EUROSMART
The Voice of the Digital Security Industry

Revision of the NIS Directive

Introduction

The NIS Directive has been instrumental in increasing the cyber-resilience of the EU. As the first piece of legislation concerning EU-wide cybersecurity, the NIS Directive is the acknowledgment that incidents in one Member State can have significant cross-border impacts, hence requiring a common level of cybersecurity throughout the EU. The revision of the NIS Directive, together with the other EU cybersecurity initiatives, is an opportunity to foster Europe's Digital Sovereignty.

The deadline for transposition of the NIS Directive dates back from two years ago -9 May 2018- but there are already elements pointing towards a need for amendments. This is the case for the identification process of Operators of Essential Services (OES), but also the lack of identification of Digital Service Providers (DSPs). There are also vital sectors for society which are currently not included in the NIS Directive (eGovernment, telecommunications etc.). Finally, compliance with the NIS security requirements would be strongly enhanced with a mandatory certification of security products used by OES and DSPs.

Eurosmart calls for a revision of the NIS Directive that would repeal the current Directive and lead to the adoption of a NIS Regulation. The adoption of a regulation would foster harmonisation across the EU and hence resolve fragmentation issues, such as different sets of security requirements and diverging identification methods.

However, the functioning of the NIS cooperation group should be maintained. In addition, the decisions and technical documents of the NIS cooperation group should be translated into legally binding documents.

Eurosmart believes that the revision of the NIS Directive should take into account the following points:

Harmonised identification of OES and DSPs

Last October, the European Commission acknowledged that there was a fragmentation issue in the identification process of OES.[1] Identification methods greatly vary from one Member State to another. This leads to competition distortion as companies of the same nature might be imposed different requirements depending on the Member State where they operate. Likewise, a same company might be identified as OES in one Member State but not in another one, hence complying with different rules

[1] European Commission, Report form the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, 28 October 2019.

which creates additional burden. Therefore, it seems necessary to create convergence between the identification methods.

Moreover, this identification procedure should also apply to DSPs. In the current system, digital service providers must comply with a set of security requirements but are not identified by the Member States. This means that compliance with security requirements entirely depends on the ability and willingness of DSPs to define themselves as entities falling within the scope of the NIS Directive.

Enlargement of the scope of the Directive

Eurosmart believes that both the scope of OES and the scope of DSPs should be enlarged to include additional sectors. The current list of essential services (Annex II of the NIS Directive) does not include some sectors which are critical for the functioning of society, such as electronic public services (eGovernment) or telecommunications.

• Enlargement of the list of essential services

The list of essential services should include electronic public services (eGovernment) which are of utmost importance for citizens and businesses, especially during pandemic times. Disruption of electronic public services could result in businesses not being able to interact with the administration for registration or tax issues, citizens not getting their welfare benefits etc. Such dramatic consequences justify the inclusion of electronic public services in Annex II of the NIS Directive.

Telecommunication operators should also be included in Annex II, as they provide vital communication means to users. Due to the increasingly deeper interaction of communication networks, mobile operators have a strong impact on the infrastructure they use and deploy. In a risk-based approach, it is more and more difficult to differentiate the service from the network. Such telecommunication operators are likely to have an increased importance with the development of 5G, which will be relied on for connected mobility, automated industry etc.

Last but not least, the security of network and information should also be considered in the light of protection of information, technology and knowledge essential to Europe’s sovereignty and wealth against industrial espionage. Therefore, the definition of OES should be expanded to include all industries, Research and Technology Organisations (RTOs) and companies essential to Europe’s sovereignty (critical technology and industry, AI, digital etc.) and wealth (exporting industry).

• Enlargement of the list of digital services

The NIS Directive refers to Directive EU 2015/1535, which defines a digital service as “any service normally provided for remuneration, at a distance, by electronic means”. However, only three types of services must comply with the NIS security requirements: cloud, online marketplaces and search engines (Annex III).

An online marketplace is defined as a “digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace”.[2] Such a definition does not cover P2P marketplaces and should be revised to cover all types of marketplaces.

[2] Article 4(17) of the NIS Directive.

In addition, OTT [3]services should also be considered DSPs in the meaning of the NIS Directive, given their increasing importance in today's society.

Mandatory certification

The NIS Directive should leverage on the European security certification schemes created under the framework of the CSA (Cybersecurity Act Framework) to demonstrate the ability of critical infrastructures (OES and DSPs) to meet a high level of protection. Following a risk-based approach, certification of highly critical products must be done at a level of assurance "High" pursuant to the CSA (Cybersecurity Act Framework). In this perspective, it is expected that the European Cybersecurity Certification Framework (ECCF) provides the appropriate security certification schemes matching the very nature of the various products used by critical infrastructures (OES and DSPs), which is instrumental to reach high level of protection.

Security certificate at level "High" issued under the CSA (Cybersecurity Act Framework) is the only mean providing a high level of trust and confidence. It ensures a continuous monitoring and maintenance of the certification scheme by a community of recognised experts from the industry. It is the only way to ensure "the state of the art" of security for critical infrastructures.

Depending on the very nature of the product, the relevant security certification scheme shall be used. For some type of products, (e.g. secure hardware based), the future EU CC Scheme which is now under public consultation may be used. For other types of products, other certification schemes of level "High" such as the one proposed by the thematic group IACS Cybersecurity Certification Framework [4]led by ERNCIP and launched by the European commission may be used.

New security requirements

Supply chain security

Cyber-attacks on suppliers can jeopardise the smooth functioning of OES or the secrecy of its key data, as demonstrated by the Airbus case in 2019[5]. It is essential to ensure security throughout the entire supply chain of OES. Therefore, the security requirements laid down in the NIS Directive shall also apply to suppliers.

Digital infrastructures

DSPs rely on physical infrastructures (server, datacentre etc.). The security of their network and information also relies on the security of these physical anchors, which depends on external factors such as their location, their security and the law ruling them. To ensure the security of their network and information, all the physical anchors of DSP should be protected against any external actions that cannot be assessed, controlled mitigated, nor countered by the Member States. Therefore, digital service providers should use physical infrastructure exclusively located in Europe.

Security of 5G and mobile network

In the light of its critical importance for sovereignty, industry development and wealth of Europe, a special focus should be given to the security and resilience of 5G and mobile network. The security of

[3] An over-the-top (OTT) media service is a streaming media service offered directly to viewers via the Internet. OTT bypasses cable, broadcast, and satellite television platforms, the companies that traditionally act as a controller or distributor of such content.

[4] https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs

[5] Reuters, "Hackers tried to steal Airbus secrets via contractors: AFP", 26 September 2019.

5G and mobile network should take into consideration their specificities, such as the identification of user on the network (International Mobile Subscriber Identity – IMSI - in 4G and a Subscription Permanent Identifier – SUPI - in 5G). Compromising the privacy of user identification on the network (IMSI or SUPI) may be a first step to compromising access to restricted resources and ultimately compromise information, as it may allow impersonation attempts.

Therefore, a particular attention should be paid on that aspect, to ensure that user identification on the network (IMSI or SUPI) is encrypted before being disclosed. A security certification covering this cornerstone service for the global security of the mobile network should be explicitly required.

Furthermore, beyond supporting the privacy of users, the encryption of SUPI is also relevant to cybersecurity of critical infrastructures. 5G is instrumental for the advent of future technologies such as IoT, connected car, or Industry 4.0. Weaknesses in the network architecture allowing to locate a connected device, or even intercept some of its communication could be exploited to threaten the security of critical infrastructures. For instance, it could become possible for an attacker to impersonate another device or to tamper with its rightful communication.

Taking into consideration these threats, both to the privacy of user but also to the security and resilience of OES, Eurosmart calls for:

- the definition of an ad hoc security certification scheme covering SUPI encryption within 5G SIM / eSIM under the CSA, taking into consideration the constraints of the market;
- regulatory act mandating (1) SUPI to be encrypted within the 5G SIM / eSIM, and (2) 5G SIM / eSIM to be mandatorily security certified, to demonstrate its security capabilities. Mandatory certification could be established via an Implementing Regulation, as foreseen by Article 16(8) of the NIS Directive.

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels** representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **GS TAG**, **Huawei**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Thales**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**,), consulting companies (**Internet of Trust, Trust CB**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multi-stakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com
@Eurosmart_EU
@Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com