Reference document on security measures for Operators of Essential Services

NIS Cooperation Group
February 2018

ABOUT

This document has been drafted and endorsed by the NIS Cooperation Group members.

Participants

Coordination

France	ANSSI (Jean-Baptiste Demaison – Chair – and Victor Cambazard)
Belgium	CCB (Jean-Luc Peeters)

Secretariat, support

Entity	**Name**
ENISA	Konstantinos Moulinos
	Paraskevi Kasse
European Commission	Aristotelis Tzafalias

Contributors

Entity	**Country/Entity**
Member States	Representatives to the Cooperation Group

1.
Introduction

Background

Directive (EU) 2016/1148[11] of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (hereinafter: "NIS Directive") was adopted on 6 July 2016.

Laying down "*measures with a view to achieving a high common level of security of network and information systems within the EU*" the NIS Directive in particular provides with measures aimed at improving the cybersecurity of operators considered "*essential for the maintenance of critical societal and/or economic activities*" [22].

Public or private entities providing services "*essential to the maintenance of critical societal and/or economic activities*", these "*Operators of Essential Services*" (OES) shall be identified by each Member State on its territory and comply with several binding provisions defined nationally.

In particular, *"Member States shall ensure that OES take appropriate and proportionate technical and organisational* ***security measures*** *to manage risks posed to the security of NIS they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed".*

Furthermore "*Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of (…) essential services, with a view to ensuring the continuity of those services*"[3].

Individually responsible for the transposition of these provisions into National law, Member States may moreover adopt or maintain provisions with a view to achieving a higher level of security of network and information systems, according the principle of minimum harmonisation set in the Directive[44].

Nevertheless, with a view of fostering mutual understanding of challenges related to the implementation of key provisions of the Directive and of supporting convergence of national approaches to their implementation, a Cooperation Group (CG) is established to facilitate exchange of information and best practices among Member States.

[1] Directive (EU) 2016/1148, article 14 (1)
[2] Directive (EU) 2016/1148, article 5 (2)a
[3] Directive (EU) 2016/1148, article 14 (2)
[4] Directive (EU) 2016/1148, article 3

Taking advantage of this possibility and upon proposal from the European Commission (EC) a group of voluntary Member States' experts (hereinafter: "the Group") was therefore established within the framework of the Cooperation Group with the support of ENISA, in view of exchanging views on the issue of security measures for OES.

The present "reference document" provides with a summary of the Group's main findings.

This panorama doesn't aim at establishing a new standard nor to duplicate existing ones (e.g. ISO) but to provide Member States with a clear and structured picture of Member States' current and often common approaches to the security measures of OES.

Beyond OES, this reference document providing with indications on domains of cybersecurity measures may be considered useful by other public or private actors in improving their cybersecurity.

Purpose

Cyberthreats to critical infrastructures are now recognized as among the most serious threats to the EU, its Member States, the economy and the society.

Essential to the functioning of the Single Market, due to their contribution to critical economic and societal functions such as in the fields of Energy, Transport or Banking, OES are indeed targets of choice. Malicious actors, constantly developing their tools and techniques often advanced and targeting the weakest may indeed choose to target OES and thus harm the critical functions supporting our economy and society.

By requiring OES to comply with "appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems"[5], the NIS Directive aimed at significantly raising the level of security of OES in view of allowing them to face the serious risks posed to the security of their critical information systems supporting their essential operations.

Reinforcing OES' cybersecurity will therefore significantly contribute to reducing the risks to the EU and Member States' cybersecurity.

Recognizing the solid and growing risk posed to OES and their potential impact on EU's economy and society and taking into account that some OES may be established in different EU Member States, the Group agreed that all may benefit from indications towards more coherent approaches to the transposition of the NIS Directive with regard to security measures for OES foreseen in article 14 (1) and (2).

[5] Directive (EU) 2016/1148, article 14 (1)

Outcome

Building upon answers provided by the Member States ENISA's questionnaire, the Group acknowledged that Member States may wish to

- Use different sources or control frameworks for security measures from European or International standards (e.g. ISO 27.000)[6] to existing or new sets of security measures (e.g. France's cybersecurity measures for OES, Germany's IT-Grundschutz, Spain's National Security Framework, etc.).
- Aim at different levels of granularity and prescription regarding specific cybersecurity requirements, objectives and controls.
- Aim to only establish cross-sectoral measures or choose to address individual sector specificities as well (with sector-specific measures).

Nevertheless, despite those differences, the Group agreed that a common consensual basis could be identified in view of fostering convergence of national approaches to the transposition of the Directive.

Thus, the Group managed draw an **inclusive picture** of Member States' existing and often common approaches regarding **principles and domains of cybersecurity measures** which should enlighten the national transposition of OES' security measures related provisions.

[6] Article 19 of the NIS Directive "Encourage the use of European and internationally accepted standards and specifications relevant to the security of Network and Information Systems".

2.
Principles

Despite different possible approaches to the national transposition of article 14 (1) and (2) of the NIS Directive on security measures for OES, the Group agreed that Member States should take the utmost into account the following general principles.

First, security measures should be:

- **Effective** in view significantly increasing the cybersecurity of OES, in relation to the current and foreseen threat landscape described above.
- **Tailored** in view of putting OES' efforts on measures having the most impact
  on their cybersecurity and avoid unnecessary effort and duplication.
- **Compatible** in view of addressing, on the short term, basic and common security vulnerabilities of OES despite their sectors, which may in the meantime be complemented with sector specific security measures;
- **Proportionate** to the risks, in view of avoiding unnecessary burden for OES, for instance by privileging applying security measures only to the critical information systems underlying the OES' information systems operating their essential services.
- **Concrete** and easy to apprehend, to ensure that the security measures are actually implemented by OES and actually contribute to reinforcing their cybersecurity.
- **Verifiable**, to ensure that operators may provide to their national NIS competent authority(ies) *"evidence of the effective implementation of security policies, such as results of a security audit carried out by the competent authority or a qualified auditor"*[7].
- **Inclusive**, to encompass all security domains which may contribute to reinforcing the cybersecurity of OES, including physical security of information systems.

Beyond these principles, Member States should:

- Acknowledge the **added-value of dialogue with public and private operators**, in particular with regard to the implementation of the security measures. Member States should consider establishing Public and Private Partnerships with OES. Such PPPs may be used in view of
  - identifying relevant cross-sectoral or sectoral measures which could be adopted, taking into account the above mentioned principles and the list of suggested cybersecurity measures' domains (below);

[7] Directive (EU) 2016/1148, article 15 (1) & 2

    - establishing a permanent dialogue with OES to facilitate the implementation of these measures.

- Find a proper **cost-benefit balance** so that to ensure efficient security measures, with respect to the security of essential services to the economy and the society, while taking into account their cost for OES'.

3.
Domains of cybersecurity measures

PART 1 - GOVERNANCE AND ECOSYSTEM

1.1 Information System Security Governance & Risk Management

Information system security risk analysis,

The operator conducts and regularly updates a risk analysis, identifying its Critical Information Systems (CIS)[8] underpinning the provision of the essential services of OES and identifies the main risks to these CIS. This process is essential to build and maintain a robust risk management organization. The results of the updates should be implemented through a virtuous circle of continuous improvement.

The risk assessment takes into account, in particular:

- new threats
- recently discovered weaknesses
- loss of effectiveness of measures
- changes to the risk situation caused by changes to the system architecture
- any other changes in the risk situation

Information system security policy

Building upon the risks analysis, the operator establishes, maintains up-to-date and implements an information system security policy (ISSP) and an information security management system (ISMS) approved by senior management, guaranteeing high level endorsement of the policy.

The policy sets out strategic security objectives, describes the security governance (or risk management organization), and refers to all relevant specific information system security policies (e.g. on the security accreditation process, security audit, cryptography, security maintenance, incident handling, etc.).

Information system security accreditation

Building on the risk analysis and according to an accreditation process[9] referred to in the ISSP, the operator accredits itself CIS identified in its information system risk analysis, including *inter alia* the inventory and architecture of the administration components of the CIS.

[8] Article 5 (2) b of the NIS Directive

[9] Here the "accreditation of CIS" should be understood as the decision by the Operator himself identifying its CIS, the risks associated and the residual risks that the Operator chooses to accept.

The purposes of the accreditation process for the operator are to integrate the CIS within the risk management organization and to formally accept the residual risks.

As part of the accreditation process and depending on the risks analysis, a security audit of the CIS should be carried out. That audit should aim at checking the application and effectiveness of the security measures that apply to the CIS.

The CIS accreditation decision should take into account the risk analysis, the security measures applied to the CIS, audit reports and the residual risks, and the reasons to justify their acceptance.

The operator maintains an up-to-date map of its CIS.

Information system security indicators

For each CIS and according to a number of indicators and assessment methods, the operator evaluates its compliance with its ISSP. Indicators may relate to the risk management organization's performance, the maintaining of resources in secure conditions, users' access rights, authenticating access to resources, and resource administration.

Information system security audit

The operator establishes and updates a policy and procedures for performing information system security assessments and audits of critical assets and CIS, taking into account the regularly updated risks analysis.

Human resource security

The operator ensures that, first, employees and contractors understand and demonstrate their responsibilities and are suitable for the roles for which they are considered and, second, commit to their roles.

The established information system security policies sets up a CIS security awareness raising program for all staff and a security training program for employees with CIS related responsibilities.

Asset management

The operator sets a suitable framework for identifying, classifying and implementing an inventory of the IT-processes, systems and components of the CIS. This asset management supports the rollout of updates and patches and where appropriate determines, which components are affected by new security issues.

1.2 Ecosystem management

Ecosystem mapping

The operator establishes a mapping of its ecosystem, including internal and external stakeholders, including but not limited to suppliers, in particular those with access to or managing operator's critical assets.

The purpose of this mapping is to identify and evaluate the potential risks represented by the relations with the stakeholders of the ecosystem. To perform this evaluation, the operator might consider four major parameters:

- **Maturity**: what are the stakeholder's technical capabilities regarding cybersecurity?
- **Trust**: Can I assume that the stakeholder's intentions toward me are reliable?
- **Access level**: What are the stakeholder's access rights to my critical assets and CIS?
- **Dependence**: To which extent is the relationship with my stakeholders critical to my activity?

Ecosystem relations

The operator establishes a policy towards its relations with its ecosystem in order to mitigate the potential risks identified. This includes in particular interfaces between the CIS and third parties. Generally, security requirements must been taken into account for CIS-components operated by third parties. The operator ensures via service level agreements (SLA) and/or auditing mechanisms that his suppliers also establish adequate security measures.

PART 2 - PROTECTION

2.1 IT Security Architecture

Systems configuration

The operator only installs services and functionalities or connects equipment which are essential for the functioning and the security of its CIS. If additional components are unavoidable (e.g. for economic reasons), they are analyzed according to the risk analysis. Those components should only be used to the necessary extent and with adequate security measures.

For example, the operator only connects to its CIS equipment, hardware peripheral and removable media that it has duly itemized and that are essential for the functioning or the security of its CIS.

System segregation

The operator segregates its systems in order to limit the propagation of IT security incidents within its systems or subsystems.

To this aim, the operator segregates physically or logically each CIS from the operator's other information systems or from third party information system. In the case a CIS itself is composed of subsystems, the operator segregates these last physically or logically. The operator allows only interconnections - between CIS and other systems or between CIS subsystems - that are essential for the functioning and security of a CIS.

The operator implements adequate security measures for unavoidable interfaces (e.g. interfaces to the IT of suppliers or customers).

Traffic filtering

The operator filters traffic flows circulating in its Critical Information Systems (CIS). The operator therefore forbids traffic flows that are not needed for the functioning of its systems and that are likely to facilitate an attack.

The operator defines and regularly updates the filtering rules (by network address, by port number, by protocol, etc.) in order to restrain traffic flows to flows needed for the functioning and the security of the CIS.

The operator filters flows entering and existing CIS and flows between CIS subsystems at the level of their interconnection, therefore limiting the flows strictly necessary for the functioning and security of CIS.

Cryptography

In its ISSP, the operator establishes and implements a policy and procedures related to cryptography, in view of ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information in its CIS.

2.2 IT Security Administration

Administration accounts

The operator sets up specific accounts for the administration, to be used only for administrators that are carrying out administration operations (installation, configuration, management, maintenance, etc.) on its CIS. These accounts are kept on an up-to-date list, which can be done for non-administration accounts as well.

To this aim, the permissions given to administrators are individualized and restricted as much as possible to the functional and technical perimeter of each administrator. The administrator accounts are only used to connect to administration information system. While these accounts are used for administration purposes only, administration operations are realized exclusively with the use of administrator accounts.

Administration information systems

Hardware and software resources used for administration purposes are managed and configured by the operator, or, where appropriate, by the service provider that the operator has authorised to carry out administration operations.

Administration information systems used for administration purposes only and to carry out administration operations and should not be mixed up with other operations. In particular administration accounts' software environment is not used for access to web sites or messaging systems on the internet, and users do not connect to a system used for administration purposes through a software environment used for other functions than administration operations.

The operator sets up a dedicated physical network to connect administration systems to the resources to be administered. The administrator uses to this purpose the resources' physical administration interface[10].

In case administration measures are not conducted through the dedicated network, administration flows are protected by authentication and encryption mechanisms[11].

No password, in form of plain text or hash is written in the logs recording events produced by the resources used for administration, or stored in such form at any time whatsoever.

2.3 Identity and access management

Authentication and identification

For **identification**, the operator sets up unique accounts for users or for automated processes that need to access resources of its CIS[12]. Unused or no longer needed accounts are to be deactivated. A regular review process should be established.

For **authentication**, the operator protects access to resources of its CIS for users or automated processes using authentication mechanism. The operator defines the rules for the management of authentication credentials of its CIS.

Whenever this is necessary, and in cases this is feasible, the operator should change authentication credentials. In particular, the operator should change from start the default authentication credentials installed by the manufacturer/supplier of a resource before that resource goes into operation. Neglecting this aspect would pose a high risk to the security of any infrastructure that such a resource is a part of or interacts with.

Access rights

Among the rules defined in its systems security policy, the operator grants access rights to a user or an automated process only when that access is strictly necessary for the user to carry out their mission or for the automated process to carry out its

[10] When this is not feasible, the operator develops a set of risk-reduction measures and describes them in the accreditation dossier of the CIS concerned.

[11] When this is not feasible, the operator develops a set of measures to protect data confidentiality and in a state of integrity, while strengthening checks and traceability of said administration operations and describes them in the accreditation dossier of the CIS concerned.

[12] When this is not feasible due to technical or operational reasons, the operator develops a set of traceability and risk reduction measures and describes them in the accreditation dossier of the CIS concerned.

technical operations. The principles of need to know and least privilege should be applied.

The operator defines access rights to the multiple functionalities of the resource, and allocates those access rights strictly to users / automated processes with a clear necessity. The operator reviews at least yearly these access rights, covering the links between accounts, associated access rights, and the resources or functionalities that are accessed with those access rights, and keep an updated list of privileged accounts (e.g. an administration account). The operator checks any potential modification to a privileged account to verify that access rights to resources and functionalities are allocated based on the principle of least privilege (only the rights that are strictly necessary are granted), and are adequate with the usage of the account.

2.4 IT Security Maintenance

IT security maintenance procedure

The operator develops and implements a procedure for security maintenance in accordance with its ISSP. To this purpose, the procedure defines the conditions enabling the minimum security level to be maintained for CIS resources. The procedure, which describes the policy on installing any new version or corrective measure for a designated resource, also states the operator's self-obligation of information on vulnerabilities and corrective security measures that concern CIS resources (hardware and software).

The operator installs[13] and maintains only versions of their CIS hardware and software resources that are supported by their suppliers or manufacturers and up to date from a security point of view. The operator checks the origin and integrity of the version before its installation (as per the timescales defined in the procedure), and analyse the technical and operational impact of that version on the CIS concerned.

The operator protects access to its CIS when access is made through third party networks. In this case, the operator protects by encryption and authentication mechanisms access to the CIS as well as the mass storage of equipments used to access the CIS, and also manages and configures the above mentioned equipments.

Industrial control systems

Many essential services depend on functioning and secure industrial control systems (ICS). If applicable, the operator takes the particular security requirements for ICS into

[13] In some cases, when justified by technical or operational reasons, the operator decides for some resources not to install a version supported by the supplier or manufacturer. In these cases, the operator applies the procedure – as per its policy – to reduce risks linked to the use of an obsolete version, and describes in its accreditation dossier the measures taken and the reasons that justified not to install the supported version.

account. For example, the classical information technology approach (which is focused on transfer of and access to information) could be replaced by an operational technology approach (hardware and software is used to cause or detect changes in a physical process).

2.5 Physical and environmental security

The operator prevents unauthorized physical access, damage and interference to the organization's information and information processing facilities.

PART 3 - DEFENSE

3.1 Detection

Detection

The operator sets up a security incident detection system of the "analysis probe for files and protocols" type. The analysis probes for files and protocols analyses the data flows transiting through those probes in order to seek out events likely to affect the security of CIS. They are positioned so that they can[17] analyse all flows exchanged between the CIS and third-party information systems.

Logging

The operator sets up a logging system on each CIS in order to record events relating, at least, to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the CIS and which covers application servers that support critical activities; system infrastructure servers; network infrastructure servers; security equipments; engineering and maintenance stations of industrial systems; network equipments; administrative workstations. The operator records through the logging system events with time and date-stamping using synchronised time sources and centralises archives for at least half-a-year.

Logs correlation and analysis

The operator creates a log correlation and analysis system that mines the events recorded by the logging system installed on each of the CIS in order to detect events that affects CIS security. The log correlation and analysis system is installed and operated by the operator (or the service provider appointed to that effect) *via* a dedicated information system used only to detect events that are likely to affect the security of information systems.

3.2 Computer Security Incident Management

Information system security incident response

The operator creates and keeps up-to-date and implements a procedure for handling, response to and analysis of incidents that affect the functioning or the security of its CIS, in accordance with its ISSP.

[17] When this is not feasible due to technical reasons, the operator describes in the accreditation dossiers for the CIS concerned the technical reasons that prevented the use of probes.

The operator puts in place a dedicated information system to handle incidents, in order *inter alia* to store the technical records of incident analysis. The operator segregates the system from the CIS affected by the incident and stores the related technical records for a period of at least half-a-year. The operator takes into account, when designing the system, the confidentiality level of stored documents.

Incident Report

The operator creates and keeps up-to-date and implements procedures for incidents' reporting.

Communication with competent authorities and CSIRTs

The operator implements a service that enables it to take note, without undue delay, of information sent out by its national competent authority concerning incidents, vulnerabilities, threats and relevant mappings (up-to-date inventory of CIS, interconnections of CIS with third-party networks, etc.). It implements a procedure for handling the information received, and, where appropriate, for taking the security measures required to protect its CIS. The operator provides its national competent authority with up to date contact details (department name, telephone number, and e-mail address) for this service. The operator is encouraged to connect its incident management with relevant Computer Security Incident Response Teams (CSIRTs).

PART 4 - RESILIENCE

3.1 Continuity of operations

Business continuity management

In accordance with its ISSP, the operator defines objectives and strategic guidelines regarding business continuity management, in case of IT security incident.

Disaster recovery management

In accordance with its ISSP, the operator defines objectives and strategic guidelines regarding disaster recovery management, in case of severe IT security incident.

3.2 Crisis management

Crisis management organization

The operator defines in its ISSP the organization for crisis management in case of IT security incidents and the continuity of organization's activities.

Crisis management process

The operator defines in its ISSP the processes for crisis management which the crisis management organization will implement in case of IT security incidents and the continuity of an organization's activities.