Position Paper – Roadmap NIS-Review

Bitkom views concerning the combined Evaluation Roadmap / Inception Impact Assessment

13 of August 2020

Introduction

Bitkom strongly welcomes the integration of relevant stakeholder opinions in order to streamline public and private efforts striving for an improved cybersecurity throughout the European Union (EU). That is why we would like to seize the opportunity and provide our feedback already at an early stage of the revision of the Directive (EU) 2016/1148 concerning measures for implementing an equivalent and commonly high level of security in network and information systems across the Union (hereafter referred to as the NIS Directive). As the first milestone on the way to a revised legislative proposal scheduled for Q4 2020, we value the recently published and combined Evaluation Roadmap / Inception Impact Assessment for sharing our insights and position with the Commission.

As in past years, Bitkom strongly endorses the EU in its efforts to substantially and sustainably strengthen the resilience of networks and systems against cybersecurity risks across Europe whilst deepening the harmonization of the European Digital Single Market and avoiding fragmentation at the same time. Our position is guided by the urgent need to create a more coherent and harmonized common level playing field for operators of essential services (OES) as well as for digital service providers (DSP) across the Union. We are convinced that common and harmonized cybersecurity rules at EU level are the most effective way to achieve a higher level of cyber resilience.

Bitkom shares the commissions' overall assessment that, since its adoption, the NIS Directive has enabled and further facilitated the advancement of cybersecurity capabilities within EU Member States. However, we are witnessing constantly evolving threat scenarios and expanding attack surfaces, putting network and information systems at great risk. Therefore, and in line with the Commissions line of reasoning expressed in their Roadmap, Bitkom equally sees the necessity to advance the deadline foreseen under Article 23(2) and to review the NIS Directive before the end of 2020.

In tangible terms, **we endorse the third policy option**, namely targeted regulatory intervention. While the empirical evidence provided by the OLS Report revealed several persisting inconsistencies that are best addressed by legal amendments, we remain cautious to adopt an entirely new legislative act. Although well-intended, the latter

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

Sebastian Artz
IT Security
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

(policy option four) would imply a long and time-consuming process that may not keep up with the constantly evolving particularities of the cyber and IT security. Hence, we call instead for an approach that addresses the most pressing issues in the first place by revising certain aspects of the NIS Directive but still offers the private sector the necessary leeway in order to develop its own content-tailored solutions and innovative ideas to significantly strengthen Europe's cyber-resilience. The protection of networks and systems against any form of disruption is in the innermost interest of OES and DSP.

Furthermore, the scope of the revised directive should be in accordance with the most serious threats for network and information security. In the case of OES, member states are allowed to impose stricter security and notification requirements than those enshrined in the current Directive. This does, however, not account for DSP. Bitkom continues to favor a "light-touch" regulatory approach as the appropriate way forward concerning DSP, especially in view of their rapidly changing nature and innovative potential.

Key Aspects

In the light of the past experiences of our membership and in line with the findings of the OLS report, we strongly recommend to **make the persisting communication bottlenecks the centerpiece of the NIS-Review**. Instead of enforcing legal compliance by means of new legal measures, we encourage a closer cooperation between the Commission, the EU member states and the private sector. To this end, the Commission is asked to consider the broad range of impactful and promising German public-private initiatives that have been already put in place. Most notably, the alliance for cybersecurity, launched by Bitkom together with the Federal Office for Information Security (BSI) in 2012, and the UP KRITIS may serve as European role models to enhance the cross-border information sharing and to strengthen the cooperation mechanisms of the member states in the area of network and information security.

Resolving communication impasses is not only of utmost importance for addressing shortcomings and inconsistencies of the past. New communication bottlenecks are looming and must be consequently addressed in a proactive manner by the Commission – in close consultation with the member states – already at this stage of the consultation period. If not properly addressed, we run risk of introducing new inconsistencies, negative feedback loops and fragmentation while actually striving for European harmonization. With this, we refer primarily to two major aspects. First, we face the **simultaneous revision of the German IT-Security Law and the NIS-Review**. Second, the revision of the NIS Directive comes together with an **unexpected parallel update of the European Critical Infrastructure (ECI) Directive 2008/114/EC**. Both will be addressed in the following.

German IT-Security Law 2.0 and the revised NIS Directive

At this point, we have to broaden the scope and touch upon the currently discussed revision of the German IT-Security Law. Back in 2016, when the NIS Directive was adopted, the German IT-Security Law from 2015 provided valuable guidance for the European NIS directive. During the current revision process, **the German example should still serve the Commission as a major point of reference and upper benchmark**, when striving for European harmonization.

However, we encourage the Commission to intensify the communication with the German government because lawmakers started working on a new IT-Security Law (2.0). To our regret, this was done without having entered into dialog with those OES that fall under the jurisdiction to properly evaluate the impact and effectiveness of the IT-Security Law as well as to assess its need for revision. As a consequence, we are concerned that the temporal overlap of the revision of the German IT-Security Law and the NIS-Review may lead to new legal misalignments and run counter to the shared objective of improving the protection of critical infrastructures. Of particular relevance in the context of the NIS-Review is the intention of the German government to introduce the new category “companies of special public interests”, as expressed in the draft law that was leaked on May 7, 2020. The introduction of such a distinct category on the national level would further splinter the pan-European understanding of critical infrastructures and essential services. **Rather than unilateral approaches we strongly advice a coordinated European answer** as the very nature of Cyber and IT-Security requires to go beyond national borders in order to develop fruitful approaches.

Interplay of the ECI and the NIS Directive

The biggest foe of security is complexity. The same holds true for legislation and respective reviews. It remains tricky to fully embrace the intention of reviewing the ECI- and the NIS-Directive simultaneously under the supervision of two distinct directorates without providing guidance or expectation management concerning the future interplay. While the ECI Directive is rooted in the identified need to counter threats from terrorism and focuses exclusively on the transport and energy sector, the NIS Directive aims to increase the levels of cybersecurity across the Union, in particular on the level of national cybersecurity capabilities and the capacity to mitigate growing security threats to network and information systems.

Although we are well aware of the fact that cyber-related issues are not yet fully congruent with all (physical) threat vectors to critical infrastructures, the division into IT and physical security is becoming increasingly blurred. This development is likely to continue in the years to come. In the context of critical infrastructure protection, we encourage the Commission to also understand cybersecurity as a means to an end for safety. Subdivisions based on the motivation of the attackers are irrelevant in most cases. It makes no difference whether an attack on critical infrastructure is launched by an economically oriented cybercriminal, a governmental organization or a terrorist. They use the same procedures and affect ultimately the same objectives to which we are committed:

- business continuity,
- readiness for response / resilience,
- better prevention.

Furthermore, the orientation by sectors and funds is not necessarily appropriate. Attacks are also launched against processes and procedures without any particular technical reference. Future legislation should take this further into account. The security of networks and systems can only be achieved holistically. Technology, organization, and the human factor must be included and also reflected in the laws. What is needed is a European harmonization of the sectors included and of the requirements (general and sectoral). This remains difficult to convey to a regional and sectoral structure of authority.

From our perspective, the NIS Directive represents a more inclusive horizontal approach and, therefore, is the more sophisticated instrument to counterbalance cybersecurity risks, including terrorism, which has become a hybrid digital threat by now. Against this backdrop, and in order to avoid any kind of double legislation, we call for a more integrative and combined approach merging the overlapping points of both directives within the NIS Directive, while taking the crucial differences between these two categories further into account, which are reflected in different levels of security risks and dependencies.

Regulatory coherence

In view of the aforementioned interplay of the ECI and the NIS Directive, we must explicitly outline that anything but seamless cooperation and close coordination between the different directorates during the parallel consultation process would be completely counterproductive and undermine the overall objective of increasing the resilience of critical infrastructures across Europe. This also applies to other ongoing European legislation and initiatives that are related to the cybersecurity resilience of infrastructure, such as the digital operational resilience act in the financial sector.

Besides the cyber-domain, the overall European legal landscape cannot be left unaddressed. The successful review of the NIS Directive must also consider reporting authorities, thresholds, timeframes, and penalties enshrined in other EU legislations (GDPR, eIDAS, among others) to ensure an overall cross-legislative alignment. Persisting redundancies in terms of incident reporting and double notification requirements under different legal regimes are to be streamlined during the current review process. In the same vein, successfully established voluntary information sharing structures should not be overburdened by simply turning them into more bureaucratic notification obligations and incident reporting requirements.

Adjusting the Scope of Critical Infrastructures

In the light of the broad range of sectors and subsectors that are considered as critical infrastructure or essential services by the different EU member states, as illustrated by the OLS report, we encourage the Commission to conduct a comprehensive cross-country sector mapping following a risk-based and layered approach combined.

We generally support an enlarged definition of what is seen as the European critical infrastructure baseline. In the German case, the government is planning to introduce “disposal” as a new sector of the critical infrastructure. From our point of view, the decision to additionally consider “disposal” as a critical sector is reasonable. However, we would appreciate that any extension of the scope of essential services / critical infrastructure is done at the European level to foster the harmonization of the Digital Single market and to avoid any form of market distortion. At the same time, the harmonization between the Member States based on a cross-border consultation process should give national authorities enough freedom in the identification process so that national and sectoral specificities can be taken into account.

In general, any expansion and harmonization must be guided by scientific reasoning and should not be the outcome of mere political interests. Empirical analyses and research with consultations from industry and other relevant stakeholders is all the more relevant when it comes to a potential extension or a changed definition of what constitutes a DSP. From our point of view, the current understanding of DSP is sufficiently precise to balance the need for above-average cybersecurity requirements with the necessary ‘light-touch’ to gives enough room for innovation. As recognized by the NIS directive, there are fundamental differences between OES and DSP, which is the reason why DSP are subject to different rules (Recital 57). The security measures for DSP should be lighter than those for OES. DSP should be free to define how they ensure the protection of their network and information systems appropriate to the risks presented. The security measures should be process-oriented and focus on risk management. They should not require that ICT products be designed, developed or manufactured in a particular manner (Recital 51). Such distinction should be maintained as the reasons for applying the different rules remain valid. When it comes to OES, the methodologies to identify operators and thresholds should be clear, transparent and comparable. Irrespective of whether the identification process is carried out by the competent authorities of the member state themselves or as part of a self-identification, it should be possible for OES within the scope to verify by themselves whether they meet the requirements.

Closely linked to the aforementioned point is our recommendation that the discussion should not only center on the mere extension of what to consider as critical infrastructures, but also on what not to consider as such. This also refers to the change in narrative during the ongoing Covid-19 pandemic. The public discourse has been marked by a different, sometimes misleading, understanding of critical infrastructures. The term was less seen under the aspect of what is worth protecting but more under the aspect of what has to function and to be maintained. That's why Bitkom recommends to stay focused on cyber threats within the scope of the NIS Directive and to **not confound the maintenance of supply chains with the criticality of the IT to ensure the supply of a good or a service**. The process of the NIS-Review should be viewed and thought through from the latter point of reference / departure. As the Roadmap also touches upon Covid-19, the Commission should stick to clear definitions and avoid any (scientifically) unjustified inflation of what to consider as critical infrastructure. Such impulse-guided scope expansion would only lead to even more fragmentation in the aftermath of the global health crisis.

Improving Information Sharing Between Countries & Stakeholders

We remain firmly convinced that further enhanced and structured information sharing between stakeholders is an essential prerequisite for the effective countering of cyber threats. After having updated and expanded the baseline of what qualifies critical infrastructure under the scope of the NIS Directive, the Commission should put its focus on establishing a common level-playing field for those sectors across countries in terms of harmonization and information sharing.

Bitkom represents more than 2,700 companies of the digital economy, including 2,000 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.