ENISA's contribution to the Critical Information Infrastructure protection (CIIP)

Workshop organised by the Working Group on Digital Union, ITRE, European Parliament
MAY 2017

www.enisa.europa.eu

European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice
Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Table of Contents

Introduction

This paper has been prepared to support the discussion at the workshop organised by the Working Group on Digital Union of the Committee on Industry, Research and Energy, the European Parliament. The workshop was held on 4 May 2017. Topics discussed at the workshop focused on the European Critical Information Infrastructures Protection (CIIP).

Due to the time allowed for contributions at the workshop, this paper only partially outlines matters associated with CIIP.

1. Status

The European ICT Industry is one of the most advanced in the world. Making the EU's single market fit for the digital age could contribute €415 billion per year to European economy and create new jobs.

The pervasiveness of high-speed connectivity and the richness and quality of online services in the European Union are among the best globally.

Such advantages have considerably increased the dependability of European citizens on ICT services. These two elements, quality of services and customer base, make this industry particularly appealing to global business. What if this important piece of the global economy becomes a target? And is Europe prepared?

Computer security attacks are increasingly used to perform industrial espionage, lead disinformation campaigns, manipulate stock markets, leak sensitive information, copy/change customer data, or sabotage critical infrastructure.

The protection of critical infrastructure was first put on the EU agenda in June 2004, when the European Council asked for the preparation of an overall strategy. At that time, the main concern was the protection against terrorist attacks.

Identification of critical information infrastructure is the first step in the process to secure and protect the availability of critical assets. Several Member States have launched different initiatives regarding this topic while others are starting now to develop their own approaches.

Experience shows that purely national or regional approaches to tackle the security and resilience challenges are not enough.

Now, with the adoption of the Network and Information Security (NIS) Directive in 2016, companies working in critical sectors will be required to report major incidents to national authorities and to adopt risk management practices. This directive also introduces a new term “essential services providers”. Those providers include sectors such as energy and water, banking and financial market infrastructures, healthcare, transport, and digital infrastructures. In addition, the NIS Directive introduces a term “digital services providers”. Since more and more providers of critical infrastructure relay on cloud services, ENISA is looking into relationship between these two providers

In the context of the NIS Directive, EU Agency for Network and Information Security (ENISA) has been assigned with a role to support the development of the baseline requirements for identification, incident reporting schemes and minimum security measures for the essential services providers. Based on previous experience of the Agency (mandatory incident reporting in telecom sector required under the Telecom Package of 2009), ENISA is already providing support to the European Commission in developing the implementing acts for such schemes and measures.

The NIS Directive is implemented through two governing bodies, namely the Co-operation Group and the CSIRTs network. The European Commission is the secretariat for the first body, dealing with strategic and policy matters. While ENISA is the secretariat of the second body, dealing with technical and operational matters among CSIRTs. Both bodies will strongly co-operate to provide a consistent and effective approach to CIIP.

The swift and effective implementation of the NIS Directive will be key in view of the increasing digitalisation of economic and societal life (also taking into account the cloud, the Internet of things, and machine-to-machine communication), growing cross-border interconnection and the fast-evolving cyber-threat landscape. In this context, the EU needs to prepare itself for the possibility of a large-scale cyber crisis, including for instance simultaneous attacks on critical information systems in several Member States.

Cyber security is one of those subjects that never remain static. Every month new issues arise to challenge the digital ecosystem which continues to grow. For example, the use of many small Internet of Things (IoT) devices in the cyber-attack has been experienced in September 2016 ("Mirai" malware) and on several other occasions since then. It is important to note that IoT are not covered by the NIS Directive. Having seen cyber-attacks that have taken place, the question is what is Europe doing to address these challenges. The other issue that Europe needs to review is the question of software liability, and in particular in the context of next generation of smart devices and artificial intelligence, which is highly dependent on software. These devices will form an integral part of our critical infrastructures, smart X, and industry 4.0.

It should be also noted that in 2017 the European Commission is planning to submit for consideration a cooperation blueprint to handle large-scale cyber incidents on the EU level .

The experience shows that there is a need for the EU cyber crisis cooperation procedures and a need to develop an EU cyber crisis cooperation plan.

Crisis management is addressed by conducting regular CIIP-related exercises. Most sector-specific and cross-sectorial exercises are being conducted in the financial, energy and the telecommunications sector. Other important sectors are public administrations, transport and logistics, and healthcare.

The cooperation at the European Union level to mitigate a potential crisis, has developed significantly since ENISA has launched series of the pan European exercises mainly tackling the Critical Information Infrastructure Protection. The first table top exercise was carried out in 2010. Now these exercises are carried out once in two years and have reached around 850 experts participating online to ensure business continuity and, ultimately, to safeguard the European Digital Single Market.

2. Challenges

Recognising IT security as the backbone of the today's society, the following challenges should be considered when discussing the CIIP:

- Complex networks and services
- Different levels of capabilities of stakeholders
- Asymmetric threats allowing remote attacks
- Increasing organised cybercrime and industrial espionage

Tools to reduce the gap include:

- Capacity building / Hands on / Training
- Policy implementation
- Recommendations / Good Practices / Standardisation

Cyber security incidents affecting CIIs are considered nowadays global risks that can have "significant negative impact for several countries or industries within the next 10 years" (source: World Economic Forum, The Global Risks Report 2016 - 11th Edition, pg. 11.).

As more and more businesses/industries benefit from the advantages of information technology, by witnessing a tighter cyber-physical systems integration, developed under concept such as Internet of Things, cyber-attacks or incidents affecting those infrastructures, including critical infrastructures are increasing dramatically, resulting in a new chapter in information security.

In August 2016 ENISA has published a study on the cost of incidents affecting CIIs . In this study it was concluded that Finance, ICT and Energy sectors appear to have the highest incident costs. The most common attack types for Financial sector and ICTs appear to be DoS/DDoS and malicious insiders, with the latter affecting the Public Administration sector as well. It is very important to highlight that these two types on their own, collectively constitute approximately half the annualized cost of all cybercrime.

Also, in the above mentioned study ENISA concluded that the most expensive attacks are considered to be insider threats, followed by DDoS and web based attacks. In terms of country loss, the values provided reach up to 1.6% of GDP in some EU countries. Other resources mention figures like 425,000 to 20 million euro per company per year (Germany).

3. Conclusion

Society and our citizens are increasingly dependent on the proper functioning of the CIIP. There is a need to ensure that operators are prepared and ready to withstand cyber-attacks. ENISA is supporting this challenge and with the continuous support of the European Parliament, and ITRE in particular, will continue to address the ever increasing complexity of these attacks.

In conclusion, the following take away points should be considered:

- **Protecting Cyber sovereignty in Europe.** Cyber sovereignty is the basis of our society's digital self-determination. The European cyber security market is dependent on a number of infrastructures that include software and hardware. Europe is not leading in either of these markets. A consequence of this situation is that Europe is effectively dependent on third countries for the manufacture and supply of cyber services and systems.

- **Updated EU governance structures with clear roles and responsibilities to address global cyber challenges:** While traditionally Member States addressed cyber security in a national context there is an increasing need to address cyber security in an EU context. In the last few years, Europe has witnessed the growth in the Digital Single Market, the interconnected Energy market and the single trading area. Other sectors such as the banking, the finance markets and the Aviation have become increasingly integrated across Europe.

- **NIS Directive and next steps:** a compromise reached over NIS Directive brings a necessity for further work to be done, in particular in the areas of IoT and crisis management at the EU level. A common understanding of criteria and approach across the EU is crucial to address the associated challenges.

- **Paradigm shift in liability and ownership of products** controlled by software and the liability questions arising from the use of software. At an EU level, there is a need for a discussion to address this paradigm shift. ENISA supports a discussion for setting a regulatory framework for this issue.

- **Harmonisation of Cyber Products, Services and Skills.** The existence of EU cyber security related standards presents good opportunities for EU manufacturers and service providers to serve the pan EU marketplace as opposed to addressing individual member state or company specific requirements.

4. Further reading

- Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, published on 16 February 2017

  https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

- The cost of incidents affecting CIIs, published on 5 August 2017

  https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis

- Stocktaking, Analysis and Recommendations on the protection of CIIs, published on 21 January 2016

  https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

- CIIP Governance in the EU (Annex) , published on 21 January 2016

  https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/ciip-governance-in-the-eu-annex

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu