kaspersky

Kaspersky's suggestions for the protection and resilience of critical infrastructure in the EU

April 2020

kaspersky

www.kaspersky.com
www.securelist.com

Executive summary

Kaspersky is grateful for the opportunity to provide comments to the EU's Critical Infrastructure Protection (CIP) policy framework. We support the improvements made in the EU in this field, including the adoption of the European Critical Infrastructure (ECI) directive (2008/114) and the Directive concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) (2016/1148).

However, both the rapid development of emerging technologies and the resulting changing threat landscape have the potential to impact the EU's CIP significantly. In particular:

- machine learning enables sophisticated and malicious attacks with the ability to learn and adapt to compromise systems with minimal chances of detection;
- interconnected devices, sensors and systems (the Internet of Things) embedded in smart cities and smart industries create a new target for malicious actors to compromise critical infrastructure or services guaranteeing public and social well-being;
- distributed ledger technologies continue to be attractive for criminal attacks, which not only result in criminal profits, but cause severe reputational damage to the victims and undermine confidence in the financial sector as a whole;
- with a growing reliance on cloud computing and related systems and data services, the number of attacks targeting vulnerabilities in these technologies increases as well;
- quantum computing raises questions regarding the security of modern cryptography and encryption methods.

In this regard, we welcome the European Commission's decision to develop a new proposal on CIP and conduct a review of the NIS Directive to adjust both legal instruments to new threats and risks.

To support this process, we are pleased to share the following suggestions to strengthen the CIP policy framework in the EU. In particular, we recommend actions for:

1. <u>Enhancing critical infrastructure cybersecurity through</u>:
   1.1. A government-industry supply-chain-security task force to identify best practices, guidelines and lessons learned for secure technology procurement, and evaluation of ICT suppliers' trustworthiness and integrity;
   1.2. Transparent vulnerability management programs to ensure the integrity of CI by ensuring operators can fix vulnerabilities before they are exploited by hostile actors; and
   1.3. Private-to-government (including government-to-government and private-to-private) threat information sharing about cybersecurity threats, vulnerabilities, and incidents, including with affected parties and companies capable of developing means to develop remediation plans against attacks. The information sharing should be voluntary, with legal protections for vendors, operators and companies against legal liability or regulatory consequences.
2. <u>Achieving full harmonization in the implementation of the CIP policy framework across EU Member States through:</u>
   2.1. Creating common data hubs/portals for competent authorities and industry with mapping of national security measures, definition, incident notification and incident reporting procedures;
   2.2. Developing thresholds, requirements and templates for incident notification and incident reporting – harmonized across Member States; and
   2.3. Achieving synchronization of the NIS Directive and ECI Directive in terms of security requirements for CI operators, vendors and competent authorities.

kaspersky

www.kaspersky.com
www.securelist.com

Enhancing critical infrastructure cybersecurity

One of the vectors for a cyberattack is through the supply chain – compromising the integrity of critical hardware and software that could undermine or disrupt CI operations. Supply chain attacks that occur when vulnerabilities in third suppliers' components or systems are exploited remain one of the most difficult to prevent. Europol reports[1] that supply chain attacks are becoming more complex, with compromised fourth or even fifth-party suppliers exploited in multi-tier supply chains.

As an example, we at Kaspersky discovered and then shared details of an attack on a large supply chain operation in 2019[2] – a server for a live software update tool for users of ASUS products had been compromised and an estimated 500 000 Windows machines received a compromised file that effectively acted as a backdoor to the devices for the attackers. The malicious file was signed with legitimate ASUS digital certificates to make it appear to be an authentic software update from ASUS.

This proves how critical the assessment frameworks for trustworthiness of third suppliers are. These assessment frameworks should be developed together with industry, including private companies, to help CI operators manage their supply chains and, therefore, ensure cyber-resilience and cybersecurity of their networks. For this, we see the value in launching Task Forces to enhance a synergy between different actors and especially between traditional industry sectors and newly created companies ('newcomers' on the market) that are all a part of the European and/or global supply chains. One of the challenges for ensuring the security and integrity of ICT supply chains is to incentivize new actors on the market to implement strong security controls to the architecture, design and testing of their products and services. Altogether under the guidance and with the close participation of relevant competent authorities, participants of such Task Forces would be able to exchange information and best practices as well as particular use cases on incident response and risk management.

What is more, we believe that not only technical aspects should be within the scope while measuring trust in a supplier's product. The highest level of assurance cannot be achieved by simply inspecting technical aspects of this product. Broader environment-related, management and organizational culture issues need to be addressed to measure user trust in software. These non-technical aspects are:

- Transparent communication over management-related and organizational processes for software development confirmed through an audit or certification, either by an independent third party or through self-attestation, depending on your organization's need for independent validation;
- Transparent reporting of the company's practices relating to data management practices of their software products, updates and operational connections and interactions back to the developing organization or to a service provider;
- The ability to assess the developing organization's internal development and maintenance processes. Software must be managed carefully with change control mechanisms that only allow authorized parties to modify the code and that enables changes to be tracked.

These aspects have been shared with the Industrial Internet Consortium and published in its recent White Paper on best practices for software trustworthiness[3].

One of the common methods for supply chain attacks is exploiting vulnerabilities in networks and systems that are a part of CI. This indicates the importance of vulnerability management programs as a part of supply chain management. This is necessary for developing processes inside the critical infrastructure operator in case there is a vulnerability found by an external researcher or company and the operator needs to know what to do to fix the issue timely. Vulnerability management programs – established in a transparent manner – indicate the maturity of CI operators to identify, remediate and publicly disclose, where needed, vulnerabilities in their systems and third party components as well as help set expectations while coordinating efforts with external companies to develop remediation plans.

---

[1] Europol IOCTA 2019 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

[2] ShadowHammer: Malicious updates for ASUS updates https://www.kaspersky.com/blog/shadow-hammer-teaser/26149/

[3] Software Trustworthiness Best Practices, Industrial Internet Consortium, March 2020 https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf

It is necessary to admit that as in any computing system, vulnerabilities in industrial components are inevitable. Each year, the Kaspersky Industrial Control Systems Cyber Emergency Response Team, (Kaspersky ICS CERT[4]), finds no less than 60 new vulnerabilities in industrial Internet of Things (IIoT) components and industrial control systems, potentially affecting hundreds and thousands of ICS or IIoT products. If undetected, these weaknesses can lead to system failure or give malware access to the product's management and critical manufacturing data, as mentioned above. One of the issues here as well is the lack of the exchange of threat information between CI operators, vendors, CERTs/CSIRTs and competent authorities. Usually CI operators, vendors and companies tend to keep silent due to potential reputational risks or risk of punishment. But when the CI operator is ready to share the information about the vulnerability found, then comes the question of how to do so in a confidential, secure and trusted manner? To whom is it necessary to pass this critical information to avoid the malicious use by criminal actors? For these reasons, we believe in the necessity of enhanced threat sharing processes between CI operators, vendors and competent authorities. These processes should be transparent and publicly communicated to CI operators in order to clarify all aspects, including contact points, communication channels, etc.

Achieving full harmonization in the implementation of the CIP policy framework across EU Member States to support the digital single market

As a company with strong digital footprint, we operate in 11 Member States and notice diverse national requirements on incident notification and incident reporting as well as different definitions and approaches to CIP (e.g., some Member States have designated multiple CSIRTs (not just one), and there is a lack of clarity to whom to report an incident in case it covers multiple sectors as well).

For these reasons, EU-created publicly available portals with mapping on national security measures, designated competent authorities and their contacts, detailed the procedures that would significantly help CI operators and companies react timely in the event of an ICT incident.

Harmonization under the guidance of the EU to develop uniform thresholds, requirements and templates for incident notification and incident reporting would also ease the process for CI operators and incentivize their responsible behavior, which would contribute to greater cyber-resilience in the end.

We also believe in the value of providing clarity on how the NIS Directive and ECI Directive work together and to which sectors and CI operators they should be applied. It may be valuable to consider transforming both Directives into regulations for enhancing harmonization of measures adopted across Member States.

Contact
For more information, or to discuss the contents of this submission in more detail, please contact Anastasiya Kazakova, Public Affairs Manager (+7 968 648 60 05, Anastasiya.Kazakova@kaspersky.com).

[4] https://ics-cert.kaspersky.com/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/#_Toc19618324