The NIS 2 Directive, Final Text

Article 12, Coordinated vulnerability disclosure and a European vulnerability database

1. Each Member State shall designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure. The CSIRT designated as coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party. The tasks of the CSIRT designated as coordinator shall include:

(a) identifying and contacting the entities concerned;

(b) assisting the natural or legal persons reporting a vulnerability; and

(c) negotiating disclosure timelines and managing vulnerabilities that affect multiple entities.

Member States shall ensure that natural or legal persons are able to report, anonymously where they so request, a vulnerability to the CSIRT designated as coordinator. The CSIRT designated as coordinator shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT designated as coordinator of each Member State concerned shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.

2. ENISA shall develop and maintain, after consulting the Cooperation Group, a European vulnerability database. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the European vulnerability database, with a view in particular to enabling entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services. All stakeholders shall be provided access to the information about the vulnerabilities contained in the European vulnerability database. That database shall include:

(a) information describing the vulnerability;

(b) the affected ICT products or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited;

(c) the availability of related patches and, in the absence of available patches, guidance provided by the competent authorities or the CSIRTs addressed to users of vulnerable ICT products and ICT services as to how the risks resulting from disclosed vulnerabilities can be mitigated.

Note: This is the final text of the NIS 2 Directive. The full name is "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)".

Articles, Directive (EU) 2022/2555 (NIS 2 Directive):

https://www.nis-2-directive.com/NIS_2_Directive_Articles.html (https://www.nis-2-directive.com/NIS_2_Directive_Articles.html)

CONTACT DETAILS

Cyber Risk GmbH, Dammstrasse 16, 8810 Horgen

+41 79 505 89 60

george.lekatis@cyber-risk-gmbh.com (mailto:george.lekatis@cyber-risk-gmbh.com;)

www.cyber-risk-gmbh.com (https://www.cyber-risk-gmbh.com)

SUPPORT

Cyber Risk GmbH has been established in Horgen, Switzerland (Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341).

The founder of the firm is George Lekatis. George has provided training and executive coaching in information security and risk management to many leading global organizations in 36 countries.

SERVICES

Home (https://www.cyber-risk-gmbh.com)

About (https://www.cyber-risk-gmbh.com/About.html)

Training (https://www.cyber-risk-gmbh.com/Training.html)

For the Board (https://www.cyber-risk-gmbh.com/Board.html)

Assessment (https://www.cyber-risk-gmbh.com/Assessment.html)

Social Engineering (https://www.cyber-risk-gmbh.com/Social_Engineering.html)

High Value Targets (https://www.cyber-risk-gmbh.com/High_Value_Targets.html)

Reading Room (https://www.cyber-risk-gmbh.com/Reading_Room.html)

Contact (https://www.cyber-risk-gmbh.com/Contact.html)

Impressum (https://www.cyber-risk-gmbh.com/Impressum.html)

© Cyber Risk GmbH. All rights reserved.