



NIS 2.0 cyber resilience and ENSURESEC – Ensuring security and privacy for the resilience of e-commerce

BY JENNY BERGHOLM - 12 JANUARY 2021

On December 2020, the [European Commission presented its proposal](#) for a revision of the [Directive on the security of network and information systems](#) (the NIS Directive). This blogpost looks into the news of NIS 2.0 and makes an initial assessments of what the proposed Directive would mean for the H2020 project ENSURESEC, which is introducing an end-to-end security solution for e-commerce providers.

In times of a global pandemic, the security pressure on e-commerce has increased. From the online presentation of the goods to the consumer to the product delivery, passing through online payment tools – every step of the process is facing threats on a cyber and/or a physical level. The Horizon 2020 project [“End-to-end Security of the Digital Single Market’s e-commerce and Delivery Service Ecosystem \(ENSURESEC\)”](#) aims to address these issues and thereby improve the EU’s vision of a reliable and trusted Digital Single Market. KU Leuven has already identified ENSURESEC as within the scope of the current NIS Directive, since some of the partners are Digital Service Providers.

As many have already noticed, the proposal of the European Commission has provided some changes to the existing cybersecurity framework. Now, let’s have a look at what NIS 2.0 would bring for ENSURESEC.

First, NIS 2.0 would scrap the existing distinction between Operators of Essential Services and Digital Service Providers. It concentrates on medium and large companies as well as companies regardless of size with a high risk profile. NIS 2.0 identifies many providers of digital infrastructure as such (Article 2(2)). The material scope of NIS 2.0 is wide. It comprises so called “essential entities”(Annex I) and “important entities” (Annex II). Both types of entities concerns public or private entities active in sectors such as transport, banking, digital infrastructures and digital providers. Under the currently in force NIS Directive, Member States have been asked to identify entities which falls under the scope of the Directive. This has been combined with generally applicable obligations applicable to all entities which fall under the definitions of the Directive.

Second, operators falling within the scope of NIS 2.0 will need to take “appropriate and proportionate technical and organisational measures to manage cybersecurity risks”. The wording highlights that the measures required for compliance depend on a case-by-case assessment, taking into account the risks of the activities of an entity. Article 18 of the proposed Directive provides a helpful, but non-exhaustive list of measures required. These are the following:

- risk analysis and information system security policies,
- incident handling, business continuity and crisis management,
- supply chain security,
- security in network and information systems acquisition, development and maintenance,
- policies and procedures assessing the effectiveness of cybersecurity risk management measures and
- the use of cryptography and encryption.

Both essential and important entities are subject to notification requirements for significant incidents (Article 20). An incident is considered significant, if it causes or could cause significant financial losses to or substantial operational disruptions for the activities of the entity (Article 20(3)). An incident is also significant if considerable material or non-material losses are caused to others (Article 20 (3)). Member States may also require that certain ICT products, services and processes comply with certain European cybersecurity certifications.

Keeping all the presented aspects in mind, the contribution of ENSURESEC in making it easier for e-commerce to comply with security obligations will be valuable. It enables entities to ensure security of their operations, throughout their whole e-commerce activity, end-to-end. This will ease the burden of entities within the e-commerce sector falling within the scope of NIS 2.0. Let’s have a closer look at the technical details of the ENSURESEC tool.

Through **prevention**, e-commerce operations using the ENSURESEC-tool are assessed and certified to be secure against certain classes of critical attacks and vulnerabilities. **Monitoring** run-time interface operations at application and network levels contributes to detecting threats more effectively as well as to building resilience against them. If an attack or a new vulnerability is detected, the ENSURESEC **response** module makes sure that the system continues its operation in a fail-safe mode, and communicates an appropriate way to react to the impact, including **mitigation** attempts, to affected users and e-commerce partners.

The e-commerce sector offer a lot of possibilities, especially in the current new normal everyday life so impacted by the COVID-19 pandemic. But with the use of e-commerce, comes also the risks of misuse of credentials, disruptions in payment services and theft of goods bought online.

ENSURESEC aims to create a security platform, which meet the security needs of the e-commerce sector, both when it comes to cyberthreats and to hybrid threats that involve physical aspects. E-commerce platforms, or parts of an e-commerce ecosystem can easily be found within the scope of NIS 2.0, especially banking services, the transport and logistics companies delivering products as well as the e-commerce platform itself. These are often accompanied with a cross-border element, with different actors in different EU Member States (or outside for that matter). The [European Commission has identified](#) the inconsistent treatment of entities in different Member States as well as the lack of cybersecurity measures taken by companies which have been out of scope of NIS 1.0 as two of the main issues of the current legislation. The fact that the treatment of the entities in Member States is intended to be aligned has potential to bring more stability to cross-border operations.

However, NIS 2.0 also raises some questions. For one, it will be interesting to see how the terms “essential entities”(Annex I) and “important entities” (Annex II) will be implemented. The European Commission motivates the difference of the two based on the “level of criticality of the sector or type of service”. According to this logic, important entities are those active in sectors which are important for economies and societies, but not as vital as essential entities. The question then arises, can an entity fall under both categories? This problem is well illustrated by the digital sector. In particular, Annex I, point 8 identifies “digital infrastructures” as essential entities. Simultaneously, Annex II identifies “digital providers” as important entities. This, and the effects the unclarity would mean for ENSURESEC, should be subject to further research.

On the role of KU Leuven for ENSURESEC:

Of a consortium of 22 partners from 14 different countries, KU Leuven’s Centre for IT & IP law (CITIP) is the legal and ethical partner, focusing its research on the law and ethics of innovative technologies in the area of privacy and security. CITIP advises the technical partners in their endeavours to create an innovative security tool with its starting point in data protection by design and default while ensuring the security of the whole lifecycle of an eCommerce business. In late 2020, KU Leuven delivered the first of its main deliverables, a report on the legal and ethical framework for a project at the cross-section of privacy, security and innovative technology.

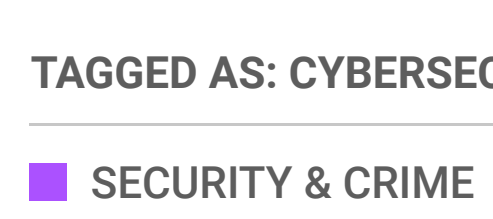
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883242.

This article gives the views of the author(s), and does not represent the position of CITIP, nor of the University of Leuven.

ABOUT THE AUTHOR – JENNY BERGHOLM
Jenny Bergholm is a Research Associate at the Centre for IT & IP Law (CITIP) of KU Leuven with a LL.M. from the University of Helsinki, with focus on EU and data protection law. Having worked for both the European Parliament and the European Commission in Brussels, she is focusing her research on data protection, cybersecurity and AI.

→ [VIEW ALL POSTS BY JENNY BERGHOLM](#)

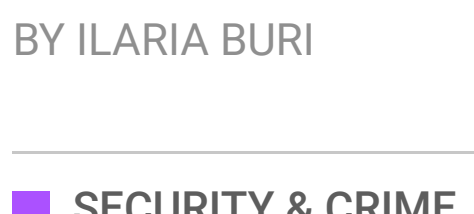
TAGGED AS: CYBERSECURITY, E-COMMERCE, H2020, RESILIENCE, SECURITY

 SECURITY & CRIME

SIMILAR ARTICLES

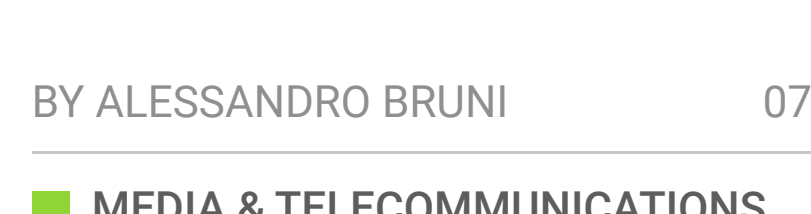
Cyber-Resilience and Critical Infrastructures: All the more reasons for a CyberSANE solution

BY ILARIA BURI
26 NOVEMBER 2019

 SECURITY & CRIME

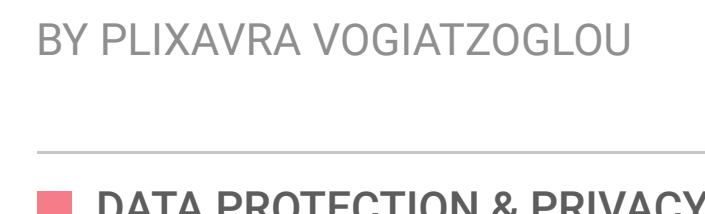
The NeverEnding story: lack of common security protocols in the electronic communication sector

BY ALESSANDRO BRUNI
07 APRIL 2020

 MEDIA & TELECOMMUNICATIONS

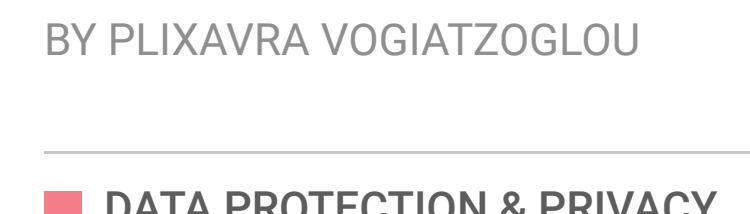
Privacy International & La Quadrature du Net: the latest on data retention in the name of national and public security – Part 1

BY PLIXAVRA VOGIATZOGLOU
15 OCTOBER 2020

 DATA PROTECTION & PRIVACY

Privacy International & La Quadrature du Net: the latest on data retention in the name of national and public security – Part 3

BY PLIXAVRA VOGIATZOGLOU
27 OCTOBER 2020

 DATA PROTECTION & PRIVACY

COMMENTS