doi:https://doi.org/10.61841/7k8bwj71 url:https://nnpub.org/index.php/SSH/article/view/2747

THE IMPORTANCE OF THE NIS2 DIRECTIVE AND THE POTENTIAL CHALLENGES IT ENTAILS

Darina Shamatonova
Catholic University of Lyon, Lyon, France
d.shamatonova@gmail.com

How to cite this article:
Shamatonova, D. . (2025). The importance of the NIS2 Directive and the potential challenges it entails. Journal of Advance Research in Social Science and Humanities (ISSN 2208-2387), 11(1), 46-48. https://doi.org/10.61841/7k8bwj71

ABSTRACT
This paper seeks to research main amendments introduced with NIS2 Directive within EU territory, its importance to cybersecurity and challenges it entails to routine workflow of corporates

KEY WORDS:NIS2, cybersecurity, cybercrime, critical infrastructure

INTRODUCTION

The NIS2 Directive[1], which entered into force on 16 January 2023, requires Member States to implement its provisions within a two-year period, until 17 October 2024. The previous legislation on cybersecurity consisted of Council Directive 2008/114/EC[2] and previous version of NIS Directive[3] with a patchwork of different pieces of sectoral regulations[4]. The new version of NIS should have played a crucial role in ensuring the cyber resilience[5] of critical infrastructure across the European Union and become an improved version of previous framework guaranteeing a better level of cybersecurity, but probably it did not meet the goal.

NOVELTIES OF NIS2

Companies regardless of their size have become dependent on various computer systems and services, which has attracted the interest of cybercriminals (Dragomir, 2021)[6]. Thus, NIS2 was aimed to identify important and essential services[7] and the establishment of security requirements for these services. It defines critical infrastructure sectors and enforces security standards, especially with vital services such as energy, water, ICT, transport, healthcare, and finance[8], which will be under the most stringent supervision of the Directive[9]. As a result, almost every and all companies, including small and medium ones, especially if they form part of supply chain for infrastructural sectors, have to put themselves into acknowledgment of NIS2 requirements and reproduce them in action, as well as comply with reporting obligations, which might be problematic for most of them. Implementation of complex security requirements is the main

[1] 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
[2] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
[3] 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
[4] Preamble (4) and (5) of NIS2, Article 4 of NIS2 (Sector-specific Union legal acts)
[5] Preamble (2) of NIS2
[6] Dragomir, A.V., 2021. What's New in the NIS 2 Directive Proposal Compared to the Old NIS Directive. SEA: Practical Application of Science, 9(27), page 156, available at: https://seaopenresearch.eu/Journals/articles/SPAS_27_1.pdf (date of access: 23 May 2024)
[7] The essential and important entities and services are defined in Article 3 of NIS2
[8] These sectors above underline those that will be under the most stringent supervision of the Directive
[9] KPMG, Levelling-up your IT and OT security capabilities in light of the NIS2, August 2023, Page 5, available at: https://assets.kpmg.com/content/dam/kpmg/kr/pdf/2023/kpmg-eu-nis2-report.pdf (date of access: 23 May 2024)

challenge of new legislation and may prove to be more difficult for smaller organizations with limited resources. Besides companies would need to draft local documents on arrangement of cybersecurity system and measures within the company and allocated liabilities for certain officers. Anyway, this is not an issue of one day and NIS2 allowed enough time for the entities to build their workflows in line with the new legislation, besides further guidelines with particulars from EU authorities would follow to make the task easier for common companies.

REPORTINGS AND PERSONAL LIABILITY

The two most **important**, significant and indisputable enhancements of NIS2 are short-reporting and personal management liability. First, the shortened 24-hours term for notification of incident replaced previous 72-hours term. The new notification is obligatory[10] and should contain only essential details of what has happened without the need to report details of counter-actions. As Schmitz-Berndt mentions (2023), where lines are blurred, there is a strong likelihood that—in addition to economic reasons to refrain from reporting – this vagueness also deters entities from incident reporting[11]. This NIS2 made notification easy for every person, even without specific knowledge, by filling up an easy form on the website and this simplification is important for popularization of notices (especially taking into account coverage by NIS2 of average companies with no experience or expertise). From perspective of cybersecurity landscape, it would mean a prompt acknowledgement of attacks happening, that might be taken into account by authorities and specialists helping to react to other targeted companies and protecting the whole system. It also brings more transparency into information on scale and types of attacks as previously many companies tended to conceal incidents data.

The second positive novelty is personal liability of top managers of companies for real and practical (and not just paper-compliance[12]) implementation of cybersecurity measures and necessity to introduce a special officer in charge, also for a regular reporting purpose. Regular reporting obligation would mean real compliance with the requirements, and feel of personal liability (as a natural person, not an entity) would motivate managers to give own attention to problems of building cybersecurity and maintaining its level within a company. Now it became impossible to delegate the issue (and liability) to someone else, and thus personal approach and permanent control is guaranteed. Additional positive side effect would probably be the increase of financing[13] to cybersecurity shield (and IT specialists) as managers would be under pressure of personal liability in case of inadequate compliance.

PUBLIC LEVEL OF NIS2

Furthermore, on a public level, NIS2 aims to improve collaboration and information sharing[14] among EU Member States by creating special teams for research and reacting to threats. It helps to improve common knowledge and practical skills (through experience sharing) in respect of different types of incidents allowing for effective allocation of efforts for prevention of large-scale attacks. Also, it helps early threat detection that is the core in protecting systems and

[10] In the previous version of NIS notification was also obligatory, but the new version underpins this obligation with a personal liability of top management as well as officials in response for cybersecurity measures with fines for non-compliance, so in updated version of NIS this reporting obligation shall become a real instrument

[11] See for example Schmitz-Berndt, S., 2023. Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. Journal of Cybersecurity, 9(1), p.9

[12] Valentino Lucini (2023). The Ever-increasing Cybersecurity Compliance in Europe: the NIS 2 and What All Businesses in the EU Should be Aware of. Russian Law Journal, 11 (6S). 149

[13] Johan David Michels marks under-investment in cybersecurity and failure to disclose information on breaches as main problems of current cybersecurity regime, see: Michels, J.D. and Walden, I., 2020. Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?. European Law Review. 28

[14] Chapter VI of NIS2 (Information sharing) is dedicated to information sharing, coordination of actions and relevant procedures

ultimately strengthens the overall security posture. The single points of contact[15] should ensure effective cross-border cooperation via forwarding notifications of significant incidents[16].

Other innovative milestones of NIS2 are standardization[17] and certification[18]: companies shall consider using certified products and services to enhance security. Member States shall encourage essential and important entities to use European standards to the security of network and information systems as well as use particular ICT products, services and processes, developed by themselves (or third parties), that are certified under European cybersecurity certification schemes. This shall prevent usage of unqualified services and enhance cyber resilience on the one hand, but on the other hand it may lead to bureaucracy in ICT sector and over paper-compliance through obtaining certificates in order to demonstrate usage of trusted technologies. However, the aim of this legal rule was to simplify check of cyber compliance of third parties before entering into relationship with them, as possibilities to check and monitor third party's resilience are limited. While such resilience is very important, especially for combating supply chain threats[19], it could be evidenced by demonstration of relevant certificate of compliance. So, this innovation may become an effective decision of a problem.

CONCLUSION

Finally, all the novelties of NIS2 are encouraged to be implemented into practice by severe penalties for non-compliance. Fines of 10m EUR or 2%[20] of turnover may become quite high and burdensome for some of the companies and even might lead to a bankruptcy or detrimental financial impact. High-scale liability is aimed to bring attention to the seriousness of the problem and add weight to the necessity of implementation of requirements. However, it may become too severe taking into account a quite sudden and complex character of new requirements without clear guidelines and schemes for those participants who lack expertise in cybersecurity field. Even with all those outlays the new legislation framework should bring more attention to current cyber threats and make the regional landscape more secure. However, according to Fergusson (2023), the application of statutory interpretation and cyberattack model analysis indicated that the cybersecurity risk management measures required of essential and important entities under the NIS2 Directive can appear to be significantly limited in their effectiveness against cyberattacks[21].

[15] Definition of single point of contact is contained in Paragraph 3 of Article 8 of NIS2: each EU Member State shall designate or establish a single point of contact (competent authority) that have adequate resources to carry out, in an effective and efficient manner, cybersecurity tasks

[16] Preamble (40) and (70) of NIS2

[17] Article 25 of NIS2

[18] Article 24 of NIS2

[19] The European Union Agency for Cybersecurity rank supply chain cyber-attacks as popular type of cyber threats, see: ENISA Threat Landscape 2023 (October 2023 report), page 7

[20] Article 34 of NIS2 requires Member States to implement administrative fines of a maximum at least EUR 10m or 2% of total worldwide annual turnover whichever is higher – for essential entities (paragraph 4); for important entities (paragraph 5) fines are EUR 7m and 1,4% of turnover. Periodic penalties are also allowed (paragraph 6). While personal data breaches are still subject to GDPR penalties (Article 35 NIS2) with no double liability

[21] Ferguson, D.D.S., 2023. The outcome efficacy of the entity risk management requirements of the NIS 2 Directive. International Cybersecurity Law Review, 4(4), pp.371-386. available at: https://link.springer.com/article/10.1365/s43439-023-00097-8 (date of access: 23 May 2024)