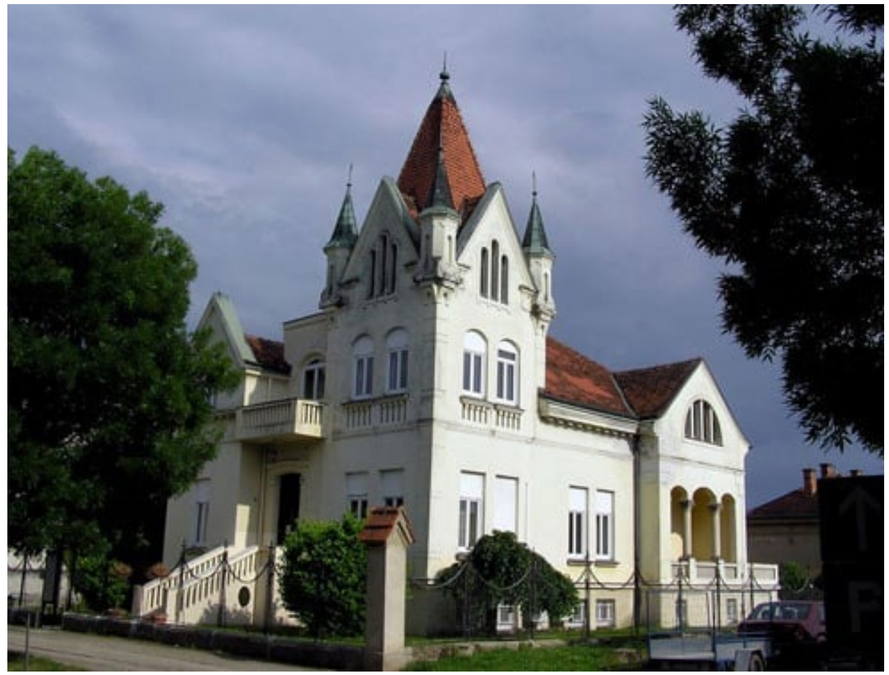
EU NIS2 Directive - Cybersec goes mainstream

OWASP Meetup Zagreb 09/2023

Porobija & Špoljarić LLC
law firm



Regulation, regulation, regulation...

NIS1 (2016) Network and information security directive - 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

Goals:

- Improving protection of critical infrastructure
- General improvement of cybersecurity and awareness
- Harmonisation across the EU
- Establishing cooperation between EU member states

Issues:

- Ambiguous scope and criteria for categorisation, penalties and reporting thresholds
- Lackluster cooperation both within the EU and outside the EU
- Rapidly evolving threat landscape

Regulation, regulation, regulation...

Notable mentions:

EU Cybersecurity Act (2019):

- Permanent mandate to the ENISA
- Increase operational cooperation at EU level, helping EU members handle their cybersecurity incidents
- Setting up and maintaining the European cybersecurity certification framework

The Digital Operational Resilience Act (DORA)

- Similar to NIS2, but is a regulation and is directly applicable across EU
- Aimed at financial institutions
- Aimed at establishing a framework for operational resilience of the financial sector

Certification, certification, certification…

Topic

› Certification

Keywords

certification

Cybersecurity Certification: Candidate EUCC Scheme V1.1.1

Following the request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act, ENISA has set up an Ad Hoc Working Group to support the preparation of a candidate EU cybersecurity certification scheme as a successor to the existing schemes operating under the SOG-IS MRA. This has been named EUCC scheme (Common Criteria based European candidate cybersecurity certification scheme) and it looks into the certification of ICT products cybersecurity, based on the Common Criteria, the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045. This version -V.1.1.1- of the scheme has been updated based on the comments received through the public consultation and from the ECCG.

Download
PDF document, 8.83 MB

Published May 25, 2021
Language English

ENISA published also the report presenting the outcome of the public consultation on the first draft of the cybersecurity certification candidate EUCC scheme.

Public Consultation on the draft Candidate EUCC Scheme

As result some major changes were implemented to the candidate EUCC scheme, mostly related to the:

Recommended publications

Public Consultation on the draft Candidate EUCC Scheme

This report presents the outcome of the public consultation on the first draft of the cybersecurity certification candidate EUCC scheme. The scheme…

Published on May 26, 2021

Cybersecurity Certification: Candidate EUCC Scheme

Published on July 02, 2020

Recommended news

Cybersecurity Threats Fast-Forward 2030: Fasten your…

The infographic released today by the European Union Agency for Cybersecurity (ENISA) highlights the top cybersecurity threats likely to emerge by…

Published on November 11, 2022

Crossing a bridge: the first EU cybersecurity certification…

Published on May 26, 2021

Recommended articles

Learn more about EU Cybersecurity Certification

EU Cybersecurity certification schemes will significantly impact the market of ICT solutions by

Regulation, regulation, regulation...

NIS2 (2022) - Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 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 (NIS 2 Directive)

- entered into force on January 16, 2023
- Member states have until October 18, 2024 to implement NIS2 into their national legislative framework

NIS2 - what is it good for?

NIS2 Structure:

I. General provisions:

- Categorisation of subjects into essential and important
- Definitions

II. Coordinated (national) cybersecurity frameworks

- Member states will need to:
  - Establish a national cybersec strategy
  - Designate one or more competent authorities responsible for cybersec and supervisory tasks + single point of contact
  - Designate one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises
  - Designate one or more CSIRTs

III. COOPERATION AT UNION AND INTERNATIONAL LEVEL

- Cooperation group (Member representatives, Commision and ENISA)
- CSIRT Network
- EU-CyCLONe
- Peer reviews

NIS2 - what is it good for?

IV. Cybersecurity risk-management measures and reporting obligations:

- Proactive (cybersecurity risk-management measures)
- Reactive (reporting obligation)
- Critical supply chain risk assessment
- Use of EU cybersecurity certification scheme

V. Jurisdiction and registration

VI. Information sharing

VII. Supervision and enforcement

- difference between essential and important entities (proportional and risk-based approach)
- opening to door to personal responsibility
- Fines up to 10 mil / 7 mil EUR or 2% / 1,4% world annual turnover, whichever is higher

VIII. Delegated and implementing acts

IX. Final provisions

NIS2 - Categorisation of entities

Entities are categorised as:

I. Essential

II. Important

- main difference is the stringency of supervision and severity of fines

Categories:

I. Sector (high criticality and other critical)

II. Size (depending on sector)

- size unimportant for:
  - DNS service providers
  - TLD name registries
  - qualified TSPs

III. Wildcard (subjective in each EU Member states

HIGH CRITICALITY

- Energy
- Transport
- Banking
- Financial sector infrastructure
- Health
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management (B2B)
- Public administration
- Space

OTHER CRITICAL

- Postal and courier
- Waste management
- Manufacture, production and distribution of chemicals
- Production, processing and distribution of food
- Manufacturing
- Digital providers
- Research

NIS2 - Cybersecurity risk-management measures

Proactive measure goals:

I. Stop cybersecurity threats

II. Mitigate consequences of incidents

Proactive measures shall include at least:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

NIS2 - Supply chains and related measures- interesting tidbits

Article 21

3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

Article 22

1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors.

Preamble:

(90) ...Potential non-technical risk factors, such as undue influence by a third country on suppliers and service providers, in particular in the case of alternative models of governance, include concealed vulnerabilities or backdoors and potential systemic supply disruptions, in particular in the case of technological lock-in or provider dependency.

NIS2 - Reporting obligations

Entities are obligated, without undue delay (within 24 hours of becoming aware), to:

- report all significant incidents to their competent CSIRT and competent supervisory authority
- in certain cases report such incidents to their service recipients

An incident shall be considered to be significant if:
(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Reporting to CSIRT:

- First report within 24 hours of becoming aware
- Update within 72 hours of becoming aware
- Immediate report upon CSIRT or competent body request
- Final report within one month of the incident

NIS2 - Croatian Cybersecurity Act proposal in consultation - tidbits for discussion

NIS2 implementation in Croatia through the Croatian Cybersecurity Act. First round of consultation was closed on August 16, 2023. Several controversial issues pointed out:

- Croatian Security and Intelligence Agency designated as competent and supervisory authority
- Imprecise categorisation provisions and very broad and subjective criteria regarding “wildcard” entities
- Imprecise provisions regarding personal responsibility of company management
- Possible barriers to market entry (authorisation given by ZSIS but no criteria provided)
- Several critical provision to be additionally implemented and decided upon by direct Decree of the Croatian Government
- Possible confidentiality and transparency issue due to implementation of the Sk@ut system within entities

Tijela za ocjenu sukladnosti

Članak 40.
(1) Ocjenu sukladnosti ključnih i važnih subjekata provode tijela za ocjenu sukladnosti.

(2) Tijela za ocjenu sukladnosti su privatni subjekti koji ispunjavaju organizacijske i stručne zahtjeve za autorizaciju propisane uredbom iz članka 24. ovog Zakona .

(3) Iznimno od stavka 2. ovog članka, tijelo za ocjenu sukladnosti za tijela državne uprave i druga državna tijela je središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti.

(4) Autorizaciju tijela za ocjenu sukladnosti iz stavka 2. ovog članka provodi središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti, a izdaje se na rok od pet godina.

(5) Središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti, tijekom važenja autorizacije provodi periodične provjere organizacijskih i stručnih zahtjeva iz stavka 2. ovog članka.

NIS2 - Conclusion

- It’s early to give accurate predictions on the precise effect of the legislation as implementation is underway;
- The wide scope of subject entities and the severity of fines for both the entities and management point to a serious intent to implement NIS2 as a regulatory framework for cybersecurity in the EU for years to come;
- We see an intent to “trickle-down” NIS2 compliance to the wider IT sector with broad supply chain provisions;
- While NIS2 will directly affect several tens of thousands of entities EU-wide, we can predict NIS2 indirectly affecting the IT sector on a wider, even global scale;
- The intent to push EU certification of IT products, services and systems may go either way as it could either make compliance easier and could provide for simpler one-stop-shop technical compliance solutions, while, on the other hand, it could be used as a possible tool for political control of the IT sector and as a tool for settling political issues with geopolitical rivals;
- We definetly expect more investments into cybersecurity in the following years as entities and subject down the supply chain seek to reach adequate compliance levels.
- We see a lack of qualified personel in the industry as a possible risk and a barrier to adequate implementation on an EU level;

Kontakt

THANK YOU!

Luka Porobija
Porobija & Špoljarić LLC

tel. 091/181-9688
mail. luka.porobija@psod.hr
https://www.linkedin.com/in/luka-porobija/