Technology Industries of Finland

Finnish Information Security Cluster Kyberala

5/20/2022

Cybersecurity: how to enhance Europe's preparedness and resilience[1]

Measures to enhance European resilience

Europe will be subject to elevated number of cyber-attacks in coming months. To protect our people, societies and businesses, Europe needs to be prepared. The ongoing war has helped us to stand united. It is the same unity that will help us prepare for cyber-attacks and raise the level of resilience.

Relevant experience also from Ukraine shows clearly that vulnerabilities of the system components can only be patched by original manufacturers. We need to have solid information of components and features of the connected products to understand and facilitate the identification of vulnerabilities and threats by the right people at the right time. We need European Cyber Security Data Space. We need co-operation between officials and companies. European co-operation should address processes to cover the ever-changing cyber threats and allow for protection of connected systems.

Europe also needs to discussion on doctrine of cyber-attacks as well as operational cyber defence capabilities. EU needs to work on the attribution capabilities and develop a real cyber diplomacy – a **Political Cyber Playbook**. One chapter of it should be the **Cyber Toolbox**, containing means under diplomatic, informational, military, and economic domains.

Cyber Resilience Act

Technology Industries of Finland (TIF) has contributed to and subscribes to the Digital Europe's position paper in full. In addition, we would like to emphasise the following three points for forthcoming EU horizontal cyber resilience regulation:

1. EU needs cyber security regulation

The regulation should form basis for elements of cybersecurity requirements, covering the whole lifecycle from design to recycling. CRA should address requirements on **software updates** and manufacturer's responsibility over their product to create security through the product lifecycle.

The business risks related to cybersecurity, caused by insecure digital products and ancillary services, are considered significant by the companies, and will increase in the future. According to a recent survey, 34 percent of Finnish SMEs regard risk of cyberattacks and data breaches high or reasonably high for their business. Only seven percent of the respondents see no risk at all. 61 percent of companies report obstacles in ensuring their cybersecurity, the biggest challenges being inadequate skills and the cost.

Especially SMEs also often find it difficult to single out quality secure -solutions and vendors from insecure ones due to the lack of transparency of cybersecurity features and standards. The absence of trust creates uncertainty and can result in SMEs holding back their much-needed investments in digitalisation.

[1] By resilience we mean the ability to withstand various cyber-attacks and recover into a defined mode of operation after an attack. It consists of technical (e.g., in design) as well as organizational (e.g., in operations) measures.

2. Regulation should cover all connected products truly horizontally

The scope of the CRA should be wide enough to create coherence across the products currently regulated under the NLF, but specific enough to only address products or product components that can be a target, or be part of, various forms of cyberattacks.

TIF warmly welcomes Commission's text in the associated *Call for Evidence for an Impact Assessment*: "This intervention would aim to improve the Internal Market's functioning by: (i) **streamlining and supplementing existing rules**; and (ii) preventing further fragmentation of cybersecurity requirements [...]".

Hence, the regulation should cover all devices connected to the Internet to deliver maximum effect. A vulnerable or unprotected connected device is a threat no matter its intended purpose, and as part of a computer-system or a network it can compromise data or the function of the system. Consequently, all connected products, including devices for general purpose computing, and all types of firmware and operating systems should be included in the scope of the regulation when they are embedded, or intended to be embedded (such as software patches) into a product, i.e., software that is necessary for the intended function of the product.

For any such connected product the cybersecurity requirements and corresponding conformity assessment should be covered by the CRA and include a stipulation that conformity with CRA provides conformity with other sectoral regulations (RED, MDR, GPSR, CSA, DORA, etc.[2]), and where not possible, make a reference to the appropriate regulatory requirement.

3. Regulation should set out baseline requirements

Defending against ever-evolving threats requires agility and innovation but drafting requirements that improve security while fostering agility and innovation can be difficult. High assurance conformity assessment methods are often costly and time consuming – and exacerbated by skills and infrastructure gaps that require long-term investment. Consequently, while building specific requirements or more demanding conformity assessment procedures on the product's intended use and a risk assessment, it is further emphasized that the object of the requirements should be the connected product itself, not its separate components *per se*, be it hardware or software.

The CRA should set out technology-neutral essential requirements for cybersecurity in the form of requirements common to the connected products that are within its scope, where required by a risk analysis. Essential requirements should include requirements for processes and design, such as secure development/production (SecDevOps/DevSecOps), vulnerability report management (including Vulnerability Disclosure Policies) and duration of lifecycle support. In practice, internationally recognised standards should be used whenever available. On global arena, EU should seek to find mutual recognition arrangements with likeminded jurisdictions and organizations. Furthermore, it should be noted that requirements *de facto* leading to product life-cycle management with updateability an expected outcome is the longer support manufacturers will provide, the higher the cost. The curve of cost increase is likely to become steep due to the complexity of supply chains and version management of prodcuts.

Due to the quantity of covered devices, conformity assessment should be managed through self-assessment as default option and should build on the conformity assessment procedures that are set out in the current NLF (Decision 768/2008). Certification should be available to actors aiming

[2] Delegated acts under the Radio Equipment Directive, the Medical Devices Regulation, the Cybersecurity Act (establishing a cybersecurity certification framework for products and services) the Draft General Products Safety Regulation and Regulation on digital operational resilience for the financial sector.

to voluntarily seek further affirmation for their products and services on a flexible and modular way, as adopted under the Cybersecurity Act, or for industrial IoT certification IEC 62443.

Such approach underlines the principle that manufacturers must guarantee and be responsible for the safety – and in this case, the cybersecurity of their products due to the simple fact that users and customers have not, and will not, be able to take such role. The preferred way is to leverage the current framework for market surveillance and compliance of products covered by Regulation 2019/1020. In the end, the effectiveness of the regulation boils down to the combination of having the right requirements, balanced and proportionate requirements and effective market surveillance.

Inquiries

Peter Sund, CEO, Finnish Information Security Cluster, +358 50 565 0621, peter.sund@techind.fi
Jussi Mäkinen, Director, EU Regulation, +358 40 900 3066, jussi.makinen@techind.fi