device and service suppliers into its risk management procedure, carries out risk assessment for them and treats the risks posed to them. The entity has selected proportionate measures in relation to supply chains and implemented the measures to those suppliers where risk management measures promote cybersecurity. See section 1.1. Cybersecurity risk management procedure.
- In considering its risk management measures, the entity has taken into account the following as regards its direct suppliers and service providers:
  - typical vulnerabilities, such as vulnerabilities caused by location, product selection or the nature of the sector;

  - overall quality and resilience of products and services;
  - cybersecurity risk management measures included in the products and services as well as the cybersecurity practices of suppliers and service providers that can be based on the practices, certifications or other evidence used by the entity.
- If necessary, the entity has included in its supply chains various cybersecurity related requirements in terms of availability, maintainability and agreements. The entity should identify the important features related to cybersecurity and set proportionate requirements. These can include service-level agreements included in contracts.
- The entity has managed the supply chain cybersecurity risk e.g. by including cybersecurity risk management measures into the contractual arrangements that the entity makes with its direct suppliers and service providers. These can include the assessment of cybersecurity features during the contractual period, requirements on personnel training and certification, vulnerability notification practices and review of service maintenance procedures. Also see section 3.2 Security of the object of acquisition.
- In selecting suppliers and service providers, the entity has also taken into account any regulations of the supervisory authority on the risk assessment results discussed in Article 22 of the NIS2 Directive.
- The entity may also request a materials list of its critical products and services (e.g. SBOM, software bill of materials; HWBOM, hardware bill of materials) so that dependencies and their vulnerabilities can be identified.

Verification

1. The supervisory authority verifies that the entity has established a security policy for supply chains. The supervisory authority verifies that the entity has implemented perspectives on supply chain security in its risk management. The entity has implemented the following:
   - The entity has taken possible supply chain disruptions into account in its own operations. The entity has prepared for supply chain disruptions with e.g. backup arrangements, in contracts or as a part of continuity management (see section 10.1).
   - The entity has taken security-related aspects into account in relation to its direct device or service suppliers. The supervisory authority verifies e.g. from documentation how security-related aspects are taken into account. This can be shown e.g. as security requirements to device and service suppliers, restrictions in relation to the entity’s network and information system and required procedures and practices (see e.g. baseline information security practices in section 11).
   - The entity has included risks caused by the supply chain into its risk management measures to the extent assessed necessary by the entity to ensure cybersecurity. This can mean e.g. taking into account vulnerabilities typical for the supplier or service provider. The entity has identified the overall quality and resilience of products and services, and taken them into account e.g. in its continuity management by targeting

risk management methods to the products or service and by protecting its key activities.

- In its supply chains, the entity has taken the cybersecurity risk management measures included in products and services into account. This means e.g. that the entity finds out the cybersecurity level of its supply chain to the extent possible and manages the risks caused as a part of its risk management. The entity may have discovered the level of cybersecurity e.g. by examining the reputation of the device or service supplier, information security certifications, as a part of an agreement or acquisition (see section 3.2) and by requesting documentation or other material. The entity may have managed residual risks inherited from the device or service supplier by identifying them and including them in its own risk management.
- In its supply chains, the entity has taken the cybersecurity practices of its suppliers and service providers into account. This can take place e.g. as described in point d above. Furthermore, the entity has generally defined the practices used by suppliers and service providers in providing their services to the entity’s network and information system. As practical examples, the entity may have defined with which devices or remote access protocols a supplier or service provider can produce its service to the entity’s network or information system. The entity may also have defined instructions, obligations and trainings (see section 6) required from a supplier or service provider (personnel).

Explanations

Severe vulnerabilities and attacks utilising the supply chain have become considerably more common in recent years. Supply chain vulnerabilities have also been exploited in attacks against basic infrastructure.

References

ISO/IEC 27002:2022 (5.19, 5.20, 5.21, 5.37, 7.9, 8.30)

ISO 28000:2022 (4.1, 4.2, 5.2, 6.1, 6.2, 7.5, 8)

IEC 62443-2-1:2024 (USER 1.4, ORG 1.1, ORG 1.6)

IEC 62443-2-4:2024 (SP.02.01)

NIST CSF 1.1 (ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4)

NIST CSF 2.0 (GV.OC-05, GV.SC-01, GV.SC-03, GV.SC-05, GV.SC-07, GV.SC-09)

NIST SP 800-37 rev 2 (2.8)

NIST SP 800-161 rev 1 (2.2, 2.3.4, 3.2, 3.4.2, A, B)

NIS CG Reference document (3.8.1 Supply chain policy)

NIS CG Implementing guidance (5.1. Supply chain security policy)

Tools
Julkri (HAL-06, TEK-16, TSU-16) Kybermittari (CRITICAL-2, CRITICAL-3, THIRD-PARTIES-1, THIRD-PARTIES-2)

5 Asset management and identification of important operations

These recommendations are based partly on Article 21(2)(i) of the NIS2 Directive. The national implementation of this point is laid down in section 9, subsection 2, paragraph 5 of the Cybersecurity Act and in section 18 c, subsection 1, paragraph 5 of the Information Management Act.

1. **Asset management procedures and instructions**: The entity should have regular and documented asset management procedures and instructions that could for example cover the identification of activities, processes and data. (See section 5.1.)

2. **Asset list and asset classification**: Asset refers e.g. to premises, devices, software, services, persons, intangible property and resources, such as intellectual property rights or IP addresses. Assets related to the network and information system could for example be identified and classified based on their protection needs. An up-to-date list of the assets could be maintained. (See section 5.2.)

3. **Using the asset list**: As a rule, asset management should be an essential element of changes in personnel, external entities and information systems as well as of device lifecycle management from implementation to secure decommissioning. (See section 5.3.)

5.1 Asset management procedures and instructions

Example implementation
This section extends section 11.2 on baseline information security practices. • The entity has drawn up policies for asset management and procedures and instructions for the use of the assets, and they are generally in line with the operating methods and procedures regarding the organisation's security. Information security policies and procedures are discussed in more detail in sections 2.1. and 2.1.1 Information security policies and procedures. • In its asset management procedures and instructions, the entity has included the systematic identification of activities, processes and data. • The procedures and instructions for asset management take into account leased equipment and software. Where necessary, they are in line with the listing in 4.1. • The policies, procedures and instructions cover the entire lifecycle of the asset from acquisition, secure transport, storage and use all the way to secure decommissioning and data removal and destruction. The entity has taken the secure use of external storage media into account in policies, procedures and instructions. • The procedures are kept up to date with regular reviews (e.g. once a year or in case of significant changes or incidents).

Verification

1. The supervisory authority reviews the documents drawn up by the entity on the policies, procedures and instructions of asset management and use. The procedures and instructions are up to date and show the entity's systematic identification of activities, processes and data and procedures for the maintenance of an asset list that has been carried out e.g. with planned intervals and in case of significant changes or incidents.

Explanations

Asset management is an efficient tool in cybersecurity risk management, and careful asset management prevents the implementation of risks and facilitates risk management. It is also one of the cheapest and easiest to deploy security management means.

References

ISO/IEC 27002:2022 (5.9, 5.10, 5.14, 5.37, 5.34, 7.10)

IEC 62443-2-1:2010 (4.3.4.4.6)

IEC 62443-2-1:2024 (CM 1.1, CM 1.3, DATA 1.1, DATA 1.2, DATA 1.4, ORG 1.1, COMP 1.2)

IEC 62443-2-4:2024 (SP.06.02)

IEC 62443-3-3:2013 (SR 2.4)

NIST CSF 1.1 (ID.AM-1, ID.AM-2)

NIST CSF 2.0 (ID.AM-01, ID.AM-02, ID.AM-04, ID.AM-08)

NIS CG Reference document (3.4.2 Asset Handling)

NIS CG Implementing guidance (12.2. Handling of assets)

NIS CG Implementing guidance (12.3. Removable media policy)

Tools

Julkri (HAL-04)

Kybermittari (ASSET-1, ASSET-2, ASSET-5)

5.2 Asset list and asset classification

Example implementation

This section extends section 11.2 on baseline information security practices.

- The entity has drawn up an asset list of activities, processes and data appropriate for its operations and purposes that can also include the entity's premises, devices, software, services, persons, intangible property and resources, such as intellectual property rights or IP addresses. The asset list includes the equipment, software and facilities used under contract by the entity. The asset list is up to date.
- The asset list can include the following kinds of information:
  - Asset and its unique identifier
  - Owner, administrator and users
  - Description
  - Location
  - Asset type (software incl. virtual machines, equipment and their operating systems and firmware, services, premises, HVAC systems, personnel, physical records)
  - Asset classification
  - Risk classification based on risk assessment (and the impact of the classification if needed, cf. section 5.3)
  - Device software version, SBOM (software bill of materials)
  - User support end date
  - Backup management
- Asset classification has been based on the asset's security needs, such as confidentiality, integrity and availability. The entity may have also included authenticity and non-repudiation in the security needs.
- Asset classification can determine the protection needs of an asset based on its criticality, sensitivity, risk and business value. The entity has assessed the risks posed to its assets as a part of its cybersecurity risk management measures. In its asset list, the entity may include the likelihood or risk classification of an external threat posed to the asset.
- Requirements related to asset availability should be in line with business continuity and recovery plans (see section 10).
- The entity has defined a classification for protected data and it is included in security training, for example. The entity has communicated it to the personnel and key stakeholders (see section 6.5).
- In classifying data, the entity may have utilised e.g. national legislation, nationally or internationally known data classification recommendations and instructions.

Verification

1. The supervisory authority reviews the entity's asset list. The asset list includes the entity's activities, processes and data mentioned in the example implementation. The entity uses asset classification based on the protection needs of assets. The entity has regularly reviewed and updated the asset list.

The correctness of the asset list can be verified with a documentation review comparing the content of the asset list to other available documentation, such as network descriptions, acquisition data, monitoring view and observations.

2. The supervisory authority inspects the correctness of the asset list by physical review. The supervisory authority may e.g. go through the entity's premises and compare the equipment found to the asset list.

   The correctness of the asset list can also be examined by technical means. The alternatives include a configuration review, e.g. the content of ARP tables (only IPv4), while taking into account that not all devices, in ICS/OT in particular, necessarily perform ARP queries automatically, DHCP database (leases database), DNS data.
3. The supervisory authority verifies the correctness of the asset list with passive and active scanning. Passive scanning makes use e.g. of data traffic recording that includes all entity devices that took part in the traffic. Active scanning goes through the entity's IP address spaces (IPv4, IPv6).

Explanations

References

ISO/IEC 27002:2022 (5.9, 5.12, 5.13, 5.34)

ISO/IEC 27005:2022 (7.2, 8.6, 10.5)

IEC 62443-2-1:2010 (4.2.3.4, 4.2.3.6, 4.3.4.4.2, 4.3.4.4.3, 4.3.4.4.6, A.2.3.3.8.3)

IEC 62443-2-1:2024 (CM 1.1, CM 1.3, DATA 1.1, DATA 1.2)

IEC 62443-2-4:2024 (SP.03.08 RE(2), SP.06.01, SP.06.02)

IEC 62443-3-3:2013 (SR 7.8)

NIST CSF 1.1 (ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5, PR.IP-1)

NIST CSF 2.0 (ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, PR.PS-01)

NIS CG Reference document (3.4.1 Asset classification)

NIS CG Reference document (3.4.4 Asset inventory)

NIS CG Implementing guidance (12.1. Asset classification)

NIS CG Implementing guidance (12.4. Asset inventory)

Tools

Attack surface mapping Hyöky.fi

Julkri (HAL-04.2)

Kybermittari (ASSET-1, ASSET-2, THIRD-PARTIES-1, ARCHITECTURE-3, ARCHITECTURE-5)

Scanning software: arp scan, nmap, Nessus, hping3

5.3 Using the asset list

Example implementation

This section extends section 11.9 on baseline information security practices.

- The entity has ensured that the asset list is up to date and that its content serves other activities as required, such as risk management, update management, business continuity and asset lifecycle management.
- The asset list has been updated regularly and e.g. in connection with significant changes that can include changes related to the networks and information systems, including technology selections, tools and accounts.
- The asset list revision history should be traceable.
- The asset list supports device lifecycle management from secure commissioning to decommissioning. The secure commissioning of a device is specified in section 3.4 Change and update management.
- The entity has noted the returning of devices, removal of data and the closing of accounts at the termination of employment or a subcontract. Further information in sections 6.1 Human resources security procedures and 6.2 Human resources security practices.

Verification

1. The supervisory authority reviews the asset list in accordance with section 5.2. The entity has updated the asset list regularly or in connection with changes.

   The supervisory authority reviews asset management e.g. as a part of the risk management procedure review in accordance with section 1. For example, this means that the entity’s risk management is in line with the identified asset. The entity may also have contained the risk posed to an asset and the impact of classification in its asset list.

Explanations

References

ISO/IEC 27002:2022 (5.9, 5.11, 5.18, 5.24, 5.34, 7.9, 8.10)

ISO/IEC 27005:2022 (7.2, 8.6, 10.5)
IEC 62443-2-1:2010 (4.2.3.4, 4.3.3.2, A.2.3.3.8.3)
IEC 62443-2-1:2024 (4.2.3.4, 4.3.3.2, A.2.3.3.8.3)
IEC 62443-2-4:2024 (SP.06.01, SP.06.02)
IEC 62443-3-3:2013 (SR 7.8)
NIST CSF 1.1 (ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5 PR.IP-1)
NIST CSF 2.0 (ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, PR.PS-01)
NIS CG Reference document (3.4.4 Asset inventory)
NIS CG Reference document (3.4.5 Return or deletion of assets upon termination of employment)
NIS CG Implementing guidance (12.4. Asset inventory)
NIS CG Implementing guidance (12.5. Return or deletion of assets upon termination of employment)
Tools
Julkri (HAL-04)
Kybermittari (ASSET-1, ASSET-2, ASSET-3, ACCESS-1, ACCESS-2)

6 Personnel security and cybersecurity training

These recommendations are based partly on Article 21(2)(i) and (g) of the NIS2 Directive. The national implementation of these points is laid down in section 9, subsection 2, paragraph 6 of the Cybersecurity Act and in section 18 c, subsection 1, paragraph 6 of the Information Management Act.

1. **Human resources security procedures**: Human resources security refers to procedures that ensure the information security responsibilities and obligations of persons, information security competence and background checks, in addition to key person risk management. Furthermore, these procedures cover the prevention of violations, such as identifying and avoiding dangerous work combinations, job rotation and the termination of an employment or contract. (See section 6.1.)

2. **Human resources security practices**: For example, the entity should have staff-related practices that also account for external operators, such as subcontractors. The practices could also include factors such as responsibilities and obligations after the end of an employment relationship or change in tasks. (See section 6.2.)

3. **Confidentiality and obligations**: If necessary, staff and external operators could be informed of the security-related responsibilities and obligations of their tasks and provided services, such as in relation to confidentiality. (See section 6.3.)

4. **Background checks**: If tasks and responsibilities are viewed to require particular reliability, a person could for example be subject to appropriate background checks as far as possible. (See section 6.4.)

5. **Security training**: The entity should ensure that its staff is able to act in a way that matches the cybersecurity management model and management measures. One way to achieve this is providing staff with training aimed at raising awareness of cybersecurity in general, alongside up-to-date procedures and practices and known cybersecurity risks. Training or other similar means should be used to ensure that, for carrying out their tasks, staff members have sufficient competence in securing the network and information system, identifying cyber security risks, risk management practices and assessing their impacts in relation to the services provided by the entity, and that this competence is also maintained at an adequate level. (See sections 6.5 and 6.5.1.)

6. **Familiarity among management**: Provisions on the obligation of the entity’s management to maintain sufficient knowledge of cyber security risk management are laid down in section 10 of the Cyber Security Act and section 18b of the Information Management Act. (See section 6.6.)

6.1 Human resources security procedures

Example implementation

- The entity has written procedures describing the information security responsibilities and obligations of persons.
- The entity’s human resources security procedures also describe third parties, such as external operators and subcontractors (see section 6.2).
- The entity’s human resources security procedures describe how the personnel’s cyber security competence is ensured (see section 6.5).
- The entity’s human resources security procedures also cover the needs related to background checks (see section 6.4) and key persons (see section 6.6).
- The human resources security procedures take the different roles into account, if necessary. This can be evident e.g. in noting management accountability as a part of the procedures. For example, the entity may define, designate and authorise roles related to the security and risk management of networks and information systems based on the entity’s needs.
- The entity may define roles, responsibilities and authorisations that apply to the requirements of the Act on Cybersecurity Risk Management, such as the performance of cybersecurity risk management measures in accordance with section 9 and the notification of incidents to the competent authority in accordance with section 11 (see sections 9.1 and 9.7).
- The entity has communicated its human resources security procedures and key security-related roles to personnel and third parties.
- The entity has ensured that the persons designated for the roles have the sufficient knowledge and skills to perform their tasks (see section 6.5).
- The entity’s procedures promote the prevention of violations. The entity has identified dangerous work combinations and ensured the separation of tasks. Task separation avoids situations where work combinations are formed that pose risks or have conflicting obligations and areas of responsibility. A typical dangerous work combination is one where a person both requests and approves a measure or where a person has access both to the supervised target and the information received in the supervision.
- The entity’s human resources security procedures describe the practices for preventing violations. These procedures may include e.g. changes in employment, task circulation and changes or terminations of contracts or employment.

Verification

1. The supervisory authority verifies that the entity has written procedures on human resources security. These procedures describe information security responsibilities and obligations that the personnel must comply with in order to achieve security. The procedures describe security trainings, background checks and key persons. If necessary, the procedures also apply to third parties, such as subcontracting partners, at least in terms of operating

methods (see section 6.2). The procedures include matters related to the prevention of violations, such as the identification of dangerous work combinations and separation of tasks as well as changes and terminations of employment and agreements.

2. The supervisory authority verifies the awareness and implementation of human resources security procedures e.g. with interviews. The interviews should describe the practical operation of key person roles so that sufficient resources and authorisations have been reserved for the task. Furthermore, the personnel are interviewed about dangerous work combinations and their separation on the practical level.

Explanations

Cyber security is a whole where the key factor is the personnel. The personnel are also often the weakest link of information security and cybersecurity, meaning that the personnel's security awareness and personnel-related procedures and operating methods are extremely important.

Personnel are the most important element of organisational risk management. It is important to harness the personnel to identify risks posed to their own tasks to the best of their ability. Cooperation usually guarantees better risk management than work carried out by a limited group of people.

References

ISO 27001:2022 (5.3, 7.1, 7.2, 7.4)

ISO 27002:2022 (5.2, 5.3, 5.5, 6.2, 6.3, 6.4, 6.5)

IEC 62443-2-1:2010 (4.3.3.2)

IEC 62443-2-1:2024 (ORG 1.1, ORG 1.2, ORG 1.3, ORG 1.4, ORG 1.5, ORG 1.6, ORG 2.1, ORG 2.2)

IEC 62443-2-4:2015 (SP 01.07)

IEC 62443-2-4:2024 (SP.01.01, SP.01.02, SP.01.03, SP.01.04, SP.01.05, SP.01.06, SP.01.07)

NIST CSF 1.1 (PR.AT-5, PR.IP-11)

NIST CSF 2.0 (PR.AT-02, GV.RR-04)

NIS CG Reference document (3.2.2 Roles, responsibilities and authorities)

NIS CG Reference document (3.5.1 Human resources security)

NIS CG Reference document (3.5.4 Disciplinary process)

NIS CG Implementing guidance (1.2 Roles, responsibilities and authorities)

NIS CG Implementing guidance (10.1. Human resources)

NIS CG Implementing guidance (10.4. Disciplinary process)

Tools

Julkri (HAL-02)

Kybermittari (THIRD-PARTIES-1, THIRD-PARTIES-2, WORKFORCE-1, WORKFORCE-2, WORKFORCE-3, General management measures)

6.2 Human resources security practices

Example implementation

- The entity’s human resources security practices implement the procedures related to changes and terminations of employment.
- Measures related to changes can include e.g. changes in access rights in devices used by a person when their tasks change.
- The practices also describe measures carried out when tasks are terminated. These can include the removal of access rights and devices, data destruction and measures related to the transfer of assets, competence and responsibilities. These measures have also been explained to the personnel.
- The human resources security practices also apply to third parties, such as external operators and subcontractors.

Verification

1. The supervisory authority verifies from documentation that the entity has practices for measures carried out in connection with changes and terminations of tasks. These practices also apply to third parties, such as external operators and subcontractors.
2. The supervisory authority can verify that the responsibilities and obligations in accordance with the practices have been implemented e.g. from the systems and configurations. For example, this can mean that access rights made redundant have been transferred or removed, devices have been returned, unnecessary data has been deleted and responsibilities are transferred to other personnel as required.

Explanations

A change in tasks is a situation with a high risk for unnecessary rights, data or devices being left with a person who is no longer authorised to have them. In particular, situations where a person’s work tasks come to an end can in some cases cause a great risk to the organisation’s cyber security unless access to resources is denied.

References

ISO/IEC 27002:2022 (6.5, 8.10) IEC 62443-2-1:2010 (4.3.3.2) IEC 62443-2-1:2024 (ORG 1.2, ORG 1.3, USER 1.1, USER 1.2, USER 1.4) IEC 62443-2-4:2015 (SP 01.07) IEC 62443-2-4:2024 (SP.01.07, SP.09.02, SP.09.03, SP.09.04) NIST CSF 1.1 (PR.IP-11) NIST CSF 2.0 (GV.RR-04) NIS CG Reference document (3.5.3 Termination or change of employment procedures) NIS CG Implementing guidance (10.3 Termination or change of employment procedures)
Tools
Kybermittari (ACCESS-1, ACCESS-2, ACCESS-3, THIRD-PARTIES-1, THIRD-PARTIES-2, WORKFORCE-1)

6.3 Confidentiality and obligations

Example implementation
• The entity ensures that the procedures described in section 6.1 include instructions and obligations related to the handling of equipment, use, management and maintenance of user accounts, internet behaviour, social media, the use of personal devices, software security and external storage media. • In particular, the entity ensures that obligations related to confidentiality are described and explained to the personnel and, if necessary, to third parties. The entity has clearly defined confidential matters. This can be implemented e.g. by marking confidential data or information systems. The entity must also ensure that data is processed correctly when it is disclosed and received. • Personnel, including third-parties, must understand, implement and comply with obligations related to human resources security. The entity has also described how the cyber security obligations are communicated to the personnel.
Verification
1. The supervisory authority verifies that the entity has defined obligations related to cyber security. These requirements are comprehensive and support the implementation of the entity's cyber security. Documentation should also describe the definitions and responsibilities related to confidentiality and how

the correct processing of confidential material is ensured when disclosing and receiving data.

2. The supervisory authority verifies e.g. with interviews that the cyber security obligations are implemented, the personnel are aware of them and the personnel identifies any confidential targets and knows the related responsibilities and obligations.

Explanations

References

ISO/IEC 27002:2022 (5.10, 6.6)

IEC 62443-2-1:2024 (USER 1.4, DATA 1.1, DATA 1.2)

IEC 62443-2-4:2024 (SP.01.03)

NIST CSF 1.1 (PR.AT-3, PR.AT-4, PR.AT-5)

NIST CSF 2.0 (PR.AT-02)

NIS CG Implementing guidance (5.1 Supply Chain Security)

NIS CG Implementing guidance (6.1 Security in acquisition of ICT services, ICT systems or ICT products)

Tools

Julkri (HAL-15)

Kybermittari (THIRD-PARTIES-2, WORKFORCE-1, WORKFORCE-3)

6.4 Background checks

Example implementation

- The entity has identified the tasks and responsibilities that require particular reliability. In these cases, the eligibility of a person for the tasks in question must be verified as needed with background checks.
- Background checks are renewed e.g. every five years or as the individual's tasks change.

Verification

1. The supervisory authority verifies that the entity has identified the tasks and responsibilities where the person selected must be subject to background checks.

Explanations

References

ISO/IEC 27002:2022 (6.1)

IEC 62443-2-1:2010 (4.3.3.2.2, 4.3.3.2.3)

IEC 62443-2-1:2024 (ORG 1.2, ORG 1.6)

IEC 62443-2-4:2015 (SP 01.04)

IEC 62443-2-4:2024 (SP.01.04)

NIST CSF 1.1 (PR.IP-11)

NIST CSF 2.0 (GV.RR-04)

NIS CG Reference document (3.5.2 Background checks)

NIS CG Implementing guidance (10.2 Background checks)

Tools

Julkri (HAL-10)

Kybermittari (WORKFORCE-1)

6.5 Security training

Example implementation

This section extends section 11.1 on baseline information security practices.

- The entity has ensured that the personnel have the knowledge and sufficient competence to act in accordance with policies concerning security in the extent that is essential for their tasks. In order to achieve this goal, regular training has been organised on the procedures and practices with the aim of improving general cybersecurity awareness and awareness of cybersecurity risks as well as ensuring sufficient competence in relation to tasks on the protection of the network and information system, identifying cybersecurity risks and assessing cybersecurity risk management practices and their impact regarding the services provided by the entity.

- The entity has defined the ways in which the entity's cybersecurity procedures are trained to the entire personnel.
- Training provided to the personnel has covered cybersecurity risk management measures. Training should particularly ensure that the personnel's operations support the implementation of management measures where this is essential for their tasks.
- The entity has also trained its personnel in cyber risk management where this is essential for their tasks. For example, this can mean information on the most typical cyber risks and the impact assessment of management measures e.g. of cyber risks related to their own tasks. Furthermore, the entity has trained its personnel to identify possible cyber risks e.g. in order to support the entity's cyber risk management.
- The entity may have identified tasks and roles that can be of particular interest. These persons can be protected with tailored training, e.g. on social engineering, influencing attempts and phishing.
- The entity can also promote the general cybersecurity awareness among personnel with lighter methods. This can make use of short briefings on recent scamming attempts or events in the sector.

Verification

1. The supervisory authority verifies from documentation that the entity offers training to its personnel on the management, identification and, if necessary, assessment of cybersecurity risks. The training contains the procedures and practices with which the entity promotes cybersecurity awareness and cybersecurity risk management. The aim of the training is that the personnel have sufficient competence in relation to their tasks on the protection of the network and information system and identifying cybersecurity risks. If necessary, training must also ensure that the personnel have the ability to assess the cybersecurity risk management practices and their impact regarding the services provided by the entity if so required by their tasks.

Explanations

References

ISO/IEC 27001:2022 (7.2, 7.3)

ISO/IEC 27002:2022 (6.3)

IEC 62443-2-1:2010 (4.3.2.4)

IEC 62443-2-1:2024 (ORG 1.3, ORG 1.4, ORG 1.5)

NIST CSF 1.1 (PR.AT-1)

NIST CSF 2.0 (PR.AT-01)

NIST SP 800-161 rev 1 (3.3)

NIS CG Reference document (3.6.2 Security training)

NIS CG Implementing guidance (8.2 Security training)

Tools

Julkri (HAL-13)

Kybermittari (WORKFORCE-2, WORKFORCE-4)

6.5.1 Security training – extended instructions

Example implementation

This recommendation is intended for the supervision of entities from whom the supervisory authority expects a higher level of maturity.

- The entity has systematically implemented training related to cybersecurity and monitored participation in the training.
- The training is sufficiently comprehensive and the understanding of its topic among training participants can also be measured.
- The entity has practices that are applied to the completion of missing training.

Verification

1. The supervisory authority verifies from documentation that the entity has defined that training takes place systematically. In addition, the entity must have practices for monitoring participation in the training.
2. The supervisory authority verifies from a record of attendance or similar that the personnel take part in trainings and that this is ensured. Interviews can also verify the personnel's cybersecurity competence and awareness.

Explanations

References

ISO/IEC 27001:2022 (7.2)

ISO/IEC 27002:2022 (6.3)

IEC 62443-2-1:2010 (4.3.2.4)

IEC 62443-2-1:2024 (ORG 1.3, ORG 1.4, ORG 1.5)

NIST CSF 1.1 (PR.AT-1)

NIST CSF 2.0 (PR.AT-01)

NIST SP 800-161 rev 1 (3.3)

NIS CG Reference document (3.6.2 Security training)

NIS CG Implementing guidance (8.2 Security Training)

Tools

Kybermittari (WORKFORCE-4)

6.6 Familiarity among management

Example implementation

- The entity must ensure that the management has sufficient competence in the general leadership of cybersecurity risk management. This could be implemented with training or self-study to ensure sufficient competence in identifying cyber security risks, risk management leadership and assessing the impacts of risk management practices.
- Management refers to the entity’s board of directors, supervisory board, CEO or others in a comparable position that in actuality directs its operations.
- The entity must ensure that the management has familiarised itself with the entity’s cybersecurity risk management and is able to make decisions based on it. The management is also aware of its own role, responsibilities and control in the management of cybersecurity risks.

Verification

1. The supervisory authority verifies from documentation that management members have participated in sufficient trainings. As a result, the management has sufficient understanding of cybersecurity risk management and of its own role, responsibilities and control in the matter. The organisation’s management is aware of the cybersecurity risk management carried out in the organisation and able to process risk management results.
2. The supervisory authority can verify e.g. from a training register or with interviews that management members have participated in cybersecurity risk management training or study modules or otherwise indicate having the sufficient competence. Furthermore, the supervisory authority may investigate how the members have taken cyber risk management measures into account in their decisions and operations.

Explanations

Functioning cyber risk management requires management commitment. Furthermore, understanding of the cyber environment and the related risks requires competence. In cybersecurity risk management, management often has great responsibility and central tasks that are related e.g. to the selection of management measures, decisions on residual risks, organisation of resources and authorisation.
References
ISO/IEC 27001:2022 (5.1, 9.3) ISO/IEC 27002:2022 (5.4) ISO/IEC 27005:2022 (10.6) IEC 62443-2-1:2010 (4.3.2.3.3, 4.3.2.6, 4.4.3) IEC 62443-2-1:2024 (ORG 1.1, ORG 1.3, ORG 1.4, ORG 2.4) NIST CSF 1.1 (GV.PO-01, GV.PO-02, PR.AT-4) NIST CSF 2.0 (PR.PS-04, PR.AT-02) NIST SP 800-30 rev 1 (3.3) NIS CG Reference document (3.1 Top management commitment and accountability)
Tools
Kybermittari (CRITICAL-2, RISK-1, WORKFORCE-4, PROGRAM-2,)

7 Access management and authentication procedures

These recommendations are based partly on Article 21(2)(i) and (j) of the NIS2 Directive. The national implementation of these points is laid down in section 9, subsection 2, paragraph 7 of the Cybersecurity Act and in section 18 c, subsection 1, paragraph 7 of the Information Management Act.

1. **Access control procedures**: Access control and authentication procedures should apply to natural users, such as staff and external operators, as well as system accounts, such as accounts used by devices, software, interfaces and other essential resources. Access control should apply to both software-authenticated access and physical access. The procedures should be based on business requirements and requirements on networks and information systems, taking into consideration the special characteristics. The entity could for example have definitions and practices for access control that ensure reliable identification and only allow access to the necessary networks and information systems, protected data and other resources. (See section 7.1.)

2. **Continuous maintenance of access control and access rights**: The entity could for example have procedures that cover the entire lifecycle of accounts and access rights and the rights should be managed accordingly. (See section 7.2.)

3. **Access control monitoring**: Access rights and their use should be monitored. (See sections 7.3 and 7.3.1.)

4. **Access control records and the principle of least privilege**: Up-to-date records could for example be kept of the access rights and roles, and users could only be assigned the permissions necessary for their designated tasks (principle of least privilege). (See section 7.4.)

5. **Administrator accounts**: Entities should have procedures in place for managing accounts with elevated privileges and administrator privileges, which could for example be done by striving to limit administrator privileges to as small a number of users as possible, and these accounts would be protected with strong methods. The use of administrator privileges should be monitored. (See section 7.5.)

6. **Selection of secure authentication methods and reliable authentication**: The selected authentication practices and technologies should optimally be based on requirements on data availability and authentication methods. The authentication methods should be sufficiently secure so that unauthorised use is prevented where possible. If necessary, the authentication method should be strong identification, multi-factor authentication (MFA) or continuous authentication if their use is an option. (See section 7.6.)

7.1 Access control procedures

Example implementation

This section extends section 11.6 on baseline information security practices.

- Access control and authentication procedures apply to natural users, such as personnel and external operators, as well as system accounts, such as accounts used by devices, software, interfaces and other essential resources.
- The entity has procedures, definitions and practices related to access control that comprehensively ensure reliable authentication (AuthN) into networks and information systems, protected data and other resources. If necessary, the entity has also drawn up a policy for access management.
- The entity's access control and authentication procedures cover both software-authenticated and physical access.
- The procedures are based on business requirements and requirements on networks and information systems, taking into consideration the special characteristics.
- The access control and authentication procedures ensure that identification is user-specific where possible and that it sufficiently ensures the identity of the user. The selection of the identification means may have been based on the system's risk assessment. In a system with a low risk level, identification based on a username and secure password can be sufficient. In higher risk level systems, authentication methods based on multiple factors have been used where possible (multi-factor authentication, MFA). In addition to the user's password, these can include time-based one-time codes, digital certificates, chip cards, tokens or biometric means.
- If the entity uses shared accounts, it is good practice to ensure that the authentication methods are managed by authorised persons and that the authentication methods can be easily changed and securely shared to the account users.
- The entity has only authorised access (authorization, AuthZ) to the necessary networks and information systems, protected data and other resources. These accesses are implemented based on definitions. Authorised access is defined based on the principle of least privilege. Authorisations based on the user should generally be avoided. Instead, it is better to use e.g. role-based access management.
- The entity has noted the sufficient separation of tasks in allowing access to the necessary resources. Further information on task separation in section 6.1 Human resources security procedures.
- The procedures and practices of physical access control are organised based on the entity's business needs and risk management. In terms of critical systems, the aim has been to be able to identify users individually, e.g. by means of physical access control. Further information on physical security and premises security in section 12.
- At its discretion, the entity can implement the zero-trust principle partly or fully as a part of its access control principles if it can be applied to the entity's

architecture. The zero-trust principle is usually applied in connection with cloud services or a hybrid cloud.

Verification

1. The supervisory authority verifies that the entity has procedures, definitions and practices for access control and authentication. The procedures are comprehensive and take the entity's different functions from physical premises to software interfaces into account. These include the access control and authentication of both person users and system accounts. The entity has also taken third parties into account in its access control. The supervisory authority ensures that the entity has arranged access control and authentication procedures, definitions and practices so that identification is reliable and based on the principle of least privilege.
2. The supervisory authority verifies that the entity's systems allow users to only perform measures that they are authorised for. This can be ensured e.g. by reviewing access rights or performing security testing, examining that the users are unable to make wider measures than those they are authorised for. The review can check that the roles and persons set in the system correspond with the described definitions (see section 7.4) and thus verify the implementation of the procedures. The systems can also be used to verify that secure authentication and identification methods are actually in use. This can make use of configuration data and screenshots.

Explanations

Access control procedures and practices ensure that access controls are correctly sized and cover all of the entity's systems. Comprehensive access control ensures that control has an impact in all necessary locations. In addition to the traditional login functions (e.g. logging in to a computer or website), the procedures and practices should observe other functions that require access control, such as file sharing. Access control disruptions may cause data leaks or breaches as unauthorised persons are able to access data that does not belong to them.

References

ISO/IEC 27002:2022 (5.3, 5.15, 5.16, 5.17, 5.18, 5.37, 8.3, 8.5)

IEC 62443-2-1:2010 (4.3.3.6, 4.3.3.7)

IEC 62443-2-1:2024 (ORG 1.1, ORG 2.2, USER 1.1, USER 1.2, USER 1.4, USER 1.5, USER 1.6, USER 1.7, USER 1.8, USER 1.9, DATA 1.1)

IEC 62443-2-4:2024 (SP.09.01, SP.09.02, SP.09.03, SP.09.04)

IEC 62443-3-3:2013 (SR 2.1)

NIST CSF 1.1 (PR.AC-4, PR.AC-7)

NIST CSF 2.0 (PR.AA-03, PR.AA-05)

NSA, CISA: Identity and Access Management: Recommended Best Practices for Administrators

NIS CG Reference document (3.7.1 Access control policy)

NIS CG Reference document (3.7.5 Identification)

NIS CG Implementing guidance (11.1. Access control policy)

NIS CG Implementing guidance (11.5. Identification)

Tools

Julkri (HAL-14, TEK-07, TEK-08)

Kybermittari (ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, ARCHITECTURE-3)

7.2 Continuous maintenance of access control and access rights

Example implementation

- The entity's access control procedures and practices ensure that accounts and rights are up to date.
- The entity's lifecycle approach to access control takes into account the impact of changes in employment, contracts and other similar factors. For example, extraneous access accounts and rights are removed after they are no longer needed.
- The procedures define the necessary practices and responsibilities related to changes in access control and access rights.
- The management of the privileges of maintenance accounts and administrator accounts has received special attention and they are continuously up to date.
- The entity has up-to-date records or a similar procedure of accounts and their rights (see section 7.4).

Verification

1. The supervisory authority verifies that the entity's access control procedures and practices include methods for monitoring the lifecycle of access rights. They take into account e.g. the user management process, the removal of privileges and the use of temporary accounts. The removal of privileges pays special attention to users who no longer work in the organisation or who no longer have an appropriate need for the resources in question, e.g. due to a change in tasks. In addition, the entity has procedures on the use of any temporary accounts.
2. The supervisory authority verifies that the entity's access control is up to date. A review can establish that unnecessary user accounts have been removed or locked. The privileges of accounts are reviewed to ensure that

they only have the minimum rights required that correspond with the entity's other documentation (see section 7.4).

Explanations

Extraneous access accounts and privileges may enable an attacker to access the system. Too extensive access rights can enable an employee to view or process resources without an appropriate need based on their tasks.

References

ISO/IEC 27002:2022 (5.18)

IEC 62443-2-1:2010 (4.3.3.5.1, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.8)

IEC 62443-2-1:2024 (USER 1.4, USER 1.5)

IEC 62443-2-4:2024 (SP.03.08, SP.09.04)

NIST CSF 1.1 (PR-AC.1)

NIST CSF 2.0 (PR.AA-01, PR.AA-05)

NIS CG Reference document (3.7.2 Management of access rights)

NIS CG Implementing guidance (11.2. Management of access rights)

Tools

Julkri (HAL-14, TEK-07.3)

Kybermittari (ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, WORKFORCE-1)

7.3 Access control monitoring

Example implementation

- The entity has monitored the access and use of systems and devices. In order to implement the monitoring, the entity has generated e.g. log data of access control events or other reliable data that enables event tracking. Events related to access control include e.g. account modification, login information (who, what, from where, to where and when), use of accounts and administrator measures.
- The log of access control events has been stored for sufficiently long in order to examine any cases of misuse at a later date, e.g. in connection with investigating an incident.
- For example, abnormal login attempts and other events based on risk management have been monitored on the basis of event logs.

- Monitoring may have been implemented e.g. with manual procedures, a system producing automatic alerts, by monitoring trends and with the help of notification channels. Further information of monitoring in section 9.3 Event logging and detection.
- As a result of incidents, the user account is closed, locked or its authentication method is reset. (See section 9.5.)
- In certain cases, the entity may also have used manual records, e.g. a visitor log. This particularly applies to physical access control in situations where automatic recording is not possible. The monitoring of access control based on manual records can be arranged e.g. by reviewing the records regularly or whenever an incident is detected.

Verification

1. The supervisory authority verifies that the entity has monitored the access and use of systems and devices. The entity may have implemented this e.g. by collecting a log on access control events and storing it for a sufficiently long time. The entity has practices for reviewing access control events. For example, the entity can review its event logs occasionally, with agreed intervals or whenever there is a reason to suspect an incident.
2. If the entity monitors the access and use of systems and devices by collecting a log, the supervisory authority verifies that the events related to access control actually generate a log. The log should at least indicate the target, source, time, user and any other factors related to access control, such as the type of multi-factor authentication used. It should also correspond to any access control documents of the entity. The supervisory authority may request the entity to point to the desired sections of the log or supply the log or parts thereof, taking security into consideration.

Explanations

The monitoring of access control is a recognised method for detecting unauthorised use of accounts, in addition to attempted breaches and misuse. The production of event logs is usually necessary for the purposes of monitoring.

References

ISO/IEC 27002:2022 (5.15, 8.15)

IEC 62443-2-1:2010 (4.3.3.6.4)

IEC 62443-2-1:2024 (USER 1.4, USER 1.5, USER 1.15, USER 2.1, EVENT 1.4, DATA 1.1)

IEC 62443-2-4:2024 (SP.08.02, SP.09.04)

NIST CSF 1.1 (PR.PT-1, PR.AC-7)

NIST CSF 2.0 (PR.PS-04, PR.AA-03)National Cybersecurity Centre Finland: Collecting and using log data[9]

NIS CG Reference document (3.7.2 Management of access rights)

NIS CG Reference document (3.11.2 Monitoring and logging)

NIS CG Implementing guidance (11.2 Management of access rights)

NIS CG Implementing guidance (3.2. Monitoring and logging)

Tools

Julkri (HAL-07, TEK-12)

Kybermittari (ACCESS-2, ACCESS-3, SITUATION-2)

7.3.1 Access control event log monitoring – extended instructions

Example implementation

This recommendation is intended for the supervision of entities from whom the supervisory authority expects a higher level of maturity.

- The entity has used event logs to monitor events such as abnormal login attempts, changes to users or access rights, maintenance operations and other events related to risk management.
- Monitoring has been implemented e.g. with a system producing automatic alerts, by monitoring trends, using manual procedures and with the help of notification channels.
- If necessary, event logs have been transferred e.g. to a SIEM (Security Information and Event Management) or other centralised log management system that can also collect log data of events in other systems.

Verification

1. The supervisory authority verifies the entity's documentation on the monitoring of access control event logs. Documentation should define how and what data of the log is monitored. It also defines the further handling measures of monitoring observations, e.g. the communication channels of automatic alerts and their monitoring or the further handling of an incident detected from a log by an administrator.
2. The supervisory authority verifies that the monitoring has produced events and that they have been handled appropriately. Events generated from log

[9] https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/collecting-and-using-log-data

monitoring should be stored and their processing history should be unambiguous.

Explanations

The immediate response enabled by continuous monitoring can prevent wider damage.

References

ISO/IEC 27002:2022 (8.16)

IEC 62443-2-1:2010 (4.3.3.6.4, 4.3.3.6.7)

IEC 62443-2-1:2024 (DATA 1.1, EVENT 1.4, EVENT 1.7, USER 1.14, USER 1.15)

IEC 62443-2-4:2024 (SP.08.02, SP.08.03, SP.09.04)

NIST CSF 1.1 (PR.PT-1, PR.AC-7)

NIST CSF 2.0 (PR.PS-04, PR.AA-03)

NIS CG Reference document (3.11.2 Monitoring and logging)

NIS CG Implementing guidance (3.2. Monitoring and logging)

National Cybersecurity Centre Finland: Collecting and using log data[10]

Tools

Julkri (HAL-07, TEK-12, TEK-13)

Kybermittari (ACCESS-1, ACCESS-2, SITUATION-1, SITUATION-2, SITUATION-3)

7.4 Access control records and the principle of least privilege

Example implementation

- The entity keeps records or has a similar procedure for logging access rights and roles. There is a procedure for maintaining these records up to date.
- Based on the records, the users are assigned only the permissions necessary for their designated tasks (principle of least privilege). The aim has been to avoid user-based authorisations where possible and instead use role-based access management.

Verification

[10] https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/collecting-and-using-log-data

1. The supervisory authority verifies the entity’s documentation on the logging procedures related to access control. The documentation shows how the access rights and roles are recorded. The entity’s access control records indicate the access rights and roles of systems. For some systems, these records can be kept manually, but it can also be an automatic and e.g. system-level recording of user and role-based access right management.
2. The supervisory authority verifies the access rights of the entity’s system and how they correspond to the records. This can be done by a random sampling of the users or by reviewing certain privileges, such as system administrator or other elevated privileges. Access rights should correspond to the records kept of them. If the system uses e.g. access right management based on roles or user groups, no undocumented user-based rights should be issued in addition to these.

Explanations

Extraneous access accounts and privileges may enable an attacker to access the system. An attacker may abuse undocumented or forgotten access rights when moving in the system or from one system to another. Access rights issued too extensively may also enable other unwanted disclosure of data.

References

ISO/IEC 27002:2022 (5.15, 5.18, 8.3)

IEC 62443-2-1:2010 (4.3.3.7)

IEC 62443-2-1:2024 (USER 1.4, USER 1.5)

IEC 62443-2-4:2024 (SP.03.08, SP.09.04)

NIST CSF 1.1 (PR.AC-4)

NIST CSF 2.0 (PR.AA-05)

NIS CG Reference document (3.7.2 Management of access rights)

NIS CG Reference document (3.7.3 Privileged and administration accounts)

NIS CG Implementing guidance (11.2. Management of access rights)

NIS CG Implementing guidance (11.3. Privileged accounts and system administra-tion accounts)

Tools

Julkri (HAL-14, TEK-07.2)

Kybermittari (ACCESS-1, ACCESS-2, ACCESS-3, ARCHITECTURE-3)

7.5 Administrator accounts

Example implementation

This section extends section 11.7 on baseline information security practices.

- The entity has a procedure for issuing elevated privileges or administrator privileges to authorised persons, devices or applications only. These privileges have only been granted to as few users as possible while still enabling backup arrangements. Furthermore, the privileges have only been issued for as long as they are necessary for performing designated tasks. This also applies e.g. to maintenance work carried out by a third party. The entity has included policies concerning administrator privileges in a possible access management policy.
- Elevated privileges and administrator privileges are protected by strong methods. This can mean e.g. stronger authentication methods, several authentication methods or sufficient protection of authentication methods.
- When the needs change, extraneous privileges are primarily removed.
- The use of elevated privileges and administrator privileges is monitored where possible. For example, this can mean that functions performed with elevated privileges accumulate a monitoring log or more than one person is required to perform a function (two-man rule).
- The entity may have drawn up instructions on the use of elevated privileges and administrator accounts. Accounts with elevated privileges and administrator accounts must not be used for basic functions, nor should basic user accounts be used for elevated privilege or administrator functions. Emergency accounts are only used for justified reasons in the case of an emergency. In terms of the emergency accounts, it has also been ensured that they are available in an emergency, while being sufficiently protected.
- The entity has established procedures and instructions for the secure use of the management network and management workstations.

Verification

1. The supervisory authority verifies the entity’s documentation on the procedures on the use and maintenance of administrator accounts. Documentation indicates the entire management lifecycle of elevated privileges and administrator privileges. The documentation should comment on the issuing and revoking of privileges, their supervision, their linking to accounts or user groups and the related special practices, such as their separation from normal accounts. The supervisory authority verifies that the entity has procedures for monitoring the use of administrator rights and that administrator accounts are protected by strong methods.
2. The supervisory authority verifies the entity’s elevated privileges and administrator privileges and the accounts or user groups linked to them by carrying out a review. The lifecycle of privileges should be reviewed to ensure that elevated privileges or administrator privileges are only issued to persons

who have an appropriate need to use them based on their tasks. The supervisory authority can review the monitoring system or the implementation of the monitoring process, e.g. by studying the status of the monitoring system, conducting interviews and reviewing the implementation of the monitoring process.

The supervisory authority verifies from the system or screenshots that strong methods (e.g. MFA) are applied to administrator accounts. In terms of the emergency accounts, it is checked that they are available in an emergency, while being sufficiently protected. The review can also check that emergency accounts have only been used for a justified reason in an emergency.

Explanations

Elevated privileges and administrator privileges enable making significant changes to the systems. Their abuse can cause severe data leaks, continuity disruptions, monetary losses or other business disruptions. They must be protected particularly well. For this reason, administrator accounts must be protected by strong methods.

References

ISO/IEC 27002:2022 (5.15, 5.18, 5.37, 8.2, 8.18)

IEC 62443-2-1:2010 (4.3.3.6.3, 4.3.3.6.4)

IEC 62443-2-1:2024 (USER 1.4, USER 1.5, USER 2.3, USER 2.4, ORG 1.1)

IEC 62443-2-4:2024 (SP.03.08, SP.09.04)

NIST CSF 1.1 (PR.AC-4)

NIST CSF 2.0 (PR.AA-05)

NIS CG Reference document (3.7.3 Privileged and administration accounts)

NIS CG Reference document (3.7.4 Administration systems)

NIS CG Implementing guidance (11.3. Privileged accounts and system administration accounts)

NIS CG Implementing guidance (11.4. Administration systems)

Tools

Julkri (TEK-04, TEK-07, HAL-14)

Kybermittari (ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, ARCHITECTURE-3)

7.6 Selection of secure authentication methods and reliable authentication

Example implementation

- The entity has only used authentication methods that are sufficiently secure in terms of the target's security needs.
- The entity has used multi-factor authentication in accordance with its own risk assessment and system capabilities. As the authentication methods, the entity has used e.g. multi-factor authentication (MFA), continuous authentication, strong identification (mobile certificate, bank credentials, Citizen Certificate) or similar if their use has been possible. Multi-factor authentication should be used especially for maintenance accounts and systems.
- The entity has ensured that confidential data related to authentication methods, such as passwords, remain confidential. Typically, e.g. passwords must be changed in connection with the initial login. When creating and delivering accounts, the user must be identified reliably. Password creation has avoided e.g. weak and predictable passwords. Exceptions can include situations where the short-term use of a weak or predictable password is justified, such as when a new employee logs in for the first time or when resetting a password. More detailed information of password protection in section 3.3 System hardening.
- If possible, the users are identified individually and e.g. the use of shared identifiers has been avoided. If the entity cannot avoid using shared identifiers, their authentication methods should be sufficiently secure.
- Sufficient logs have been kept on the use of authentication methods, and the detected incidents, such as fatigue attacks, have been responded to e.g. by slowing down the login of the targeted account. More detailed information on logging practices is available in sections 7.4 Access control event log monitoring and 9.3 Event logging and detection.
- Interactive system login sessions should time out after a predefined time.

Verification

1. The supervisory authority verifies that the entity has documentation on the authentication methods of its systems. This covers e.g. password practices, system-specific specifications and procedures on the secrets of authentication methods, such as passwords and their distribution. The supervisory authority reviews from documentation the entity's procedures for reliable authentication (e.g. MFA).
2. The supervisory authority verifies from screenshots or by reviewing the system that the entity uses documented authentication methods. Authentication methods are used comprehensively in different systems and defined for different user groups. Screenshots or system reviews also show the use of reliable authentication and the selected authentication method.

Explanations

Accounts and authentication methods, their sections open to a public network in particular, face a notable amount of breach attempts, which is why their security is important. The authentication methods of systems in the internal network must also be selected carefully and include no default accounts or passwords. Reliable authentication methods increase the security of the systems that use them by protecting them against phishing in particular.

References

ISO/IEC 27002:2022 (8.5)

IEC 62443-2-1:2010 (4.3.3.6.1, 4.3.3.6.3)

IEC 62443-2-1:2024 (USER 1.8, USER 1.9, USER 1.11, USER 1.12, USER 2.3)

IEC 62443-2-4:2024 (SP.09.05, SP.09.06, SP.09.07, SP.09.08, SP.09.09)

NIST CSF 1.1 (PR.AC-7)

NIST CSF 2.0 (PR.AA-03)

NIS CG Reference document (3.7.5 Identification)

NIS CG Reference document (3.7.6 Authentication)

NIS CG Reference document (3.7.7 Multi-factor authentication)

NIS CG Implementing guidance (11.5. Identification)

NIS CG Implementing guidance (11.6. Authentication)

NIS CG Implementing guidance (11.7. Multi-factor authentication)

Tools

Julkri (TEK-04, TEK-08)

Kybermittari (ACCESS-1, SITUATION-1)

8 Policies and procedures regarding the use of cryptographic methods and, where appropriate, measures for using secured electronic communication

These recommendations are based on Article 21(2)(h) and partly (j) of the NIS2 Directive. The national implementation of these points is laid down in section 9, subsection 2, paragraph 8 of the Cybersecurity Act and in section 18 c, subsection 1, paragraph 8 of the Information Management Act.

1. **Policies and procedures in cryptography**: The entity should create policies and procedures regarding the use of cryptography to protect the confidentiality, authenticity and integrity of data as required. (See section 8.1.)

2. **Data encryption technologies**: Data encryption can be necessary e.g. when data is transferred in an open data network or stored without sufficient physical protection. In such cases, an encryption technology with sufficient protection in relation to the quality, encryption classification, protection duration and performance requirements of the encrypted data should be selected. In terms of encryption technologies, in addition to algorithms, uses and key strengths, the availability of keys and their secure storage, creation and management must also be taken into account. (See section 8.2.)

3. **Encryption lifecycle**: The requirements of the encryption method used should be up to date throughout the lifecycle of the system, meaning that the encryption algorithm should be changeable (crypto-agility). (See section 8.3.)

8.1 Policies and procedures in cryptography

Example implementation
This section extends section 11.8 on baseline information security practices. • As a part of its risk management, the entity has identified data that require cryptographic protection. • The entity has defined policies related to cryptography, such as the encryption products used when transferring and storing data.
Verification
1. The supervisory authority verifies from documentation that the entity has identified and classified assets that are to be protected by cryptographic methods to ensure confidentiality (e.g. encryption), authenticity (e.g. signature) and integrity (e.g. hash). The documentation also describes policies regarding cryptography, which can entail e.g. defining authorised encryption products and any related configurations.

Explanations

Data encryption can prevent data from ending up with an unauthorised person in a legible format. Currently, it is reasonably easy to encrypt data in many systems. For example, the encryption of web traffic is a common measure nowadays. Likewise, most operating systems offer drive encryption with only a couple of clicks. Cryptographic procedures can also ensure that the data have not been changed intentionally or unintentionally and that the data come from the correct source. These measures can aim to prevent malicious material from ending up in the information systems or ensure that stored data is not corrupted.

References

ISO/IEC 27002:2022 (5.31, 5.37, 8.24)

IEC 62443-2-1:2024 (ORG 1.1, DATA 1.5, DATA 1.6)

IEC 62443-3-3:2013 (SR 4.3)

NIST CSF 1.1 (PR.DS-1, PR.DS-2, PR.PT-4)

NIST CSF 2.0 (PR.DS-01, PR.DS-02, PR.IR-01, PR.AA-06)

NIS CG Reference document (3.10.1 Policies and procedures on cryptography)

NIS CG Implementing guidance (9. Cryptography)

Tools

Julkri (TEK-16)

Kybermittari (ARCHITECTURE-5)

8.2 Data encryption technologies

Example implementation

- The entity's procedures on cryptography define the protocols to be used in addition to encryption algorithms, strengths and products, among others.
- The procedures and operating methods related to cryptography are proportionate to the data protection needs, such as classification and storage period as well as performance requirements.
- The entity has defined the management of cryptographic keys (including certificates and similar) so that it supports the encryption needs. Matters to take into account include e.g. the following:
  - Ensuring key availability, which includes key distribution and key backups, among others

- Key lifecycle management, such as creation, exchange, storage, revoking and destruction
- Technical features of the keys, such as length, rights and service life
- Revoking compromised keys and
- Logging key-related events.

Verification

1. The supervisory authority verifies from documentation that the entity has defined procedures and operating methods on cryptography so that they are proportionate to the need to protect data. The entity has identified the cases where data is transferred or stored without sufficient protection and where the use of encryption is necessary. The entity has selected an encryption technology with sufficient protection in relation to the quality, encryption classification, protection duration and performance requirements of the encrypted data. The reviewed details in terms of encryption include the algorithms used, sufficient in terms of the protection requirements, uses of encryption and key strength. In terms of the length and complexity of keys (in particular, symmetrical keys, pre-shared keys), attention must be paid to key management. Things to take into account in key management include the secure storage, availability, secure creation and lifecycle management of keys. The creation can be verified e.g. by creating keys in a secure, often isolated, target with sufficient entropy. Details to take into consideration in lifecycle management include key removal and renewal.
2. The supervisory authority verifies e.g. with interviews and configuration reviews that the defined policies on cryptographic methods are implemented. This can be implemented e.g. by reviewing the services using encryption and their encryption-related definitions, such as algorithms, key creation procedures and the secure storage of keys.
3. The supervisory authority verifies the use of sufficient encryption e.g. by scanning services, systems or software that produce encrypted traffic. For example, these scanning software can check the encryption algorithms that the service will approve. The algorithms used should correspond to the definitions. Furthermore, the validity period of keys (certificates, in particular) can be reviewed against well-known good practices.

Explanations

The efficiency of data encryption is almost fully based on the selected encryption algorithms and key management, in particular. Weak encryptions are easy to breach. A compromised or weak key can in turn destroy the benefits of encryption entirely. If the key is not destroyed reliably and it ends up in the wrong hands, it can be used to decrypt all traffic encrypted with it. The availability of the encryption key is equally important, so that the encrypted data can be used when it is needed.

References

ISO/IEC 27002:2022 (8.24)

IEC 62443-2-1:2024 (DATA 1.5, DATA 1.6)

IEC 62443-3-3:2013 (SR 1.8, SR 1.9, SR 3.1, SR 4.1, SR 4.3)

NIST CSF 1.1 (PR.DS-1, PR.DS-2, PR.PT-4)

NIST CSF 2.0 (PR.DS-01, PR.DS-02, PR.IR-01, PR.AA-06)

NIS CG Reference document (3.10.1 Policies and procedures on cryptography)

NIS CG Implementing guidance (9. Cryptography)

CISA: Quantum-Readiness: Migration to Post-Quantum Cryptography

On the State of Crypto-Agility

Tools

Attack surface mapping Hyöky.fi

Julkri (TEK-04.2, TEK-05.1, TEK-16)

Kybermittari (ARCHITECTURE-5)

Scanning software: Nessus, nmap, sslscan

8.3 Encryption lifecycle

Example implementation

- The entity has maintained the selected encryption technologies in such a way that encryption technologies that have proven to be weak have been replaced with new, stronger alternatives, if necessary. In the future, this will be particularly evident in the adoption of post-quantum cryptography (PQC).
- The entity has implemented its encryption-related arrangements in a way that makes changing the encryption and encryption keys as easy as possible. For example, this means changing the service configurations into new, stronger encryption technologies, certificate lifecycle management and using keys in services and products in a way that enables them to be changed with reasonable effort.

Verification

1. The supervisory authority verifies from documentation that the entity has implemented its encryption and cryptographic methods in such a way that e.g. the change of encryption algorithms and keys can be implemented with reasonable effort. The option of changing the encryption algorithms and keys may also be included in the acquisition process, e.g. in requirements defined by the entity in relation to product selections.

2. The supervisory authority verifies, e.g. by reviewing configuration, that the cryptographic arrangements support lifecycle management. For example, this means that the parameters related to cryptography are not hardcoded into software, but that they can be managed e.g. with configuration files.

Explanations

As computing capacity increases and algorithms break, encryption methods end up in a state where their breaking may even become trivial. For this reason, the changing of encryption parameters should be made as easy as possible. In the future, the development of quantum computers may also cause increased need to change the encryption used. This must be taken into account particularly in systems that have a long lifecycle or high security needs.

The lifetime of certificates is limited. It is also true that encryption keys may sometimes become compromised accidentally or intentionally. For this reason, changing the keys should also be simple so that the encryption strength does not weaken due to the weakness of a key.

References

ISO/IEC 27002:2022 (8.24)

IEC 62443-2-1:2024 (DATA 1.5, DATA 1.6)

IEC 62443-3-3:2013 (SR 4.3)

NIST CSF 2.0 (ID.AM-08, PR.PS-06)

NIS CG Reference document (3.10.1 Policies and procedures on cryptography)

NIS CG Implementing guidance (9. Cryptography)

Tools

Julkri (TEK-16)

Kybermittari (ARCHITECTURE-5)

9 Incident detection and handling in order to maintain and recover security and reliability

These recommendations are based on Article 21(2)(b) of the NIS2 Directive. The national implementation of this point is laid down in section 9, subsection 2, paragraph 9 of the Cybersecurity Act and in section 18 c, subsection 1, paragraph 9 of the Information Management Act.

1. **Incident response procedures**: For incident response, the entity should have pre-documented procedures, roles and responsibilities on incident prevention, detection, analysis, management, recovery and reporting. (See section 9.1.)

2. **Incident reporting channels**: The entity should have reporting channels for internal and external operators for the purposes of incident detection. (See section 9.2.)

3. **Event logging and detection**: As a rule, the entity should have tools and processes for the purposes of event logging and detection. It would be necessary for the detection and analysis ability that the entity collects and uses sufficient log data on matters such as maintenance, changes, use and errors. (See section 9.3.)

4. **Incident analysis and classification**: The entity should for example assess relevant events to investigate whether they cause an incident. The entity should have practices for assessing and, if necessary, classifying the severity and impact of an incident. (See section 9.4.)

5. **Incident handling**: Incident handling should also involve practices for incident response, and as necessary, incident limitation, resolution and the elimination of effects. (See section 9.5.)

6. **Root cause analysis and learning from experiences**: After an incident, the entity should strive to assess the causes that led to the incident and learn from the experience to better prepare for similar incidents in the future. (See section 9.6.)

7. **Additional recommendations for significant incidents**: There should be procedures, responsibilities and communication channels in place for warning other operators in the case of significant incidents. (See section 9.7.)

8. **Security of information sharing**: Incident handling should also contain procedures for information sharing that does not compromise the entity or other organisations. (See section 9.8.)

9. **Incident response lifecycle management**: Incident handling procedures should be maintained and developed throughout their lifecycle and updated based on experiences. (See section 9.9.)

9.1 Incident response procedures

Example implementation

This section extends section 11.12 on baseline information security practices.

- The entity has comprehensive incident response procedures – and policy if necessary – that describe the measures of incident handling. The measures include e.g. incident prevention, detection, analysis, handling and recovery. Incident response procedures may refer to other documents, if necessary, if these describe the essential content. For example, incident prevention may refer to the entity's cybersecurity risk management procedure and risk management measures.
- Incident response procedures contain the necessary roles and reporting and communication channels. It is recommended that a communications plan is prepared for incidents so that the necessary internal and external communications are defined beforehand. Furthermore, the procedures describe measures related to incident handling, such as incident classification (categorisation), measures related to severe disruptions and reporting. Further information on security-related roles in section 6.1 Human resources security procedures.
- Incident response procedures contain sufficient documentation that describes operations during the handling of the incident. For example, this can mean measures and resources related to investigating an incident.
- After severe incidents in particular, it may be useful to hold a debriefing session among the people that took part in the handling of the incident. This means that similar incidents can, at best, be avoided in the future and operations in incidents can be improved. This measure also promotes the creation of a final report included in the NIS2 incident notification.
- The entity can create e.g. the following instructions for incident response:
  - Incident response playbooks
  - Instructions and tables related to escalation
  - Contact lists
  - Templates
- Incident response procedures describe the relationship between continuity (Business Continuity Plan, BCP) and incident response. Incident response also describes measures related to recovery. This is often a separate document (Disaster Recovery Plan, DRP).
- Incident response procedures describe the statutory requirements for incident response.

Verification

1. The supervisory authority verifies from documentation that the entity has procedures related to incident response. These are in writing and located in a place where they are available when incidents occur. In addition to these

procedures, the entity has defined roles and responsibilities for the different stages of incident response. These include incident prevention, detection, analysis, management, recovery and reporting. The content of these procedures may be made up of the following matters described in sections 1 Risk management policy, 9 Incident detection and handling and partly in section 10 Backup management, recovery planning:

- Incident prevention. Incident prevention may refer to the entity's cybersecurity risk management procedure and risk management measures (see section 1).
- Incident detection. Incident detection procedures describe the means used to detect incidents. These can include detection systems or communication channels (see section 9.3).
- Incident analysis. There should be classification criteria for the purposes of incident analysis that are based e.g. on direct and indirect impact, scope, time and resources. If necessary, the analysis can also describe more technical procedures (see section 9.4).
- Incident management and recovery. These can utilise the necessary specifying documents or sections, such as the communications plan and those linked to continuity and recovery (BCP, DRP) (see section 10.1).
- Incident reporting channels (see 9.2).
- Internal roles and responsibilities. This covers roles required during incident response, including e.g. internal and external communications (see sections 2.2, 9.7), human resources required for incident resolution and management This may have been implemented with a crisis (group) created in an agreed process.
- The procedures should also describe statutory requirements. These include NIS notifications, notification requirements related to data breaches and the consequent procedures.

2. Furthermore, the supervisory authority can verify that the procedures are complied with by using event logs, tickets, interviews and other similar sources.

Explanations

Incident response procedures are an essential part of preparedness. A well-planned operation during an incident can make incident handling faster and smoother as well as help with incident classification, ensuring a proportionate response.

A communications plan as a part of roles is a central tool in many incidents. It ensures that information reaches the correct people and can also prevent extraneous communications that make the situation worse, e.g. several reports on the same incident.

References

ISO/IEC 27002:2022 (5.24, 5.30)

ISO/IEC 27035-1:2023 (4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7.1, 5.1, 5.2)

ISO/IEC 27035-2:2023 (4.3, 6.2, 6.4, 6.7, 7)

IEC 62443-2-1:2010 (4.3.4.5.1, 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4)

IEC 62443-2-1:2024 (EVENT 1.1, EVENT 1.8)

IEC 62443-2-4:2024 (SP.08.01, SP.08.02, SP.08.03)

NIST CSF 1.1 (RS.RP-1, RS.CO-1, RS.IM-2)

NIST CSF 2.0 (GV.SC-08, RS.MA-01, PR.AT-01, ID.IM-03)

NIST SP 800-61 rev 2 (2.1, 2.2, 2.3, 2.4, 2.5, 3.1)

NIS CG Reference document (3.11.1 Incident handling policy)

NIS CG Implementing guidance (3.1 Incident handling policy)

Tools

Julkri (HAL-08)

Kybermittari (CRITICAL-3, RESPONSE-1, RESPONSE-2, RESPONSE-3, RESPONSE-4, RESPONSE-5)

9.2 Incident reporting channels

Example implementation

- The entity has a reporting channel where personnel, suppliers, vulnerability researchers, authorities and clients can report incidents, suspected incidents, vulnerabilities and other similar observations.
- The entity ensures that the personnel are aware of the reporting channel. In addition, the reporting channels are communicated to external operators.
- The reporting channel is confidential as necessary. People processing the reports are aware of the report processing practices. This applies especially when they contain e.g. personal data or other data, the processing of which is subject to statutory requirements.
- In defining reporting channels, situations where the normal reporting channels may be compromised due to an incident must also be taken into account. The key thing is to identify such a possibility and create a backup plan or alternative independent channels with these situations in mind.

Verification

1. The supervisory authority verifies that the entity has reporting channels available e.g. to personnel, suppliers, vulnerability researchers, authorities

and clients. The reporting channels are implemented in a way that makes them easy to find in relation to the need and accessible to users. The reporting channels must acknowledge situations where the reporting channel is compromised. For example, email cannot be used when the email service is possibly being controlled by an attacker (see section 10.4).

2. If necessary, the functioning of the reporting channels can be tested e.g. by having the entity make an example report through the channels and the supervisory authority monitor the processing of the report.

Explanations

References

ISO/IEC 27002:2022 (6.8)

ISO/IEC 27035-1:2023 (4.7.2, 5.2)

IEC 62443-2-1:2010 (4.3.4.5.3, 4.3.4.5.4, 4.3.4.5.5)

IEC 62443-2-1:2024 (EVENT 1.2, EVENT 1.3, EVENT 1.8, EVENT 1.9, ORG 1.1)

IEC 62443-2-4:2024 (SP.03.03, SP.08.01)

NIST CSF 1.1 (RS.CO-1, RS.CO-2)

NIST CSF 2.0 (PR.AT-01, DE.AE-07, RS.CO-02)

NIST SP 800-61 rev 2 (3.1.1)

NIS CG Reference document (3.11.3 Event reporting)

NIS CG Implementing guidance (3.3. Event reporting)

Tools

Kybermittari (RESPONSE-1, WORKFORCE-2)

9.3 Event logging and detection

Example implementation

This section extends section 11.13 on baseline information security practices.

- The entity has processes and tools for incident detection. Furthermore, the entity is able to detect events that impact security and process them according to their criticality.

- The entity has gathered a log of its network and information system in the required extent and accuracy. In order to achieve a comprehensive detection ability, log data has been collected e.g. from the following events where possible:
  - Network traffic going out and in
  - User creation, change and destruction and adding access rights.
  - Events related to the access control of systems and applications
  - Administrator measures or measures carried out with elevated privileges in systems, services and software
  - Processing of configurations and backup files essential for operations or security, including reading, changing and destroying
  - Log produced by security-related systems and applications (e.g. endpoint detection and response EDR, intrusion detection system IDS, firewall, remote access points)
  - System resource use and performance
  - Functions related to physical access or use (e.g. access control), if necessary
  - Access and use of network and communication devices
  - Events related to the environment (e.g. condition alerts), if necessary
  - Change regarding a log source and its security, such as turning on and off and suspending
- Logs have enabled the detection of abnormal or undesired events. Monitoring is as automatic as possible, while taking into account the risk management need and resources. Alerts of observations are created automatically, if possible. Analytics can also be used to monitor trends. If necessary, one way to replace automation is regular reviews. There is a process and resources for the processing of alerts. If necessary, the entity may have used solutions such as a network operations centre (NOC) or security operations centre (SOC).
- Log data are stored for a sufficiently long period and they are backed up as possible and as necessary. The storage period can depend e.g. on needs based on legislation, criminal law or risk management. For example, six months may be sufficient in terms of risk management for less critical log data, whereas criminal law may require a storage period of several years.
- Log data should primarily be exported to a separate device that is isolated from the rest of the system. Furthermore, the entity has implemented task separation so that a person with access to the log server cannot access the log sources (and vice versa). These measures can usually avoid the destruction of evidence in cases of misuse. If the separation of tasks is not possible, e.g. due to resources, the entity has implemented sufficient replacement measures to reduce the risk.
- The entity has a reliable, centralised time source, and all log sources should be configured so that the log time stamps can be combined.
- The entity has maintained an up-to-date list of different log sources, and the status of these sources and the functioning and availability of monitoring have been reviewed regularly.

- The processing and storing of log data take into account any requirements related to legislation or regulation. There must be sufficient storage space reserved for logs and usually an alert if the storage space is about to become full.
- In terms of log data and detection, events related to physical security have also been taken into account, especially when physical security produces cybersecurity risk management means.

Verification

1. The supervisory authority verifies the entity's event logging and detection ability by making use of existing documentation. Such documentation can include e.g. log policies, descriptions of log sources and log content, statutory requirements on logs and monitoring, monitoring system descriptions, monitoring process descriptions and log system descriptions. Furthermore, screenshots or samples of the log and monitoring systems can be requested to indicate the functionality and coverage of the system in relation to the size of the sample (see example implementations). The handling of observations based on logs can be verified e.g. from processing history, with interviews and from monitoring views.
2. The status of log and monitoring systems can be verified by inspecting the configurations and monitoring views of different systems with the entity's assistance, if necessary. Interviews can also be used for this purpose. Depending on the size of networks and information systems, the configurations related to the creation of log data in different devices, services or other resources can be examined either as a sampling or in its entirety. The sampling must at least include devices on the outer edges of the network and information system (e.g. firewall, remote access point, encryption device), key resources for operations and security, as well as other most critical assets picked from risk management and the asset list. The sampling should also contain a group of other targets in order to achieve sufficient coverage. In terms of the logs selected for the sampling, it is verified that logs are created for all central systems (see example implementation above), their content is comprehensive in relation to the entity's needs, their timestamps are consistent, logs are transferred to a log system and that logs are stored for a sufficiently long time and sufficient storage space is reserved for them. The storage period should be in the right proportion compared to needs based on legislation, criminal law or risk management. Storage periods can vary from one system to another and could even be years. The detection of the functionality of log sources can be reviewed e.g. by inspecting the related rules from the monitoring system. Event logs that are created e.g. manually can be inspected with a review. The related reviews and incident detection can use interviews and any other information, such as incident-related tickets.
3. The logging and detecting ability can be tested e.g. by monitoring the alerts produced. The entity's maintenance staff or information security auditors can offer help here. Testing can simulate different abnormal events, monitor the generation of the event log and ensure that an alert of the event is generated. A simulated event can be e.g. a failed login attempt, the use of

maintenance accounts, attempted execution of an unauthorised but secure software or bringing an EICAR test virus file into the system. However, testing must ensure that it does not cause a threat to the system. Any extraneous accounts, files and access rights must be cleared out after testing.

Explanations

Incident detection ability is important in order to identify any cyber threats as early as possible. Event logging enables the analysis of events after the fact, and in most cases, it is impossible to find out the root causes of an incident without a comprehensive log.

Log systems and monitoring should be kept separate from the rest of the system, also in terms of roles. These systems usually provide evidence that something bad has happened. In these events, it is important that no one is able to destroy evidence. If necessary, these systems could also produce evidence of the maintenance staff not producing the incident even when such is suspected.

It is typical that incidents are not noticed in time. In particular, it can take notably long to detect the initial access gained by an attacker. For this reason, detection ability is important as, at best, it can prevent a severe incident from occurring.

References

ISO/IEC 27002:2022 (5.24, 5.28, 8.15, 8.16, 8.17)

ISO/IEC 27035-1:2023 (4.7.3, 5.3)

IEC 62443-2-1:2010 (4.3.3.6.4)

IEC 62443-2-1:2024 (EVENT 1.4, EVENT 1.5, EVENT 1.8, DATA 1.1, NET 1.9)

IEC 62443-2-4:2024 (SP.03.04, SP.08.01, SP.08.02, SP.08.03)

IEC 62443-3-3:2013 (SR 1.11, SR 1.12, SR 1.13, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 6.1, SR 6.2)

NIST CSF 1.1 (DE.CM, RS.AN-1)

NIST CSF 2.0 (DE.AE-06, DE.CM, RS.MA-02, RS.AN-07)

NIST SP 800-61 rev 2 (3.2, 3.2.1, 3.2.2, 3.2.3, 3.2.5)

NIS CG Reference document (3.11.2 Monitoring and logging)

NIS CG Reference document (3.11.4 Event assessment and classification)

NIS CG Reference document (3.11.5 Incident response)

NIS CG Implementing guidance (3.2. Monitoring and logging)

NIS CG Implementing guidance (3.4. Event assessment and classification)

NIS CG Implementing guidance (3.5. Incident response)

Finnish Transport and Communications Agency instruction on recording information on traffic data processing (Traficom/376384/03.04.05.01/2022)

Tools

Attack surface mapping Hyöky.fi

Julkri (TEK-12)

Kybermittari (ACCESS-2, ACCESS-3, SITUATION-1, SITUATION-2, SITUATION-3)

Incident testing: EICAR test virus file https://www.eicar.org

9.4 Incident analysis and classification

Example implementation

- The entity has identified security-related incidents from log data and analysed the impact and severity of the incidents based on a set of criteria. Assessing the severity of an incident can be based e.g. on the material or non-material damage and financial loss caused by the incident, the extent to which the functioning of the service is affected, the duration of the incident and the number of affected recipients of services.
- If necessary, the entity has procedures for log analysis and correlation which improves the detection of incidents. The entity should be able to reassess old incidents in the light of new threat information (see section 1.4).
- If necessary, the entity has a system that automatically analyses and correlates log data and utilises the generated data e.g. as a part of its threat hunting (threat intelligence).

Verification

1. The supervisory authority can verify the implementation of incident analysis and classification e.g. from documents describing incident response procedures. The entity has described the procedures related to the analysis of events. The entity should have clear criteria for identifying events as incidents, classifying incidents and assessing whether the incident is a significant incident in accordance with the Cybersecurity Act. This classification should be unambiguous and be based e.g. on legislation and classifications inherited from asset management. The classification is dependent on the case, but the assessment of the severity of an incident can be based e.g. on the material and non-material damage and financial loss caused by the incident, the extent to which the functioning of the service is affected, the duration of the incident and the number of affected recipients of services. The implementation of the procedures can be verified e.g. from

tickets and with interviews. This can make use of detected incidents and examination of the related implementations.

2. If the entity has the need and ability to carry out automatic log data analysis and correlation, the supervisory authority can verify the related procedures and operating methods from documentation. In addition, the functionality of the system performing the analysis and comparison and the experts' ability to carry out analysis can be reviewed. Interviews and e.g. the ticketing system can be used to verify that analysis and comparison have been carried out and that it has had an impact if necessary. This can be evident e.g. in the changes caused by the findings that can be verified from the change management log.

Explanations

The purpose of incident analysis and classification is to have incident management measures be as proportionate as possible. This means that e.g. extra resources are not inadvertently used to resolve an incident with non-existent impacts, but also that significant incidents are identified in time in order to manage severe consequences.

It is often typical for more advanced attacks that the initial access is gained notably sooner than the actual damage is caused. For this purpose, some entities may have a risk-based need to analyse incidents automatically e.g. based on correlation.

References

ISO/IEC 27002:2022 (5.25)

ISO/IEC 27035-1:2023 (5.4)

ISO/IEC 27035-2:2023 (6.5, 6.6)

IEC 62443-2-1:2010 (4.3.4.5.6, 4.3.4.5.7)

IEC 62443-2-1:2024 (EVENT 1.7)

IEC 62443-2-4:2024 (SP.08.01)

NIST CSF 1.1 (DE.AE-4, RS.AN-2, RS.AN-4)

NIST CSF 2.0 (DE.AE-03, DE.AE-04, DE.AE-07, DE.AE-08, RS.MA-03, RS.MA-04, RS.MA-05, RS.AN-08)

NIST SP 800-61 rev 2 (3.2, 3.2.4, 3.2.6, 3.2.7)

NIS CG Reference document (3.11.4 Event assessment and classification)

NIS CG Implementing guidance (3.4. Event assessment and classification)

Tools

Julkri (TEK-13)

Kybermittari (SITUATION-2, SITUATION-3)

9.5 Incident handling

Example implementation

- The entity has written procedures for incident handling. These procedures cover:
  - Practices for reacting to incidents
  - Measures that prevent the more severe consequences and the spreading of the incident
  - Resolving the incident, i.e. discovering and removing the impact and cause of the incident.
- Incident resolution must ensure that the incident is prevented from reoccurring in the future.
- The entity has created prerequisites for handling significant incidents (see 9.7) and, if necessary, for reporting minor incidents to the national CSIRT and/or supervisory authority.
- The work leading to resolving the incident should be documented with such detail that it is possible to later be used in reporting (see 9.7) and to be learned from (see 9.6).

Verification

1. The supervisory authority verifies e.g. from documentation that the entity has procedures related to incident handling. The procedures describe the practices used for reacting to incidents.

   The reaction practices can include e.g. measures related to incident response, such as measures that minimise the impacts of the incident and prevent the incident from spreading to other operators and systems, among others. The documentation should also indicate the procedure for preventing the impact and occurrence of the incident in the future. In order to achieve this, documentation should show that extensive investigation of the incidents is carried out and that the entity itself has sufficient competence for this purpose or that it procures it from a third party. The above-mentioned should be considered against the fact that new incidents can be caused by an old incident not being examined sufficiently in the past. In order to prevent the impact of the incident from increasing and spreading, the entity has sufficient knowledge of bodies who may be affected by the incident. Informing the above-mentioned bodies must take place rapidly, clearly and be allocated to designated people (see section 9.7). Furthermore, obligations arising e.g. from legislation must be taken into account. These and the related responsibilities should be clearly recorded.

2. The supervisory authority examines the implementation of the procedures, where possible. This work can make use of interviews, documentation from incident handling, such as tickets and logs, and changes and communications.

Explanations

References

ISO/IEC 27002:2022 (5.24, 5.25, 5.26, 5.37)

ISO/IEC 27035-1:2023 (4.7.4)

IEC 62443-2-1:2010 (4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8, 4.3.4.5.9, 4.3.4.5.10)

IEC 62443-2-1:2024 (EVENT 1.7, EVENT 1.8, ORG 1.1)

IEC 62443-2-4:2024 (SP.08.01)

NIST CSF 1.1 (PR.IP-9, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-3, RS.MI-1, RS.MI-2, RC.RP-1, RC.CO-1, RC.CO-2, RC.CO-3)

NIST CSF 2.0 (ID.IM-04, RS.MA-01, RS.MA-04, RS.CO-03, RS.AN-06, RS.MI-01, RS.MI-02, RC.RP-01, RC.CO-03, RC.CO-04)

NIST SP 800-61 rev 2 (3.3, 3.3.1, 3.3.2, 3.3.3, 3.3.4)

NIS CG Reference document (3.11.5 Incident response)

NIS CG Implementing guidance (3.5. Incident response)

Tools

Julkri (HAL-08, TEK-13)

Kybermittari (CRITICAL-3, SITUATION-3, RESPONSE-3)

9.6 Root cause analysis and learning from experiences

Example implementation

- After significant incidents, in particular, the entity carries out a review of its incident response. This includes factors related to incident detection, management and resolution.
- If the entity has detected shortcomings in the handling of an incident, the entity has improved its methods, instructions and resources, such as abilities or competences.

Verification

1. The supervisory authority verifies from documents that the entity has practices in place for root cause analysis (RCA) and learning from experiences. Root cause analysis and learning from experiences make use of documentation. The measures of root cause analysis should be described and allocated to designated people. The necessary competence and resources should be available. Learning from experiences should be one of the measures of the incident response procedures.
2. The supervisory authority verifies the entity's significant incident from the materials related to its handling and with interviews. The purpose is to check that the entity has implemented root cause analysis and learned from the experience. Learning from experience can be verified e.g. by reviewing that the entity has planned or implemented corrective measures after the incident.

Explanations

The purpose of root cause analysis and learning from experiences is to find practices that can prevent the generation of incidents and enable better and more efficient operations in the future. Root cause analysis is a tool of regulatory requirements, helping the entity produce the final report of the NIS notification.

References

ISO/IEC 27002:2022 (5.27, 5.28)

ISO/IEC 27035-1:2023 (4.7.5, 9.6)

ISO/IEC 27035-2:2023 (9.6)

IEC 62443-2-1:2010 (4.3.4.5.8, 4.3.4.5.11)

IEC 62443-2-1:2024 (EVENT 1.4, EVENT 1.5, EVENT 1.7, EVENT 1.8, ORG 1.1)

NIST CSF 1.1 (DE.AE-2, RS.IM-1)

NIST CSF 2.0 (DE.AE-02, ID.IM-03, RS.AN-03)

NIST SP 800-61 rev 2 (3.4.1)

NIS CG Reference document (3.11.6 Post-incident review)

NIS CG Implementing guidance (3.6. Post-incident review)

Tools

Kybermittari (RESPONSE-3, RESPONSE-4)

9.7 Additional recommendations for significant incidents

Example implementation

This section extends section 11.12 on baseline information security practices.

- Incident response procedures also cover the response to significant incidents. For this purpose, the entity has defined roles and responsibilities and communication channels e.g. to the necessary authorities.
- The entity has taken into account any sector-specific specifications in the definition of a significant incident and threshold values.
- The entity has planned the monitoring of situational development to identify any significant incidents and initiates the necessary measures in such situations.
- The entity has a communication plan and channels with parties potentially affected by the incidents in order to protect these operators.
- The entity has planned ways of assessing the financial losses caused by an incident and planned procedures for situations where financial losses are significant.
- The entity has defined procedures for initial and further notifications of significant incidents using the NIS notification form and the delivery of a final report.
- The entity is prepared to collect and submit the necessary Indicators of Compromise (IoC) for the investigation of the incident. This information is needed in a follow-up notification, for example.

Verification

1. The supervisory authority verifies that the procedures for significant incidents are described separately in documentation. Significant incident response procedures typically contain the escalation of the incident. The assessment and handling of significant incidents, as well as the needs related to communications and roles, should be clearly defined in the incident response procedures and related documents. Significant incidents often require different communications e.g. towards authorities, and this should be taken into account. In case of significant incidents, the security of information sharing (see section 9.8) and the related backup communication systems (see section 10.4) should be described and defined beforehand.

Explanations

References

ISO/IEC 27002:2022 (5.26, 5.29, 5.30)

ISO/IEC 27035-2:2023 (6.5, 6.6)

IEC 62443-2-1:2010 (4.3.4.5.3, 4.3.4.5.5)

IEC 62443-2-1:2024 (EVENT 1.2, EVENT 1.8, AVAIL 1.1)

IEC 62443-2-4:2024 (SP.08.01, SP.08.03)

NIST CSF 1.1 (ID.GV-2, ID.GV-3, RC.CO-3)

NIST CSF 2.0 (GV.RR-02, GV.OC-03, DE.AE-08, RS.AN-07, RS.AN-08, RC.CO-03)

Tools

Julkri (HAL-08, TSU-14)

Kybermittari (RESPONSE-2, RESPONSE-3, RESPONSE-5)

9.8 Security of information sharing in incidents

Example implementation

- The entity’s communication channels in connection with cybersecurity incidents are sufficiently secure in terms of their availability, confidentiality and integrity.
- The selection of communication channels should account for situations where ordinary communication channels are not available.
- Any information related to hostile activities is shared so that it does not end up with the attacker.

Verification

1. The supervisory authority verifies that the entity’s documentation defines such communication channels that are secure to use in an incident. The availability of communication channels is a central security feature, and situations where ordinary services are not available have been taken into account here (see section 10.4). Furthermore, the selection of communication channels should take into account that the shared information does not compromise different parties. This may have been implemented by means of encryption and other technology separate from the compromised system. The documentation and plans should also account for situations where an incident impacts the communication channel and then produce a backup plan and backup communication channel (see section 10.4). It should also be reviewed that the entity maintains and regularly tests the functioning of its communication channels.
2. The supervisory authority can also verify the security of information sharing by testing it. For example, the entity may be requested to send SMS via different communication channels. At the same time, it can be verified that the protections of messages, such as encryption, can be utilised.

Explanations

When an incident happens, it must be ensured that information related to the incident is shared securely. It is essential that this is defined beforehand, as the need for resources is directed elsewhere during an incident.

The security of information sharing must note several matters, such as if the information related to the attack is classified and therefore to be protected, how to prevent the attacker from accessing information and how the accessibility of information sharing is ensured. The information must be protected from the attacker so that it does not gain a benefit from knowing any weaknesses of the entity and cannot use the entity’s situational data from examining the attack.

References

ISO/IEC 27002:2022 (5.24, 5.26, 5.28, 5.29)

ISO/IEC 27035-1:2023 (4.6)

ISO/IEC 27035-2:2023 (4.2, 6.3, 6.8, 8.9)

IEC 62443-2-1:2024 (EVENT 1.4, EVENT 1.8, AVAIL 1.1)

IEC 62443-2-4:2024 (SP.08.01, SP.08.03)

IEC 62443-3-3:2013 (SR 4.1 RE 1)

NIST CSF 1.1 (PR.DS-2, PR.PT-4)

NIST CSF 2.0 (PR.DS-02, PR.AA-06, PR.IR-01)

NIST SP 800-61 rev 2 (3.4.2, 4.1, 4.2, 4.3)

NIS CG Implementing guidance (3.3. Event reporting)

NIS CG Implementing guidance (4.1. Business continuity and disaster recovery plans)

NIS CG Implementing guidance (4.2. Backup management)

NIS CG Implementing guidance (4.3. Crisis management)

NIS CG Implementing guidance (6.7. Network security)

NIS CG Implementing guidance (9. Cryptography)

NIS CG Implementing guidance (12.2. Handling of information and assets)

Tools

Julkri (TEK-16)

Kybermittari (RESPONSE-3, RESPONSE-5, ARCHITECTURE-5)

9.9 Incident response lifecycle management

Example implementation

- Cybersecurity incident response procedures are maintained and improved regularly and after significant incidents in particular.
- The entity keeps the roles, resources, incident classification criteria and other essential information related to incident response up to date.

Verification

1. The supervisory authority verifies from documentation that the entity has recorded the measures related to the regular development of procedures, such as planned update schedule and practices for updating issues learned from severe incidents.
2. The supervisory authority can verify the implemented development from change history and with interviews

Explanations

The regular maintenance of incident response procedures promotes incident response in a real situation. The continuous development of the procedures is important. However, it is natural that the resources related to incident response also change continuously, e.g. due to changes in personnel. There is generally no time for updating and figuring things out during an incident.

References

ISO/IEC 27002:2022 (5.24, 5.27)

ISO/IEC 27035-1:2023 (5.5)

ISO/IEC 27035-2:2023 (9, 10, 11, 12)

IEC 62443-2-1:2010 (4.3.4.5.8)

IEC 62443-2-1:2024 (EVENT 1.8, ORG 1.1)

NIST CSF 1.1 (PR.IP-7, DE.DP-5, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2)

NIST CSF 2.0 (ID.IM-03)

NIST SP 800-61 rev 2 (3.3.4, 3.4, 3.5)

NIS CG Reference document (3.11.1 Incident handling policy)

NIS CG Implementing guidance (3.1. Incident handling policy)

Tools

Julkri (HAL-08)

Kybermittari (RESPONSE-3, RESPONSE-5)

10 Backup management, disaster recovery planning, crisis management and continuity management of operations and, where appropriate, the use of protected backup/emergency communication systems

These recommendations are based on Article 21(2)(c) and partly (j) of the NIS2 Directive. The national implementation of these points is laid down in section 9, subsection 2, paragraph 10 of the Cybersecurity Act and in section 18 c, subsection 1, paragraph 10 of the Information Management Act.

1. **Continuity and recovery planning**: The entity should have documented procedures on the continuity of operations and recovery from disruptions. One way of ensuring continuity could be a continuity plan and a recovery plan created on the basis of risk management. The plans could contain the conditions where they are activated, plans for necessary roles, resources, measures and communication channels, and any necessary protected backup communication systems. The plans should include crisis management procedures for at least very serious incidents, or the entity should otherwise plan such procedures. In accordance with other risk management, the plans should be maintained and developed regularly, and operations complying with them should be practiced. (See section 10.1.)

2. **Backup copies and backup systems**: With regard to backup copies, the entity could for example define the backup copies of data, systems and backup systems that are required based on risk assessment. As a rule, the entity should have practices covering matters such as the frequency of backups, the retention period of backups, the protection of backups and the testing of recovery in situations where the original system is not available. The retention period of backup copies should be assessed in relation to the purpose of the retention, and backup copies should be taken sufficiently often so that functions can be recovered quickly enough and with sufficiently fresh data in case of incidents and crises. (See section 10.2.)

3. **Recovery testing and backup copy protection**: The functionality of recovery could be tested regularly to ensure functionality. Backups could for example be protected so that they are not subject to the same threats as the system that is being backed up. (See section 10.3.)

4. **Backup communication systems**: The need for the use of protected backup communication systems could arise from the fact that the risk assessment states it necessary to ensure communication channels also when the systems regularly in use (e.g. telephone, email, instant messaging) are not available. If there is a need for it, the entity could for example define the backup communication systems used and their need and implementation method. (See section 10.4.)

10.1 Continuity and recovery planning

Example implementation

- The entity has documentation describing the procedure for operational continuity and incident recovery. For example, the documentation includes a business continuity plan (BCP), disaster recovery plan (DRP) and business impact analysis (BIA) that are based on a risk assessment, operational requirements and legislation (see section 9.1).
- Continuity and recovery plans can include a description of situations where the processes and measures described by the plans are implemented, the order of the processes and measures, communication channels and personnel resources with roles, recovery procedures, dependencies on other systems, resources needed for recovery, interim arrangements and recovery objectives (see section 6.1).
- Continuity and recovery plans also describe measures, communication channels and identification definitions related to extremely severe incidents (crises) (see section 9.7).
- The continuity and recovery plans are maintained regularly and their processes, operating methods and resources are developed and practised, especially after significant incidents or changes in the business environment.

Verification

1. The supervisory authority verifies that the entity has documented procedures for operational continuity and incident recovery. For these purposes, the entity has at least a continuity plan and recovery plan based on risk management or documentation with comparable content. The plans contain comprehensive information based on which the measures of the plan are initiated. Furthermore, the plans contain the roles, resources, measures and communication channels used during incident response. The plans also deal with severe disturbances and crises where the entity or the entity’s operational environment face a situation severely disrupting the operations. The supervisory authority verifies that the plans have been maintained, developed and practiced regularly. These can be verified e.g. from documentation updating history or documents related to exercises. In its lightest form, the exercise can mean simulating the continuity and recovery procedures through discussion (so-called tabletop exercise).
2. The supervisory authority verifies e.g. with interviews that the entity’s continuity and recovery planning procedures are implemented in practice. This can be verified e.g. by ensuring that resources for the plans exist and persons are aware of their tasks in the implementation of the plans. Furthermore, the supervisory authority can examine the maintenance and exercise of plans with interviews. If the entity has experienced incidents where the plans have been used, the supervisory authority may extend its interviews to these incidents and review data related to them.
3. The supervisory authority may participate in the entity’s continuity and recovery planning exercise e.g. as an observer, in cooperation with the entity.

Exercises can also utilise cooperation between several operators and organise national cybersecurity exercises joined by authorities, operators and other cooperation partners.

Explanations

Continuity and recovery planning is an essential part of incident and crisis response. Pre-defined operating methods, resources, circumstances and communication channels promote recovery from incidents and the continuity of operations.

Practicing the plans beforehand typically speeds up recovery and makes it more straightforward. Even a tabletop exercise can help discover issues with the plans and prevent them from being implemented in a real situation.

References

ISO/IEC 27002:2022 (5.30, 5.37)

IEC 62443-2-1:2010 (4.3.4.5)

IEC 62443-2-1:2024 (ORG 1.1, EVENT 1.8, AVAIL 1.1)

IEC 62443-2-4:2024 (SP.12.09)

NIST CSF 1.1 (PR.IP-9-10, ID.BE-5, ID.SC-5, RC.RP-1, RC.IM-1, RC.IM-2)

NIST CSF 2.0 (ID.IM-02, ID.IM-03, ID.IM-04, GV.OC-04, GV.SC-08, RC.RP-01, RC.RP-02, RC.RP-04, RC.RP-05, RC.RP-06)

NIS CG Reference document (3.12.1 Business continuity and disaster recovery plans)

NIS CG Implementing guidance (4.1. Business continuity and disaster recovery plans)

Tools

Julkri (VAR-02, TEK-13, TEK-22.1)

Kybermittari (CRITICAL-3, RESPONSE-3, RESPONSE-4, RESPONSE-5)

National Cybersecurity Centre Finland's Cyber exercise instructions11

[11] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Instructions%20for%20organising%20cyber%20exercises.pdf

10.2 Backup copies and backup systems

Example implementation

This section extends section 11.11 on baseline information security practices.

- The entity has planned, implemented, tested and described its backup and recovery processes and backup copies.
- Backup copies have been made sufficiently frequently so that the systems and their data can be recovered with data that is sufficiently up to date (recovery point objective, RPO). Furthermore, the recovery systems should be scaled so that the recovery can take place sufficiently quickly (recovery time objective, RTO).
- The backup copies have been stored securely and for a sufficiently long time considering the business needs and statutory requirements.
- All necessary data and systems have been backed up. This should also take into account e.g. the backups of configurations and cloud services.
- The entity has rapidly deployable backup systems independent of other systems, containing abilities and capacity based on preparedness and related to factors such as premises, devices, network connections, information systems, communication channels and staff.
- Additional capacity may include reserving capacity from two different cloud service providers, preconfigured backup devices, or setting up the information system to be resilient with regard to critical functions. Ensuring capability can be achieved with substitute role arrangements and competence development.
- The entity’s backup copies and backup systems meet legislative and operative requirements.

Verification

1. The supervisory authority verifies that the entity has defined the data and systems that need to be backed up in order to ensure operational continuity. This definition has also taken into account the systems and data of which other services are dependent and whose functionality is therefore necessary for the operations. Furthermore, the supervisory authority verifies that the entity has sufficient backup systems, if necessary. Backup systems are described e.g. in the architecture descriptions and the plans described in section 10.2. In certain cases, backup systems can also replace some of the backup copying. The supervisory authority verifies that the entity has defined values for the storage period of backup copies and the frequency of backing up. The supervisory authority ensures that the values are in line with how much data the entity may lose in an incident and how quickly the data needs to be recoverable. The values can vary for different systems and data. The storage period of backups takes into account statutory requirements and various risk scenarios where the backups may be required after a longer period of time, e.g. due to undetected data corruption, long incident response

time or other such reason. The entity may have defined that backups are stored for a longer period of time in small numbers, e.g. so-called full backups are taken to a long-term storage once a month and the copies (e.g. incremental) are otherwise stored for a couple of weeks.

2. The supervisory authority verifies e.g. from screenshots or by reviewing systems that the entity has implemented the backup systems and backup copies described in point 1 of the verification. If the entity has experienced incidents, interviews and review of the related event log can be used to verify that the implementation of backup systems and backup management is sufficient.
3. Together with the entity, the supervisory authority can test the functionality of backup systems and backup recovery.

Explanations

In many incidents, particularly severe ones, backup systems and backup copies play an extremely important role in recovering the operations. Incidents can be intentional or unintentional, and in certain types of incidents in particular, such as attacks that encrypt all data, the existence of backup copies is particularly important.

Furthermore, some systems and them not working could cause massive issues with recovery. Also, these are often particularly desirable targets for attackers. They include e.g. services related to access control (e.g. Active Directory, AD), and their rapid recovery should be taken into account.

References

ISO/IEC 27002:2022 (8.13, 8.14)

IEC 62443-2-1:2010 (4.3.4.3.9)

IEC 62443-2-1:2024 (AVAIL 1.2, AVAIL 2.3)

IEC 62443-2-4:2024 (SP.12.01, SP.12.02, SP.12.03)

NIST CSF 1.1 (PR.IP-4)

NIST CSF 2.0 (PR.DS-11, PR.IR-03, RC.RP-03)

NIS CG Reference document (3.12.2 Backup and redundancy management)

NIS CG Implementing guidance (4.2. Backup management)

Tools

Julkri (TEK-20, VAR-02, VAR-07, VAR-08)

Kybermittari (CRITICAL-2, ASSET-2, RESPONSE-4)

10.3 Recovery testing and backup copy protection

Example implementation

This section extends section 11.11 on baseline information security practices.

- The recovery of backup copies and the functionality of backup systems should be tested regularly, primarily automatically. The testing should also inspect the integrity of backup copies. Backup recovery testing must be carried out in a secure way that does not compromise the production system.
- Backup copies must be stored in a secure place that is sufficiently separated from the backed up system based on the entity's risk management. This can mean some other premises or a separate combustion space. If necessary, backup copies can be stored in several formats whose recovery speeds may vary, e.g. drive backups and separate long-term archives.
- The protection of backup copies can acknowledge their need for integrity, availability and confidentiality. This means e.g. sufficient physical protection and other controls, such as encryption.

Verification

1. The supervisory authority verifies that, where possible and relevant, the entity has defined measures for the regular testing of backup copies and systems, e.g. once a week. This can be either automated or manual. The key thing is that in addition to mechanical recovery, it is also inspected that data can be recovered intact and usable and that any backup system can be established with correct data. The supervisory authority verifies that the backup copies are sufficiently protected. For example, architecture descriptions, system documentation or similar should describe how the backup system or a part thereof is separated from the rest of the system. This should ensure that if an attacker is able to access the network and information system, it does not get access to all backups.
2. The supervisory authority verifies with reviews and interviews how the entity tests the functioning of its backup copies where possible and relevant. This should include e.g. the measures taken to ensure the integrity of backup copies and the regularity of the testing. If necessary, the supervisory authority may also use physical reviews in ensuring that the backup copies are sufficiently separated from the rest of the system. The reviews should ensure e.g. that threats, such as fires, floods and person threats, do not apply to both the backed up system and the backup copies.
3. If justified logical separation is used instead of physical separation, the supervisory authority may use scanning and contact attempts performed by the entity to ensure that the separated backup copying system is inaccessible from the side of the backed up network and information system.

Explanations

In connection with recovering from an incident, it is far too often the case that recovery is not successful or that the attacker manages to destroy both the information system and the backup copies. For this reason, the comprehensive and regular testing of recovery and the protection of the recovery system can be vital for operations.

References

ISO/IEC 27002:2022 (5.33, 8.13, 8.14, 8.24)

IEC 62443-2-1:2010 (4.3.4.3.9)

IEC 62443-2-1:2024 (DATA 1.1, DATA 1.2, DATA 1.5, DATA 1.6, DATA 1.7, AVAIL 1.2, AVAIL 2.3)

IEC 62443-2-4:2024 (SP.12.01, SP.12.02, SP.12.03, SP.12.04, SP.12.05, SP.12.06, SP.12.07)

NIST CSF 1.1 (PR.IP-4, RC.RP-1, RC.IM-1, RC.IM-2)

NIST CSF 2.0 (PR.DS-11, RC.RP-01, RC.RP-05, ID.IM-03)

NIS CG Reference document (3.12.2 Backup and redundancy management)

Tools

Julkri (TEK-20, VAR-09)

Kybermittari (RESPONSE-4, ARCHITECTURE-1, ARCHITECTURE-5)

10.4 Backup communication systems

Example implementation

- Based on a risk assessment, the entity should have secure communication channels that enable sufficient and secure communications with the authorities, clients, service suppliers and other essential bodies. These systems should be such that they also function in severe disruptions and during crises. Also see section 9.8 Security of information sharing.
- These backup communications systems should be independent and separate from the functionality of other systems.
- A backup communication channel can be based e.g. on a courier procedure, alternative instant messaging service or mobile network.

Verification

1. The supervisory authority verifies that the entity has defined the necessary backup communication systems based on its risk assessment. Backup

communication systems are used when the regularly used systems are unavailable. These systems are mentioned e.g. in the plans described in section 10.1. In particular, the supervisory authority verifies that the selected backup communication systems are not dependent on the entity’s other infrastructure.

2. In cooperation with the entity, the supervisory authority verifies that the backup communication systems are functional. This can be implemented e.g. by sending SMS via the backup communication system.

Explanations

References

ISO/IEC 27002:2022 (5.5, 5.29, 5.30, 7.13)

IEC 62443-2-1:2024 (ORG 1.1, AVAIL 1.1, AVAIL 1.2)

IEC 62443-2-4:2024 (SP.08.04, SP.12.09)

NIST CSF 2.0 (RC.CO-03)

NIS CG Reference document (3.12.3 Crisis management)

NIS CG Implementing guidance (4.3. Crisis management)

Tools

Julkri (VAR-06, TEK-22.1)

Kybermittari (RESPONSE-3)

11 Baseline information security practices to ensure the security of operations, network and communication systems, hardware, software and applications

These recommendations are based partly on Article 21(2)(g) of the NIS2 Directive. The national implementation of this point is laid down in section 9, subsection 2, paragraph 11 of the Cybersecurity Act and in section 18 c, subsection 2, paragraph 11 of the Information Management Act.

The entity should use baseline information security practices to protect its network and information system. The entity should ensure that the necessary information security measures have been implemented and that employees comply with them. These information security practices – or cyber hygiene practices – should be scaled to the criticality of the activities. The selected measures should be based on general good practices and risk assessment.

Information security practices, or cyber hygiene practices, refer to general good practices on information security measures that ensure a appropriate level of using systems, programs and services securely. This would mean securing these targets with the baseline technical and other measures addressed above.

The recommendations on the baseline information security practices described in this section are drawn up in a way that also allows entities outside the scope of application of the NIS regulation to follow them and assess the maturity level of their organisation’s cybersecurity and improve it. The baseline information security practices are a light collection of all measures presented in this recommendation, meaning that they partly overlap with the other sections of the recommendation.

The supervisory authority can use the baseline information security practices in order to create an overall image of the cybersecurity level of supervised entities and the status of the sector.

The information security practices can contain both administrative and technical measures. The baseline information security practices presented in the recommendation are:

1. The entity has provided instructions on the baseline information security practices to personnel, subcontractors and other partners (see sections 11.1 and 11.1.1).

2. The entity has identified its most critical assets (see section 11.2).

3. The entity has secured its network and information system (see section 11.3).

4. The entity has separated its critical and vulnerable networks and information systems from other environments (see section 11.4).

5. The entity has secured its networks and information systems against malicious and unauthorised software (see section 11.5).

6. The entity has organised secure identification into its internal and external services and devices (see section 11.6).

7. The entity has separated the administrator accounts and accounts with elevated privileges from other accounts in its systems (see section 11.7).

8. The entity has ensured that its confidential data is processed securely (see section 11.8).

9. The entity has ensured that its systems are updated regularly and that critical updates are installed without delay (see section 11.9).

10. The entity has ensured that its services and devices are configured securely (see section 11.10).

11. The entity has ensured that its critical services and information assets are backed up (see section 11.11).

12. The entity is prepared to maintain its operations in severe incidents (see section 11.12).

13. The entity employs event logging of critical activities (see section 11.13).

11.1 The entity has provided instruction on the baseline information security practices to personnel, subcontractors and other partners

Example implementation
• The entity has written baseline information security practices and they are available to the personnel, subcontractors and other partners. These parties are also aware of the location of the documents. The practices are regularly reviewed and, where necessary, updated, e.g. once a year. • Baseline information security practices support the improvement of cybersecurity awareness. • Information security practices are in line with security policies and other sector-specific policies. There are contact persons and contact channels for information security practices. • The entity's baseline information security practices may include the practices presented in the recommendation. The entity has also included other measures in the practices in accordance with the risk assessment. • The measures may include good security practices that personnel adhere to, and security-related procedures used by the organisation.

Verification

1. The supervisory authority verifies that the entity has written baseline information security practices that are available to the entire personnel, subcontractors and other partners.

   Their content covers the operating methods described in the information security practices that include e.g. information security operating methods, notification channels, data and device processing instructions, password and account practices, remote access solutions, protection against phishing, protection against invoicing fraud and the identification of other common threats.
2. The supervisory authority verifies the awareness among the entity's personnel and the practical implementation of information security practices with interviews.

Explanations

The entity's personnel should know the baseline practices in order for the entity's general cybersecurity awareness to be considered to be on a reasonable level. When implemented correctly and comprehensively, the baseline information security practices can at best prevent the most common information security threats.

References

CCB CYFUN Basic (PR.AT-1)

ISO/IEC 27002:2022 (6.3)

IEC 62443-2-1:2010 (4.3.2.4.1, 4.3.2.4.2)

IEC 62443-2-1:2024 (ORG 1.4, ORG 1.5)

IEC 62443-2-4:2024 (SP.01.01)

NIST CSF 1.1 (PR.AT-1)

NIST CSF 2.0 (PR.AT-01)

NIS CG Implementing guidance (8.1 Awareness raising and basic cyber hygiene practices)

NIS CG Implementing guidance (8.2 Security training)

Tools

Julkri (HAL-13, HAL-15)

Kybermittari (WORKFORCE-1, WORKFORCE-2, PROGRAM-1, PROGRAM-2, General management measures)

11.1.1 Cyber awareness programme – extended instructions

Example implementation

This recommendation is intended for the supervision of entities from whom the supervisory authority expects a higher level of maturity.

- The entity has a training programme to increase cyber awareness among its employees. The purpose of the programme is to raise employee awareness of cybersecurity risks related to employees' work, the importance of cybersecurity, and general good practices for cybersecurity. The aim of the programme is to prevent the most common cyber incidents.
- The programme is intended for all employees, including senior management.
- The programme should be ongoing to reach all employees, including new hires.
- The programme should be based on the entity's existing cyber security practices so that it can remain relevant to their objectives.
- The programme should cover risk management measures relevant to employees, plus contact channels and other resources, such as contact persons and data banks for cyber security guidelines, and general good practices related to cyber security.
- The programme must be updated regularly to keep it up to date.

Verification

1. The supervisory authority verifies that the entity has a training programme for cyber awareness. The programme, its objectives and the practices related to updating it should be in writing.

Explanations

Personnel play a major role in the realisation of an entity's cyber security. For example, the entity's staff may be subjected to a high volume of skilfully targeted social manipulation and phishing, where ordinary employees play a major role in prevention and detection. Various types of malware may also be spread by uninformed employees, but malware epidemics can be warded off with good cybersecurity awareness among employees.

References

ISO/IEC 27001:2022 (7.3)

IEC 62443-2-1:2024 (ORG 1.4)

IEC 62443-2-4:2024 (SP.01.01)

NIST CSF 1.1 (PR.AT-1)

NIST CSF 2.0 (PR.AT-01)

NIS CG Implementing guidance (8.1 Awareness raising and basic cyber hygiene practices)

Tools

Kybermittari (WORKFORCE-2)

11.2 The entity has identified its most critical assets

Example implementation

This baseline information security policy is introductory to sections 5.1, 5.2 and 5.3.

- The entity has identified targets critical to its operations. These targets are such that the entity cannot operate without them, are subject to sector-specific statutory requirements or whose data breach can cause great damage. The targets can be e.g. devices, software, applications or business-critical data.
- The entity has drawn up, communicated and made readily available practices in accordance with the network and information system security policy and instructions for asset management.
- The entity's asset management should be regular and consistent, and it should cover the critical activities and services, data resources and other material or non-material assets, such as the services, accounts and licences it uses, identified by the organisation.

Verification

1. The supervisory authority verifies that the entity has practices and instructions related to asset management. There is written evidence of the regularity and consistency of asset management. Asset management covers at least the key components of the operations. User instruction or training describes the security-related practices concerning these systems.

Explanations

The identification of critical assets and asset classification enable a risk-based approach. A risk-based approach to cybersecurity improves the entity's cybersecurity level by making it more systematic and less random in nature. The most important assets in terms of operations must receive particular attention, as a disturbance targeting them may cause great damage to the entity.

References

CCB CYFUN Basic (ID.AM-1, ID.RA-1))

ISO/IEC 27002:2022 (5.9, 5.12)

IEC 62443-2-1:2010 (4.2.3.4, 4.2.3.6)

IEC 62443-2-1:2024 (CM 1.1, CM 1.3)

IEC 62443-2-4:2024 (SP.06.02)

NIST CSF 1.1 (ID.AM-1, ID.RA-1)

NIST CSF 2.0 (ID.AM-01, ID.RA-01)

Tools

Attack surface mapping Hyöky.fi

Julkri (HAL-04)

Kybermittari (CRITICAL-1, ASSET-1, ASSET-2, ASSET-5)

11.3 The entity has secured its network and information system

Example implementation

This baseline information security policy is introductory to sections 3.8 and 3.9.

- The entity has restricted access to its services based on the principle of least privilege.
- The entity uses a solution that prevents malicious or undesired traffic from untrusted networks, such as a firewall.
- Depending on the entity’s risk management, it may also use solutions such as intrusion detection or prevention systems.
- There is at least simple documentation available of the entity’s network and information system, such as network descriptions and diagrams.

Verification

1. The supervisory authority verifies from documentation supplied by the entity that access to the entity’s services is restricted based on the principle of least privilege particularly from unsecure networks.

   The documentation shows that the entity has selected network protections in a manner that ensures they are sufficient based on the organisation’s risk management.

Explanations

Networks and information systems connected to the internet face considerable amounts of automated malicious traffic that looks for and abuses weaknesses in systems. Restricting access to services from authorised sources and by closing communications ports that are unnecessarily open can prevent most automated threats. A similar principle also applies between different trusted and partly trusted networks.

In designing its network, the entity should also take the structure of its internal network into account. The entity should aim to protect its internal network so that if an attacker manages to access a workstation in the network, it would be difficult for them to advance further in the network.

References

CCB CYFUN Basic (PR.AC-3)

ISO/IEC 27002:2022 (8.20, 8.21)

IEC 62443-2-1:2010 (4.2.3.5)

IEC 62443-2-1:2024 (NET 1.1, ORG 1.1)

IEC 62443-2-4:2024 (SP.03.02)

IEC 62443-3-3:2013 (SR 1.13, SR 3.1, SR 5.2, SR 7.7)

NIST CSF 1.1 (PR.AC-3)

NIST CSF 2.0 (PR.AA-03)

Tools

Attack surface mapping Hyöky.fi

Julkri (TEK-01, TEK-02)

Kybermittari (ACCESS-2, ACCESS-3, ARCHITECTURE-2, ARCHITECTURE-3)

11.4 The entity has separated its critical and vulnerable networks and information systems from other environments

Example implementation

This baseline information security policy is introductory to section 3.8.

- The entity has separated the systems that are very vulnerable or critical or whose compromise may lead to the compromise of the entire network or system. Such systems include e.g. management networks and management workstations.

- The separation can be carried out using a variety of techniques, such as physical or logical separation.
- The entity has secured its wireless networks so that they do not compromise other systems.
- The principle of least privilege is taken into account in the traffic between the separated networks of the entity (see section 11.3).

Verification

1. The supervisory authority verifies from documentation supplied by the entity that the entity has identified the most critical systems in its operations and separated them. These systems and the implementation of their separation is described. The separation must take into account public networks, the entity's own networks and any connections to third-party networks.

   In certain cases, like in very small networks or information systems, separation may be unnecessary in terms of risk management. The acceptance of residual risk based on risk management may be sufficient in these cases.

Explanations

The separation of networks is an important protective measure that protects e.g. the most vulnerable systems. In many cases, separation can prevent malicious traffic, such as ransomware, from spreading from one system and network to another. The separation of networks divides the information system into smaller and clearer sections, making filtering rules and other protective measures easier to manage. In the event of a problem, the investigation can target a more restricted section of the network due to separation, facilitating recovery.

References

CCB CYFUN Basic (PR.AC-5)

ISO/IEC 27002:2022 (8.22)

IEC 62443-2-1:2010 (4.3.3.4)

IEC 62443-2-1:2024 (NET 1.1)

IEC 62443-2-4:2024 (SP.03.02)

IEC 62443-3-3:2013 (SR 5.1)

NIST CSF 1.1 (PR.AC-5)

NIST CSF 2.0 (PR.IR-01)

Tools

Attack surface mapping Hyöky.fi

Julkri (TEK-01, TEK-02, TEK-04)

Kybermittari (ARCHITECTURE-2)

11.5 The entity has secured its networks and information systems against malicious and unauthorised software

Example implementation

This baseline information security policy is introductory to section 3.9.

- The entity has written policies for installing software and staying protected against malware. The entity has provided instruction to its personnel on the most common online frauds, such as phishing and scam messages.
- The entity should have an automatic system to manage installing and running software and the use of storage media.
- The entity has technical controls against malicious and unauthorised software. These may include malware protection, such as antivirus software for terminal devices and email services, intrusion detection or prevention systems, or a proxy server.

Verification

1. The supervisory authority verifies that the entity has instructions or practices for preventing the installation and execution of malicious or unauthorised software.

   Any adopted malware protections or software blocking the execution of programs are enabled and sufficiently up to date.
2. The supervisory authority requests the entity to verify how it has implemented the identification of malicious messages, the prevention of unauthorised external storage media and applications and keeping malware protections up to date.

Explanations

Malware are spread both in a targeted manner, e.g. via email and links, as well as through sources that appear reliable, such as software impersonating genuine ones. Phishing messages and other similar malicious messages are one of the most common cyber threats.

The spreading of malware can be prevented with both administrative and technical methods. Malware can be present in any software, e.g. due to supply chain attacks, or the software itself can increase the attack surface.

References

CCB CYFUN Basic (DE.CM-1, DE.CM-4, DE.CM-5)

ISO/IEC 27002:2022 (8.7, 8.19)

IEC 62443-2-1:2010 (4.3.4.3.8)

IEC 62443-2-1:2024 (COMP 2.1, COMP 2.2, COMP 2.3, CM 1.4)

IEC 62443-2-4:2024 (SP.10.01, SP.10.03)

IEC 62443-3-3:2013 (SR 3.2)

NIST CSF 1.1 (DE.CM-1, DE.CM-2, DE.CM-4, DE.CM-5, DE.CM-7)

NIST CSF 2.0 (DE.CM-01, DE.CM-02, DE.CM-03, DE.CM-09)

Tools

Attack surface mapping Hyöky.fi

Julkri (TEK-11)

Kybermittari (ASSET-3, ARCHITECTURE-3, ARCHITECTURE-4)

11.6 The entity has organised secure identification into its internal and external services and devices

Example implementation

This baseline information security policy is introductory to section 7.1.

- The entity has password practices that instruct in the selection of secure and unique account names and passwords and in the notification of compromised accounts.
- The use of secure and unique accounts and passwords can be promoted with the help of a password manager.
- The entity has identified the systems where stronger identification and authentication methods, such as multi-factor authentication (MFA), can and must be adopted.

Verification

1. The supervisory authority verifies that the entity has password practices and that they have been instructed to personnel. The practices contain instructions for reporting compromised accounts.

   The entity has analysed the need for strong authentication methods and implemented them where possible. The entity has a list of systems the use of which requires a strong identification and authentication method. The entity has a list of systems the use of which does not require strong identification and authentication methods, and grounds for not adopting strong identification and authentication methods for them.

Explanations

High-quality passwords and authentication methods based on multiple factors can prevent accounts from being broken into. If the same accounts are used in several places, the theft of one account allows the attacker unauthorised access into other systems as well. Such systems can include social media platforms where organisation accounts can be abused for malicious purposes. Weak passwords can compromise e.g. email accounts that can then be used to spread scamming or malware emails in the entity's name. These accounts can also allow the attacker to access the entity's internal systems.

References

CCB CYFUN Basic (PR.AC-1)

ISO/IEC 27002:2022 (5.15, 5.17, 8.5)

IEC 62443-2-1:2010 (4.3.3.6)

IEC 62443-2-1:2024 (USER 1.4, USER 1.5, USER 1.11, DATA 1.1)

IEC 62443-2-4:2024 (SP.09.01)

IEC 62443-3-3:2013 (SR 1.1, SR 1.7)

NIST CSF 1.1 (PR.AC-1, PR.AC-7)

NIST CSF 2.0 (PR.AA-01, PR.AA-03)

Tools

Julkri (HAL-14, TEK-07, TEK-08)

Kybermittari (ACCESS-1)

11.7 The entity has separated the administrator accounts and accounts with elevated privileges from other accounts in its systems

Example implementation

This baseline information security policy is introductory to section 7.5.

- The entity's personnel performing administrator or maintenance tasks has separate accounts for the performance of these tasks.

- The entity has practices for issuing and maintaining administrator accounts and accounts with elevated privileges. The practices define the lifecycle management of accounts, such as their issuing, changing and removal.
- Administrator accounts and accounts with elevated privileges must not be used for basic functions, nor should basic user accounts be used for administrator functions.
- Unnecessarily extensive access rights should be avoided. For example, users only have basic privileges to their workstations, unless the performance of their tasks requires workstation administrator privileges.

Verification

1. The supervisory authority verifies that the entity has practices for issuing and maintaining administrator accounts or accounts with elevated privileges and their authorised use. The separation of administrator accounts and accounts with elevated privileges from basic user accounts is taken into account in the practices.

   Administrator accounts and accounts with elevated privileges are only issued when needed and they are removed or modified e.g. when tasks or some other functional needs change.
2. The supervisory authority requests the entity to verify that administrator privileges are only issued to persons who need them in their tasks. Furthermore, the documented and configured administrator privileges can be compared.

Explanations

Administrator privileges enable causing notably more damage than limited basic privileges.

Administrator accounts are the most desirable targets for attackers due to the opportunities they offer. Therefore, it is vital that threats posed to these accounts are minimised.

References

CCB CYFUN Basic (PR.AC-4)

ISO/IEC 27002:2022 (5.15, 8.2)

IEC 62443-2-1:2010 (4.3.3.5)

IEC 62443-2-1:2024 (USER 1.4, USER 1.5)

IEC 62443-2-4:2024 (SP.09.04)

NIST CSF 1.1 (PR.AC-4, PR.AC-7)

NIST CSF 2.0 (PR.AA-05)

Tools
Julkri (TEK-04, TEK-07.2) Kybermittari (ACCESS-1, ACCESS-2, ACCESS-3, ARCHITECTURE-3)

11.8 The entity has ensured that its confidential data is processed securely

Example implementation

This baseline information security policy is introductory to sections 2.3, 3.2, 5.2, 8.1 and 9.8.

- The entity has practices for defining the confidentiality of data. The entity's practices contain written instructions on the processing of data, such as how and where confidential data is stored, processed, transferred between systems and destroyed.
- The secure practices have been instructed to the organisation's personnel, subcontractors and other partners that process confidential data.
- Confidential data is primarily transferred encrypted. Confidential data located on the devices used by the entity (computers, phones, external storage media) are encrypted as necessary, e.g. with drive encryption (see section 11.10).

Verification

1. The supervisory authority verifies that the entity has instructions on the practices for secure storage, processing, transfer and destruction of confidential data. If necessary, these practices also apply to subcontractors and other operators that process confidential data.
2. The supervisory authority makes use of e.g. interviews and reviews in examining the procedures related to confidential data. Interviews can e.g. verify how personnel process confidential data. Furthermore, the storage locations, storage methods and destruction practices can be reviewed on site or by using material supplied by the entity.

Explanations

Careless processing or transferring of data may reveal it to unauthorised users. There may also be statutory requirements for confidential data, e.g. the EU General Data Protection Regulation (EU) 2016/679[12] or sector-specific

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on

requirements. In case of devices or storage media disappearing, e.g. in the case of theft, it is important that the lost device is encrypted. This prevents unauthorised users from accessing the data in the device.

References

CCB CYFUN Basic (PR.DS-1, PR.DS-2)

ISO/IEC 27002:2022 (5.12, 5.14, 5.33, 5.34, 7.1, 7.9, 7.10, 8.3, 8.24)

IEC 62443-2-1:2010 (4.3.4.4)

IEC 62443-2-1:2024 (DATA 1.1, DATA 1.2, DATA 1.5, DATA 1.6, DATA 1.7, NET 1.1, ORG 1.1, ORG 3.1, USER 1.11)

IEC 62443-2-4:2024 (SP.03.10)

IEC 62443-3-3:2013 (SR 4.1, SR 4.3)

NIST CSF 1.1 (PR.DS-1, PR.DS-2, PR.DS-5, PR.IP-6)

NIST CSF 2.0 (PR.DS-01, PR.DS-02, PR.DS-10)

Tools

Attack surface mapping Hyöky.fi

Julkri (TEK-16, TEK-18)

Kybermittari (THIRD-PARTIES-2, ARCHITECTURE-5, ARCHITECTURE-6)

11.9 The entity has ensured that its systems are updated regularly and that critical updates are installed without delay

Example implementation

This baseline information security policy is introductory to sections 3.2, 3.4 and 5.3.

- The entity has practices for monitoring the critical security updates of the operating systems, applications and firmware it uses and installing them without delay based on a risk assessment, e.g. by automatic updates. The practices may also include vulnerability scans.
- The entity has drawn up appropriate written instructions for critical security updates.
- Systems that cannot be updated must be secured with other methods, and updates must be installed in a controlled manner when it is possible.

the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- Other than critical security updates are also made regularly, for example monthly, when the system supplier publishes new updates.

Verification

1. The supervisory authority verifies the entity’s updating practices and the implementation of updates from documentation. Furthermore, the practices for detecting the need for updates are reviewed. The supervisory authority also reviews the method of managing deviations in the updates. This may have been implemented e.g. by documenting exemptions or by risk management methods.

Explanations

Software vulnerabilities are a typical way of spreading malware that can enable the misuse of a system or the unauthorised access to the system by abusing a vulnerability. Extensive exploitation of critical vulnerabilities in particular happens fast, meaning that the immediate installation of critical security updates is particularly important. Systems that cannot be updated can be very vulnerable, and they must be protected e.g. by separating them from other systems.

References

CCB CYFUN Basic (PR.MA-1)

ISO/IEC 27002:2022 (8.8, 8.19, 8.32)

IEC 62443-2-1:2010 (4.3.4.3.7)

IEC 62443-2-1:2024 (COMP 3.1, COMP 3.2, COMP 3.3, COMP 3.4, COMP 3.5, EVENT 1.9, ORG 2.4, CM 1.4)

IEC 62443-2-4:2024 (SP.11.01, SP.11.02, SP.11.03, SP.11.04, SP.11.05)

NIST CSF 1.1 (PR.IP-3, PR.MA-1)

NIST CSF 2.0 (PR.PS-01, PR.PS-02, PR.PS-03)

Tools

Attack surface mapping Hyöky.fi

Julkri (TEK-17, TEK-19)

Kybermittari (ASSET-4, THREAT-1)

11.10 The entity has ensured that its services and devices are configured securely

Example implementation

This baseline information security policy is introductory to section 3.3.

- The entity has practices based on which it removes unnecessary features from its systems. These include among others disabling or removing extraneous services or devices.
- The entity has changed the default settings, such as default passwords, of its systems and devices, and stores the updated passwords securely. If the entity has created accounts for emergencies, their protection, use and availability in case of emergencies must be ensured.
- The entity has implemented the security functions offered by its systems. These can include e.g. automatic software updates, secure identification means, encryption and the implementation of event logging.

Verification

1. The supervisory authority verifies that the entity has practices for checking device configuration before commissioning and in connection with updates, as necessary. These practices include the removal of unnecessary and unsecure features and changes to unsecure default settings. Many devices include easily enabled security features that the entity should adopt as a part of this process, e.g. workstation storage media encryption, automatic updates, secure control connections and protocols that use encryption.

Explanations

The removal of unnecessary features reduces the attack surface and weakens the attacker’s ability to access the entity’s systems. For example, default accounts and passwords are widely utilised in connection with automated scanning. Any device or service can enable access to critical systems as well, or devices can be abused in criminal activities. Unprotected devices, such as security cameras, can reveal confidential data.

References

ISO/IEC 27002:2022 (8.9, 8.27, 8.32)

IEC 62443-2-1:2024 (ORG 2.3, CM 1.4)

IEC 62443-2-4:2024 (SP.03.05)

IEC 62443-3-3:2013 (SR 7.6, SR 7.7)

NIST CSF 1.1 (PR.IP-1, PR.IP-3)

NIST CSF 2.0 (PR.PS-01, PR.PS-02, PR.PS-03)

Tools

Attack surface mapping Hyöky.fi

Julkri (TEK-10)

Kybermittari (ASSET-3, ARCHITECTURE-3, SITUATION-1)

11.11 The entity has ensured that its critical services and information assets are backed up

Example implementation

This baseline information security policy is introductory to sections 10.2 and 10.3.

- The entity has practices in place for backup copying, recovery practices and backup copy lifecycle management. If the backup copies contain data subject to statutory requirements, the entity also has practices for the timely destruction of backups.
- Critical data resources have been backed up regularly. The backup copies are separated physically and logically from the systems of which they are made. The backup copies are protected with procedures at least equal to those protecting the original data.
- Backup recovery testing has been carried out regularly.

Verification

1. The supervisory authority verifies that the entity has practices based on which the backing up of data resources deemed important to operations is implemented. The practices also indicate how backup copies are protected and how they are separated from the backed up systems. The entity has also documented the means by which the functionality of backups is tested regularly.
2. The supervisory authority verifies, e.g. with interviews, information supplied by the entity or reviews, that the practices on backup copies are implemented. The supplied information can include e.g. screenshots, configurations and event logs relating to backup copies and their practices. A physical review can contain e.g. reviewing the location of the backup system or the storage location of storage media and its security.

Explanations

Backup copies protect against intentional or unintentional loss of data. With the help of backup copies, the system can be recovered even in situations where the entire system is encrypted by the attacker. In these cases it is particularly important that the attacker is unable to encrypt the backup copies as well.

Recovery should be tested regularly, as backup copies often contain errors and their recovery fails. System recovery is often required in severe disruptions. Recovery from disruptions should be planned as a whole, e.g. as a part of continuity and recovery planning.

References

CCB CYFUN Basic (PR.IP-4)

ISO/IEC 27002:2022 (5.30, 8.10, 8.13)

IEC 62443-2-1:2010 (4.3.4.3.9)

IEC 62443-2-1:2024 (AVAIL 1.1, AVAIL 2.1, AVAIL 2.3, DATA 1.4, EVENT 1.8)

IEC 62443-2-4:2024 (SP.12.01, SP.12.02)

IEC 62443-3-3:2013 (SR 7.3)

NIST CSF 1.1 (PR.IP-4, PR.IP-6, PR.IP-9, PR.IP-10)

NIST CSF 2.0 (PR.DS-11)

NIST SP 800-82 rev 2

Tools

Julkri (TEK-20, TEK-22)

Kybermittari (CRITICAL-1, CRITICAL-2, RESPONSE-4, RESPONSE-5, ASSET-2, ARCHITECTURE-5)

11.12 The entity is prepared to maintain its operations in severe incidents

Example implementation

This baseline information security policy is introductory to section 9.7.

- The entity has written practices for defining responsibilities and measures for severe incidents in particular.
- The entity has written practices for making an NIS notification or other official notification in the case of an incident.

Verification

1. The supervisory authority verifies that the entity has written practices for incidents. The practices indicate the reporting obligations, up-to-date and

concrete contact information and channels for internal and external contacts, responsibilities and obligations, any emergency accounts and operating instructions.

2. If the entity has experienced incidents, the supervisory authority verifies the entity’s incident response procedures, e.g. with interviews and documentation related to incident handling. In particular, it is verified that incident response has been sufficient, it has discovered the type of the threat or root cause that likely caused the incident and that incident response has implemented statutory requirements, such as incident notifications. These can be verified e.g. from material supplied by the entity, such as an incident’s final report.

Explanations

Well-planned operating methods and practices shorten the recovery time in incidents. The notification obligation practices ensure that statutory notifications, such as that complying with the NIS2 Directive, are not neglected in an incident.

References

CCB CYFUN Basic (RS.RP-1, RC.RP-1, RC.CO-3)

ISO/IEC 27002:2022 (5.5, 5.24, 5.26)

IEC 62443-2-1:2010 (4.3.4.5)

IEC 62443-2-1:2024 (ORG 1.3, EVENT 1.8)

IEC 62443-2-4:2024 (SP.01.05, SP.01.06, SP.12.09)

NIST CSF 1.1 (RS.RP, RC.RP, RC.CO-3)

NIST CSF 2.0 (RS.MA-05, RC.RP-02, RC.CO-03)

Tools

Julkri (HAL-08)

Kybermittari (RESPONSE-1, RESPONSE-2, RESPONSE-3, RESPONSE-5)

11.13 The entity employs event logging of critical activities

Example implementation

This baseline information security policy is introductory to section 9.3

- The entity has ensured that event logging is generated for events related to critical activities.

- Event logging is generated e.g. for administrator measures and changes to privileges, and where possible, all security-related events over the entire network and information system.
- Event logging is also generated on the processing of confidential data based e.g. on statutory requirements.
- The event log should at least answer the following questions where possible: who, what, from where, when, where to.
- The event log is protected against changes and managed with separate accounts. The event log is backed up at regular intervals or copied into a separate system.

Verification

1. The supervisory authority verifies that the entity has defined the need for logs and, if necessary, the network and information system log architecture. The scope of the log system is proportionate to the entity’s needs.
2. The supervisory authority verifies from material supplied by the entity or by performing a review that logs are created at least for the targets and functions central to operations and that they are stored securely in a way that prevents unauthorised changes.

Explanations

In the case of disruptions, event logs are key to finding out how the event played out. Without appropriate event logs, finding out the root cause of the disruption may be impossible.

Backing up event logs is important due to ransomware in particular, as ransomware often encrypts the entire storage media. If this is the case, the event log also becomes illegible, unless it has been separately backed up or moved to a system inaccessible to the attacker.

References

CCB CYFUN Basic (PR.PT-1, DE.AE-3)

ISO/IEC 27002:2022 (5.28, 5.34, 8.15)

IEC 62443-2-1:2010 (6.10.1, 6.10.3)

IEC 62443-2-1:2024 (EVENT 1.4, DATA 1.1, DATA 1.2)

IEC 62443-2-4:2024 (SP.08.02, SP.08.03)

NIST CSF 1.1 (PR.PT-1, DE.AE-3)

NIST CSF 2.0 (PR.PS-04, DE.CM-01)

Finnish Transport and Communications Agency instruction on recording information on traffic data processing (Traficom/376384/03.04.05.01/2022)

Tools
Attack surface mapping Hyöky.fi Julkri (TEK-12) Kybermittari (ASSET-4, ACCESS-3, SITUATION-1, RESPONSE-4)

12 Measures to secure the physical environment and premises of networks and information systems as well as availability of the necessary resources

These recommendations are based on the introductory wording of Article 21(2) of the NIS2 Directive on the measures protecting the physical environment of networks and information systems. The national implementation is laid down in section 9, subsection 2, paragraph 12 of the Cybersecurity Act and in section 18 c, subsection 1, paragraph 12 of the Information Management Act.

1. **Premises security and physical access control**: The entity should identify factors in the physical environment whose security is important for the operation of networks and information systems and protect them from the impacts of disturbances and threats that affect their operation. The entity should also observe the physical environments impacting networks and information systems that can vary greatly and e.g. be geographically extensive or restricted. (See section 12.1.)

2. **Protection against physical and environmental threats**: Physical threats include environmental factors and hostile operators. Networks and information systems could for example be monitored and protected against unauthorised physical access, damage and disruptions. Furthermore, they must be protected against natural and social events, such as fires, floods and unrest. (See section 12.2.)

3. **Ensuring the continuity of resources necessary for operations**: The entity should prepare for disruptions in necessary resources, such as power supply, telecommunications and cooling, and prevent the destruction or damaging of networks and information systems and the suspension of the entity’s critical operations due to the lack or disruption of necessary resources. (See section 12.3.)

12.1 Premises security and physical access control

Example implementation
• The entity has identified the most critical areas in terms of the security of networks and information systems. The entity has protected the areas critical to security from unauthorised access and other damage and disruption. • Critical areas can include offices, server rooms and other technical premises. Depending on the entity, even the yard area in the vicinity of the entity’s premises may need to be surrounded by a fence, for example. The connections of resources such as energy, telecommunications and transport can cover very large geographical areas and may have been built over decades. The effectiveness of risk management for the premises security of these resources and the scale of any residual risk should be monitored in particular.

- Access to areas critical to the entity has been restricted solely to authorised persons with the help of physical access control. This can be implemented e.g. by locking doors and using structural boundaries, alarms and security personnel.
- Event logs for access control have been created whenever possible. The event log should indicate who has passed through a particular door or passage, at what time and how any locking on the door has been opened. Event logging can be automatic or carried out on paper.
- The most important doors and passages can be monitored with a recording CCTV system. The need for surveillance is based on a risk assessment carried out by the entity (see section 1).
- The entity has paid attention to the access control of third party persons in particular.
- The entity has practices for defining the access of visitors to security-critical areas, moving in the area and leaving the area.
- If necessary, the entity has defined other practices related to premises security, such as the clear desk and clear screen policy, keeping identifiers visible and preventing external persons from accessing the premises in connection to a door being opened (tailgating).
- The entity has practices for the secure reuse, recycling or other destruction of outdated or otherwise decommissioned equipment or storage media. Further information in section 5 Asset management.

Verification

1. The supervisory authority verifies that the entity has documented the most critical areas in terms of network and information system security and their access control principles. The principles indicate the definition of critical areas in accordance with the risk assessment and e.g. the related physical access control practices and other principles of premises security, principles of event logging and possible CCTV. Where possible, the principles must cover all premises of the entity where networks and information systems are located.
2. The supervisory authority verifies the entity's premises security and protections in terms of networks and information systems by reviewing e.g. the capability of physical access control at the entity's premises. The authority may pay attention e.g. to CCTV and its coverage, physical access control and the location of server equipment and their physical protection.

Explanations

Access by unauthorised persons into the entity's critical premises may compromise the confidentiality, integrity and availability of operations. Premises where the entity stores protected assets, personal data or classified data must particularly be protected against external persons.

References

ISO/IEC 27002:2022 (7.1, 7.2, 7.4)

IEC 62443-2-1:2024 (ORG 3.1, AVAIL 1.1, AVAIL 1.2, EVENT 1.1)

NIST CSF 1.1 (PR.AC-2, DE.CM-2)

NIST CSF 2.0 (PR.AA-06, DE.CM-02)

“Rakennusten digitaalinen turvallisuus” guidelines for the digital security of buildings (RT 103206 [ST 70.40], RT 103207 [ST 70.41] and RT 103208 [ST 95.12])

NIS CG Reference document (3.13.1 Perimeter and physical access control)

NIS CG Implementing guidance (13.3. Perimeter and physical access control)

Tools

Julkri (FYY-02, FYY-07, TEK-09)

Kybermittari (CRITICAL-1, ACCESS-3, ARCHITECTURE-3)

12.2 Protection against physical and environmental threats

Example implementation

- In its operations, the entity has taken into account physical and environmental threats to the networks and information systems and made its risk management measures proportionate to its operations in the prevailing conditions by monitoring and protecting them from unauthorised physical access, damage and disruptions. These threats can be caused by intentional or unintentional physical acts or natural phenomena. These risks can include fires, floods, storms, vandalism or terrorism.
- Actions mitigating the risks and protections against physical and environmental threats can include automatic extinguishing systems, compartmentation, ensuring and correctly sizing the structural strength of the building, protection related to building technology and property automation, such as temperature and humidity monitoring, overvoltage protection. If risk is managed by monitoring metrics (such as heat or humidity), clear thresholds should be set for them, and going above or below them should trigger an alarm or other measures.
- The entity’s risk management should treat the above-mentioned threats based on the all-hazards approach. Further information in section 1.2 All-hazards approach.
- In the case of accidents or other disturbances, the entity has assessed the related risk management and its proportionality. The entity has updated its operational practices as needed to prevent the events in question from reoccurring.

Verification

1. The supervisory authority verifies that the entity has observed physical and environmental threats to its networks and information systems in its risk management and continuity planning. Risks directly compromising the operations are managed with applicable management measures. The entity must meet any statutory requirements e.g. concerning fire-proofing.

Explanations

Physical and environmental threats may compromise the continuity of operations. In the worst-case scenario, threats can impact the entity so that business operations can no longer be continued.

References

ISO/IEC 27002:2022 (7.3, 7.5)

IEC 62443-2-1:2024 (ORG 3.1, AVAIL 1.2)

NIST CSF 1.1 (PR.IP-5)

NIST CSF 2.0 (PR.IP-02)

"Rakennusten digitaalinen turvallisuus" guidelines for the digital security of buildings (RT 103206 [ST 70.40], RT 103207 [ST 70.41] and RT 103208 [ST 95.12])

NIS CG Reference document (3.13.2 Protection against physical and environmental threats)

NIS CG Implementing guidance (13.2. Protection against physical and environmental threats)

Tools

Julkri (FYY-02)

Kybermittari (CRITICAL-2, THREAT-2, RISK-2, RISK-3, RISK-4, ACCESS-2, RESPONSE-3)

12.3 Ensuring the continuity of resources necessary for operations

Example implementation

- The entity has observed the continuity of resources necessary for the operations of networks and information systems (support services). These include power supply, water and gas distribution, cooling, sewerage and data communications connections.

- The entity has made the risk of disturbances in support services proportionate to its own operations and compensated for them as needed, e.g. prepared for a power failure with an emergency generator, battery insurance or alternative power sources. Data connections should be resilient as necessary, e.g. with backup connections. Arrangements for exceptional situations may be supported, where appropriate, through contracts with external partners, for example to ensure the availability of fuel for emergency generators.
- The entity has updated and maintained its operating instructions regularly and as needed after a disruption, so that the disruption or its consequences can be avoided in the future.
- The entity has clear operating instructions for severe disruptions.
- The entity has monitored the status of support services and the related disruption notifications. The entity should have up-to-date contact information of support service suppliers in case of disruptions.
- The entity should practice and test its backup systems regularly. The exercises are planned carefully and they ensure that the simulation of a disruption does not cause any real danger to the operations or the environment.

Verification

1. The supervisory authority verifies that the entity has prepared for disruptions in necessary resources, such as power supply, telecommunications and cooling, and prevented the destruction or damaging of networks and information systems and the suspension of the entity’s critical operations due to the lack or disruption of necessary resources. The entity has assessed the necessary resources for its operations and continuity, and if necessary, defined related management measures to compensate for the risks. The management methods can include contracts on backup arrangements, separate backup connections and plans on their implementation.
2. The supervisory authority verifies that the backup arrangements of resources necessary for the entity’s operations have been tested or that running on them has been exercised in practice.

Explanations

Disruptions in support services can cause interruptions or disturbances to the entity’s operations, which in turn can cause reputational damage or compromise the continuity of operations. A wide variety of incidents can cause data loss or other damage. Examples of exceptional situations include power failures, issues in device cooling and water damage.

References

ISO/IEC 27002:2022 (7.11) IEC 62443-2-1:2024 (AVAIL 1.2, ORG 1.6) IEC 62443-2-4:2024 (SP.08.04) NIST CSF 1.1 (ID.BE-1, ID.BE-2, ID.SC-2) NIST CSF 2.0 (GV.OC-01, GV.OC-05, GV.SC-03, PR.IR-03, PR.IR-04) “Rakennusten digitaalinen turvallisuus” guidelines for the digital security of buildings (RT 103206 [ST 70.40], RT 103207 [ST 70.41] and RT 103208 [ST 95.12]) NIS CG Reference document (3.13.3 Supporting utilities) NIS CG Implementing guidance (13.1. Supporting utilities)
Tools
Julkri (VAR-05, VAR-07) Kybermittari (CRITICAL-3, RESPONSE-3, RESPONSE-4, RESPONSE-5, THIRD-PARTIES-1, THIRD-PARTIES-2, General management measures)

III References

Regulation and instructions related to the recommendation

National

Act on Cybersecurity Risk Management (124/2025)

Act amending the Act on Information Management in Public Administration (125/2025)

Act on Information Management in Public Administration (906/2019)

Finnish Transport and Communications Agency Regulation on information security in telecommunications operations (M67) (TRAFICOM/248815/03.04.05.00/2022)

Digital and Population Data Services Agency's instruction: Handbook of secure software development. Published 19 May 2020.

Finnish Transport and Communications Agency instruction on recording information on traffic data processing (Traficom/376384/03.04.05.01/2022)

Ministry of Finance publications 2023:54: Risk management handbook for central government administration: https://urn.fi/URN:ISBN:978-952-367-633-6

Ministry of Finance publications 2023:57: Recommendation on information security in procurement for a target audience of information management units and public authorities: https://urn.fi/URN:ISBN:978-952-367-645-9

International

Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive, Cybersecurity Directive)

NIS Cooperation Group: NIS CG Reference document (on security measures for important & essential entities)

Standards and frameworks related to the recommendation

National

Assessment criteria for information security in public administration (Julkri): Recommendation and criteria: http://urn.fi/URN:ISBN:978-952-367-458-5

Finnish Transport and Communications Agency's Kybermittari: Kybermittari.fi

International

CCB CYFUN (CyberFundamentals) Framework Basic

COSO Enterprise Risk Management Framework

IEC 62443-2-1:2013 Industrial communication networks. Network and system security. Part 2-1: Establishing an industrial automation and control system security program

IEC 62443-2-4:2019 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

IEC/TR 62443-3-1:2013 Industrial communication networks. Network and system security. Part 3-1: Security technologies for industrial automation and control systems

IEC 62443-3-3:2019 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Information security management systems. Requirements.

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection. Information security controls.

ISO/IEC 27003:2018 Information technology. Security techniques. Information security management systems. Guidance

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection. Guidance on managing information security risks

ISO/IEC 27035-1:2023 Information technology - Information security incident management - Part 1: Principles and process

ISO/IEC 27035-2:2023 Information technology - Information security incident management - Part 2: Guidelines to plan and prepare for incident response

ISO 31000:2018 Risk management. Guidelines

NIST CSF 1.1 Cybersecurity framework 1.1

NIST CSF 2.0 Cybersecurity framework 2.0

NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations: https://doi.org/10.6028/NIST.SP.800-53r5

NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide: https://doi.org/10.6028/NIST.SP.800-61r2

NIST SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security: https://doi.org/10.6028/NIST.SP.800-82r3

OWASP Application Security Verification Standard

OWASP Top Ten

The STRIDE Threat Model

The DREAD risk assessment model

Other publications

Finnish Transport and Communications Agency’s National Cyber Security Centre: Vulnerabilities – how to report them correctly

Finnish Transport and Communications Agency’s National Cyber Security Centre: Collecting and using log data

Finnish Transport and Communications Agency’s National Cyber Security Centre: Cyber exercise instructions

Finnish Transport and Communications Agency’s National Cyber Security Centre: Coordinated vulnerability disclosure CVD process

NSA, CISA: Identity and Access Management: Recommended Best Practices for Administrators

Annex 1 Cross-reference table

Cross-reference table with examples of well known standards, frameworks and guidelines related to this Recommendation.