ETSI TR 103 456 V1.1.1 (2017-10)

CYBER;
Implementation of the Network and Information Security (NIS) Directive

Reference

DTR/CYBER-0021

Keywords

cyber security, cyber-defence, information assurance, privacy

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document provides guidance on the available technical specifications and those in development by major cyber security communities worldwide designed to meet the legal measures and technical requirements relating to implementation of the NIS Directive, including the sharing of information and network based risks and incidents and necessary defence measures. The guidance includes: considerations for incident notification and best practices in cyber security risk management. The present document provides a broader cyber security context than the NIS Directive or the ENISA Standardization Gaps Report to facilitate evolution toward significant emerging open global platforms, and includes treatment of challenges associated with harmonizing the implementations across the diverse network and services sectors and Member State legal and operational environments.

Introduction

The Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 [i.1] concerning measures for a high common level of security of network and information systems across the Union (commonly called the NIS Directive or NISD contains legal measures which include:

- requiring Member States to be appropriately equipped, e.g. via Computer Security Incident Response Teams (CSIRTs) a competent national NIS authority for a number of sectors, and a national information security strategy;

- setting up a cooperation framework among Member States by means of a Cooperation Group, in order to support and facilitate strategic cooperation and the exchange of information among Member States, including and a CSIRT Network, for voluntary operational cooperation on specific cyber security incidents and sharing information about risks; and

- requiring Member States to provide the frameworks and necessary obligations on businesses in sectors identified by the Member States as operators of essential services, including those that operate in sectors identified in the Directive, as well as providers of certain digital services, are implementing appropriate security measures and notifying the relevant national authority of serious incidents having significant impact in their services.

These legal measures in turn invoke a set of common cyber security technical requirements that include:

- structured sharing of information on risks and incidents;

- notification of incidents;

- outcomes-focused cybersecurity risk management practices and controls to identify and protect assets, detect anomalous analyses and potential incidents, and respond to and recover from incidents that may impact network and information systems; and

- international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues through harmonised standards.

The present document provides implementation guidance for meeting these requirements based on ETSI's capabilities as a regional and global organization that brings together industry expertise and global cyber security knowledge, including its own cyber security technical specifications and report.

1 Scope

The present document provides guidance in accordance with the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 [i.1] concerning measures for a high common level of security of network and information systems across the Union (commonly called the NIS Directive or NISD) on the available technical specifications and those in development by major cyber security communities worldwide designed to meet the legal measures and technical requirements relating to the sharing of information on network based risks and incidents and also the necessary defence measures to enable the protection of its essential security interests.

The present document is intended be used by all that need to consider the effects, use or perform the legal transposition of the NIS Directive into national legislation. These include national regulators who need to update regulations or guidelines for specific industries identified in the NIS Directive as Operators of Essential Services (OES) or national policy makers wishing to provide guidance for Digital Service Providers (DSP). The present document might also be used by OES' and DSPs themselves for their own implementation. The present document is not intended to be prescriptive in the selection or use of technical specifications or requirements as organizational risk based approach yields the most effective industry wide implementations.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive (EU) 2016/1148 of The European Parliament and of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

NOTE: Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

[i.2] ENISA: "Gaps in NIS standardisation Recommendations for improving NIS in EU standardisation policy" V.1.0, November 2016.

[i.3] ETSI TR 103 305: "CYBER; Critical Security Controls for Effective Cyber Defence".

[i.4] ETSI TR 103 421: "CYBER; Network Gateway Cyber Defence".

[i.5] Transposition of the EU Network and Information Security (NIS) Directive, Digital Europe, Brussels, 5 July 2016.

[i.6] ETSI TR 103 331: "CYBER; Structured threat information sharing".

[i.7] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and proforma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.8] ETSI ETR 340: "Telecommunications Security; Guidelines for security management techniques".

[i.9] Recommendation ITU-T X.700 series (ISO/IEC 10160): "Information technology - Open Systems Interconnection - Systems Management".

[i.10] Recommendation ITU-T X.800 series (ISO/IEC 10181, ISO/IEC 11586): "Information technology - Open Systems Interconnection - Security frameworks for open systems, Generic upper layers security".

[i.11] Recommendation ITU-T X.1300 series: "Network security".

[i.12] Recommendation ITU-T X.1050 series: "Security Management".

[i.13] Recommendation ITU-T X.1200 series: "Cybersecurity".

[i.14] Recommendation ITU-T M.3000 series: "Security for the management plan".

[i.15] ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.16] ISO/IEC 27000 series: "Information technology -- Security techniques -- Information security management systems".

[i.17] IEC 62443: "Industrial communication networks - Network and system security".

[i.18] ISACA: COBIT 5 series.

[i.19] ETSI GS ISI 001 (all parts): "Information Security Indicators (ISI)".

[i.20] ETSI TR 103 303: "CYBER; Protection measures for ICT in the context of Critical Infrastructure".

[i.21] ETSI Security Week 2017.

NOTE: Available at http://www.etsi.org/etsi-security-week-2017.

[i.22] ETSI Security Week, NFV Security Tutorial.

NOTE: Available at https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/04_NFVTUTORIAL/ETSI_ISGNFV_TUTORIALMATERIAL.pdf.

[i.23] ETSI Security Week, 5G Security: a government view.

NOTE: Available at https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/06_5GSECURITY/S02/NCSC_HAIGH.pdf.

[i.24] Sean Barnum: "The MITRE Corporation, Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)", 2012.

[i.25] ISO/IEC 15408: "Evaluation criteria for IT security".

[i.26] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.27] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[i.28] Recommendation ITU-T X.1500 series: "CYBEX Cyber security information Exchange".

[i.29] U.S. NIST Cybersecurity Framework.

NOTE: Available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[i.30] ETSI TR 103 305-4: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.31] CCRA: "Common Criteria for Information Technology Security Evaluation", Version 1.0.

NOTE: Available at https://www.commoncriteriaportal.org/cc/.

[i.32] Federal Ministry of the Interior: "National Plan for Information Infrastructure Protection".

NOTE: Available at http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf.

[i.33] Federal Ministry of the Interior: "Critical Infrastructure Protection (CIP) Implementation Plan".

NOTE: Available at http://www.qcert.org/sites/default/files/public/documents/GER-PL-CIP%20Implementation%20Plan-Eng-2007.pdf.

[i.34] IETF draft-ietf-inch-requirements-03: "Requirements for the Format for INcident information Exchange (FINE)".

[i.35] IETF draft-ietf-inch-iodef-02: "The Incident Data Exchange Format Data Model and XML Implementation".

[i.36] IETF draft-ietf-inch-rid-00: "Incident Handling: Real-Time Inter-Network Defense".

[i.37] IETF draft-ietf-inch-implement-00: "The Incident Object Description Exchange Format (IODEF) Implementation Guide".

[i.38] Recommendation ITU-T X.1500: "Overview of cybersecurity information exchange".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in the NIS Directive [i.1] apply.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ANSSI	Agence Nationale de la Sécurité
BSI	German Federal Office for Information Security
CCDB	Common Criteria Development Board
CCRA	Common Criteria Recognition Agreement
CDXI	Cyber defence Data eXchange and Collaboration Infrastructure
CERT	Computer Emergency Response Teams
CIA	Confidentiality, Integrity, Availability
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
COBIT	Control Objectives for Information and related Technology
CPNI	Centre for the Protection of National Infrastructure
CSAF	Common Security Advisory Framework
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CTIP	Cyber Threat Intelligence Program
CVRF	Common Vulnerability Reporting Framework
CYBEX	cybersecurity information exchange
CybOX	Cyber Observable expression
DIB	Defense Industrial Base
DMARC	Domain-based Message Authentication Reporting and Conformance
DNS	Domain Name System
DSP	Digital Services Providers
ENISA	European union agency for Network and Information Security

FIRST	Forum of Incident Response and Security Teams
FYROM	Former Yugoslav Republic Of Macedonia
GDPR	General Data Protection Regulation
IAD	Information Assurance Directorate
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IODEF	Incident Object Description Exchange Format
ISAC	Information Sharing and Analysis Centre
ISACA	Information Systems Audit and Control Association
ISI	Information Security Indicators
IT	Information Technology
IXP	Internet eXchange Point
MACCSA	Multinational Alliance for Collaborative Cyber Situational Awareness
MAPP	Maturity Assessment, Profile and Plan
MEC	Mobile Edge Computing
MILE	Managed Incident Lightweight Exchange
MISP	Malware Information Sharing Platform
MS	Member State
MSRC	Microsoft Security Response Center
NATO	North Atlantic Treaty Organization
NCIRC	NATO Computer Incident Response Capability
NCSC	National Cyber Security Centre
NFV	Network Function Virtualization
NII	Network Information Infrastructure
NIS	Network and Information Security
NISD	NIS Directive
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OES	Operators of Essential Services
OSSI	Office of Security and Strategic Informatio
OTT	Over The Top
RID	Real-time Inter-network Defense
SDN	Software Defined Networking
SGDSN	Secretariat-General for National Defence and Security
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
TC	Technical Committee
TLD	Top-Level Domain

4 Overview of the NIS Directive

4.1 The context for NIS

The NIS Directive (NISD) focuses on strengthening cyber authorities at the national level, increasing coordination among them and introduces security requirements for key industry sectors.

The two main objectives of the NIS Directive are [i.5]:

1) ensuring a high level cyber security of the country's critical infrastructures;

2) establishing an effective cooperation mechanism among EU Member States to further advance this objective.

The Network Information Security domain is one of the many dimensions of the multi-dimensional cyber-security landscape that can be visualised as a set of linked questions:

a) What is cyber security?

b) Who or what is affected? i.e. What is the cyber environment?

c) What measures enable protection?