EAI Endorsed Transactions
on Security and Safety

Research Article EAI.EU

NIS directive: The case of Greece

Leandros Maglaras[12,*], George Drivas[2], Kleanthis Noou[2], Stylianos Rallis[2]

[1]Cyber Security Centre, De Montfort University, Leicester, LE1 9BH, UK
[2]General Secretariat of Digital Policy, Ministry of Digital Policy Telecommunications and Media, Athens, Greece

Abstract

The directive on security of network and information systems (NIS directive) is one of the latest steps that the EU has taken in order to strengthen security of its systems. The directive describes specific steps that each member state should follow. Greece that has recently published its cyber security strategy is moving towards the implementation of the NIS directive. The road ahead is long and a cooperation in both technical and strategic level is needed. This article describes the roadmap of the implementation of the NIS directive in Greece, the milestones, the problems and possible solutions.

Keywords: Information Security, European Directive

Received on 22 February 2018; accepted on 24 February 2018; published on 15 May 2018

doi:10.4108/eai.15-5-2018.154769

1. Introduction

During the winter of 2014, fear spread among 70 million Americans accross the North East due to lack of power in sub-zero temperatures conditions. Lights went out, banks lost its operations, hospitals lost power, air traffic was shut down and internet and communications were lost, all due to a cyber attack [1]. A group of hacktivists decided to spread panic by attacking critical infrastructure. The attack revealed the importance of energy to our modern smart society. Energy generation and distribution is getting smarter, no more stand-alone units for the massive network of devices, this is the digital age. Smart grid means more data, new threats, emerging risks and countless cyber-attacks. Comfort and lifestyles of citizens are at risk while financial institutions, communications and hospitals are becoming more vulnerable to external and internal attacks. Critical infrastructures are becoming interdependent [2]; a failure in one, may lead to an uncontrollable chain reaction. The European Union's security and economic robustness must be protected, therefore energy cyber security has become a strategic concern. New energy cyber security solutions, along with energy device performance databases are needed to continually mitigate and counter vulnerabilities. If we are connected to the grid, everyone is connected to us; therefore we must know exactly how vulnerable energy assets are.

Malware remain hidden until activated or detected, and the harmful effects persist long after an attack was launched [3]. These effects present threats to safety and security, especially if they are located in critical national infrastructure. Cyber attacks upon critical infrastructure such as public water supplies, the power grid or air traffic control have potential to threaten civilian life and security. Member States now work to detect attacks and minimise their impact on civilians keeping critical infrastructure operational.

Cyber attacks could contribute towards the collapse of a state if they initiate or prolong the failure of critical national infrastructure. Nations are becoming reliant on the cyber domain to provide services that keep a nation running: power grids, water supplies, communications, transportation and finance are all increasingly becoming cyber dependant [4]. Cyber warfare which causes blackouts, cuts off supplies to safe drinking water, makes travelling dangerous or destabilises a national economy is clearly a threat to the stability of a nation and is therefore a threat to international peace and security. Despite the apparent risk to critical infrastructure, the security of ICS is not considered a significant investment area. Authors in [5] argue that the costs involved in ICS security are prohibitive, especially within critical systems, when the perceived risks to an organisation or infrastructure cannot be adequately quantified and a business case not satisfactorily articulated. This often leads to an underdeveloped incident response capability in the deployed operational ICS. Although a lot of research studies were conducted recently, introducing new methods and frameworks that can increase security level of CIs [6, 7], what is missing is the legal framework that can help member states to impose security measures to providers of essential services and make the notification of incidents mandatory.

[*]Corresponding author. Email: leandros.maglaras@dmu.ac.uk

Unavailability of critical infrastructure (e.g., electrical power, transportation) can have economic impact far beyond the systems sustaining direct and physical damage. These effects could negatively impact the local, regional, national, or possibly global economy. European Union in the upcoming years is expected to face great challenges especially in the area of security and safety. In order to increase the level of security of its critical infrastructures and thus the trust and safety of European citizens, EU has published several directives, during the last couple of years, that describe the legal measures that each member state should take towards this direction. NIS directive encourages the cooperation of the member states both in strategic and operational level and it grants additional rights and responsibilities to the competent authority that each member state should establish. Providers of essential services should take appropriate security measures and should notify critical incidents to the relevant authority.

In Greece the National Cyber Security Authority (NCSA) was established in the newly formed Ministry of Digital Policy Telecommunications and Media following a Presidential Degree. NCSA is responsible for coordinating all competent Ministries and independent authorities of Greece, in order to take all necessary steps towards a secure Greek Cyber space. In close cooperation with the National CERT, NCSA will have to handle all critical incidents, issue binding instructions to the operators of essential services and impose penalties when necessary. For the NIS directive to take effect in Greece, a lot of mandatory steps need to be completed, e.g. indentification of essential services, determination of significant disruptive effects, publishing of the National Cyber Security Strategy, establishment of a national incident notification procedure, legistation regarding rules and penalties etc.

2. Real-world attacks in Critical Infrastructures (CIs)

In December 2016, a power blackout in Ukraine's capital Kiev was caused by a cyber attack and preliminary findings indicated that workstations and SCADA systems, linked to the 330 kilowatt sub-station "North", were influenced by external sources outside normal parameters [8]. The analysis of the impact of symptoms on the initial data of these systems indicates a premeditated and multi-level invasion and cyber experts are still trying to compile a chronology of events, create the list of compromised accounts, and determine the penetration point, while tracing computers potentially infected with malware in sleep mode.

The STUXNET worm infection [9] perfectly represents the frailty of the regulatory systems devoted to control critical infrastructures. First isolated in mid-June 2010, STUXNET was a computer virus specifically designed for attacking Windows based industrial computers and taking control of Programmable Logic Controller (PLCs), influencing the behaviour of remote actuators and leading to instability phenomena or even worse. The lesson the CIIP (Critical Information Infrastructure Protection) community has learned from the spread of the STUXNET worm is that, in order to effectively react to a specific low level menace, there is the need to consider both the global and the local perspectives. In fact, besides obtaining a wider perspective on the state of the System of Systems, there is the need to increase the intelligence of equipments and devices that are used to influence the behaviour of the system, such as RTUs, valves, etc.

Moreover, as emphasised by several episodes [10], another effective way to paralyse a CI via cyber attack is to saturate the bandwidth of the carrier used for the communication (this was, for example, the way in which the SLAMMER worm operated in 2003 to affect the SCADA of two United States (US) utilities and a nuclear power plant). Indeed, as emphasised also by the ANSI/ISA.99 (American National Standards Institute/ International Society of Automation), availability is the most crucial attribute of information security. The lack of timely information to/from the field may cause dramatic consequences because the field is unable to receive the adequate command, hence even trivial episodes may provoke dramatic impact, as shown by the US black-out.

Evaluating the Mariposa botnet infection that took place in an ICS organization, the US Department of Homeland Security [11] found that the infection initiated from an infected USB drive that was attached to a corporate computer for downloading presentation materials. From this initial point of infection the visus managed to spread to over 100 hosts of the orgnization, revealing for one more time that human factor is one of the most vulnerable aspects of cyber security[12] incidents.

The security of CI communications is becoming more complicated because the decision has been taken to link the SCADA networks with IT networks to allow better and faster communications. But these new features have increased the threats and risks on SCADA communications. A number of EU (European Union) projects such as the FP6 SAFEGUARD and FP7 CRUTIAL (CRitical UTility InfrastructurAL Resilience) have explored the technical feasibility to improve cyber security of CIs system by improving the smartness of the field devices.

3. NIS Directive Obligations and Deadlines

NIS directive [13] has certain obligations that each member state should follow, each one with a specific deadline. The main obligations that are derived from the

NIS directive for Greece and for each member state in chronological order are stated below:

1. By 9 February 2017 Member States shall ensure appropriate representation in the Cooperation Group and the CSIRT network (Article 24)

2. Each Member State shall establish a national strategy for the security of network and information systems setting out the strategic objectives and appropriate policy and regulatory measures aimed at achieving and maintaining a high level of network and information security. Member States shall notify their national network and information security strategy to the Commission within three months of its adoption (Article 7)

3. Each Member State shall designate one or more national competent authorities for the security of network and information systems (”the competent authority”). Member States may delegate this role to an existing authority or authorities. Each Member State shall designate a national single point of contact for the security of network and information systems (”single point of contact”). Member States may delegate this role to an existing authority. Each Member State shall without delay notify the Commission of the designation of the competent authority and of the single contact point, their tasks and any subsequent amendment. Each Member State shall make public the definition of the competent authority and the single contact point. (Article 8)

4. Each Member State shall designate one or more CSIRTs which comply with the requirements referred to in Annex I, point 1, and are responsible for the handling of risks and events based on a clearly defined procedure. Member States shall inform the Commission of the mandate as well as of the main elements of the incident handling procedure from their CSIRTs (Article 9)

5. Member States shall lay down the rules and penalties applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall notify those rules and measures to the Commission by 9 May 2018 and shall inform it without delay of any subsequent amendment (Article 21)

6. By 9 August 2018, and thereafter each year, the single contact point shall submit to the Cooperation Group a summary report on the notifications received, including the number of notifications and the nature of the notified incidents and the measures taken in accordance with Article 14 (3) and (5) and Article 16 (3) and (6) (Article 10)

7. By 9 November 2018, Member States shall identify key service providers established in their territory (Article 5)

As it is obvious from the aforementioned list, the obligations that are derived from the NIS directive for each member state are demanding and time constrained. Greece and each of the member states need to take quick actions and work closely with all major players in the field of cyber security, e.g. Ministries, authorities, providers of essential services, CSIRTs etc.

4. Current State in Greece and the Way Forward

Having to cope with the obligations of the NIS directive and to meet strict deadlines, Greece has taken some steps forward during 2017. With the Presidential Degree of 82/2017 a National Cyber Security Authority (NCSA) was established along with the Single Point of Contact, both of which operate in the newly formed General Secretary of Digital Policy, Ministry of Digital Policy, Telecommunications and Media. Also a National Cyber Security Strategy that sets out the strategic objectives, priorities and appropriate policy and regulatory measures to ensure a high level of protection of digital systems at national level was published in September of 2017. From late 2017, NCSA is representing Greece in the Cooperation Group and the National CERT in the CSIRT network of the EU.

These important actions cover fully items 1-3 and partially item 4, of the obligations stated in the previous section. What remains for item 4 to be fully covered is the setting up of an incident handling procedure. This action along with the actions needed to cover items 5-7, especially for item 5 where the deadline is the 9th of May, make necessary the acceleration of the implementation of the NIS into full operational mode.

Along with the obligations that directly arise out of the NIS directive, Greece and all other member states should also take further actions for enhancing cyber security. One important action is the enhancement of digital skills and the development of a strong public and private security culture, exploiting the potential of the academic community and public and private sector actors. Continuous adaptation of the national institutional framework to the new technological requirements, always in line with the European regulations on data protection and security will help Greece fight cyber crime. In this content the General Data Protection Regulation (GDPR) - General Data Protection Regulation (Regulation (EU) 2016/679 of the

European Parliament and of the Council of 27 April 2016, concerns the development of a single legislative framework for the processing personal data in the Member States of the European Union [14].

Investing in innovation, research and development on security issues through the promotion of public-private partnerships aiming at cooperation and the mutual exchange of know-how is also an important step towards a safe and secure cyber space. This initiative includes the exploitation of all available financial tools and the design of new specialized development programs to enhance security and privacy. Conducting frequent cyber security exercises is also an efficient tool [15–17]. In 2018, European countries and the EU Agency for Network and Information Security (ENISA) will organise the 5th pan European cyber crisis exercise and Greece is going to participate. During this events large-scale cybersecurity incidents that escalate to EU-wide cyber crises are simulated which make member states face complex business continuity and crisis management situations. Finally the cooperation at European and international level through the representation of the country in all decision-making bodies and joint working groups with the aim of continuously improving Greece's capabilities to protect against cyber attacks, with particular emphasis on critical infrastructure is mandatory.

5. Discussion

NIS aims at boosting the overall level of cybersecurity in the EU, by securing critical infrastructures of each member state. CIs rely on Industrial Control Systems along with tradiniotal IT systems. ICS face the same attack vectors as IT systems [7]. Connectivity to the Internet allows reconnaissance activity around an ICS as well as an opportunity or malware delivery. Spear phishing is as much of a threat to ICS as to general IT networks. Similarly, controls within a corporate network, or lack thereof, provide an environment in which malware can propagate and extend its reach within an organisation. However, the range of attack vectors grows within an ICS as vendor engineers access control equipment either remotely or locally, with little control over the security of their devices or network connectivity.

In all of these scenarios, traditional IT security mechanisms are both appropriate and effective means to defend the boundaries of an organisation. Firewall architectures, email scanning, DPI, VPNs, HIDS, NIDS [18, 19] are all established ways by which an organisation can reduce the opportunities for the ingress of malicious software into their environments. As a complimentary measure, the practice of locking-down unused ports, USB devices, use of access controls through corporate directories and the enforcement of least-privilege access all reduce the insider threat.

In order for an enterprise architecture to be properly defined, the assets managed by the business must be identified. Device scanning can expose the operation to unwarranted risk as it is common for devices to crash when overwhelmed with specific messages. A full audit of all devices must be undertaken when assessing an ICSs security, as must the physical protection of those devices if deployed outside of the organisations main operating facilities.

Furthermore with the use of control software that constantly improves power consumption and optimize costs, the future smart grid can improve the security and reliability of the existing power grid [20]. Smart Grid cannot be widely deployed without considering the security requirements such as authentication, integrity, non-repudiation, access control, and privacy. Recently, researchers in the field of computer security have proposed several privacy-preserving schemes for Smart Grid communications [21] while on the same time EU has published GDPR regulation that imposes a series of new obligations on controllers of data, which are based on the principle of transparency in data collection, processing and keeping.

National Cyber Security Authority of Greece needs to be able to have a general overview of the current situation in terms of hardware, software and security procedures that CIs. In order to achieve this a creation of an IT inventory along with a security inventory of all CIs that reside inside Greece, along with all critical operational centers of the public sector and governmental clouds [22] is an essential first step. The information that is going to be gathered during the creation of the inventory can be used to reveal interdependencies between different systems, similar configurations or technology that come along with common vulnerabilities, and possible lack of basic security measures that need to be applied immediately [23]. During this procedure a network with security officers of CIs will be created which can be used in an ad hoc mode in order to create expert working groups that can deal with specific situations.

6. Conclusions

As modern smart societies face new challenges in the area of cyber security, EU is struggling to strengthen Critical Infrastructures by publishing new directives. The NIS directive that presents legal measures that each member state need to take in order to boost the overall level of cybersecurity in the EU will take effect from the 9th of May of 2018. The common objective is to "Shield Europe from external threats" and to provide a secure digital environment for all European citizens. The current article describes the obligations that are derived from the NIS directive, real world attacks to CIs and current and future steps that Greece is taking towards a safe and secure cyber space.

References

[1] Riley Walters. Cyber attacks on us companies in 2014. *The Heritage Foundation*, 4289:1–5, 2014.

[2] Tiago Cruz, Luis Rosa, Jorge Proença, Leandros Maglaras, Matthieu Aubigny, Leonid Lev, Jianmin Jiang, and Paulo Simões. A cybersecurity detection framework for supervisory control and data acquisition systems. *IEEE Transactions on Industrial Informatics*, 12(6):2236–2246, 2016.

[3] Eric D Knapp and Joel Thomas Langill. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

[4] L. A. Maglaras, K. Kim, H. Janicke, M. A. Ferrag, S. Rallis, P. Fragkou, A. Maglaras, and T. J. Cruz. Cyber security of critical infrastructures. *ICT Express*, 2018.

[5] Martin Naedele. Addressing IT security for critical control systems. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference*, pages 115–115. IEEE, 2007.

[6] Allan Cook, Helge Janicke, Richard Smith, and Leandros Maglaras. The industrial control system cyber defence triage process. *Computers & Security*, 70:467–481, 2017.

[7] Allan Cook, Helge Janicke, Leandros Maglaras, and Richard Smith. An assessment of the application of it security mechanisms to industrial control systems. *International Journal of Internet Technology and Secured Transactions*, 7(2):144–174, 2017.

[8] Pavel Polityuk, Oleg Vukmanovic, and Stephen Jewkes. Ukraine's power outage was a cyber attack: Ukrenergo, 2017.

[9] Robert McMillan. Siemens: Stuxnet worm hit industrial systems. *Computerworld*, 14, 2010.

[10] Sandro Bologna and Roberto Setola. The need to improve local self-awareness in CIP/CIIP. In *Critical Infrastructure Protection, First IEEE International Workshop on*, pages 6–pp. IEEE, 2005.

[11] Prosenjit Sinha, Amine Boukhtouta, Victor Heber Belarde, and Mourad Debbabi. Insights from the analysis of the mariposa botnet. In *Risks and Security of Internet and Systems (CRiSIS), 2010 Fifth International Conference on*, pages 1–9. IEEE, 2010.

[12] Mark Evans, Leandros A Maglaras, Ying He, and Helge Janicke. Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, 9(17):4667–4679, 2016.

[13] George Christou. The eu's approach to cybersecurity. 2017.

[14] WS Blackmer. Gdpr: Getting ready for the new eu general data protection regulation. *Information Law Group, InfoLawGroup LLP, Retrieved*, 22(08):2016, 2016.

[15] Samuel Chapman, Richard Smith, Leandros Maglaras, and Helge Janicke. Can a network attack be simulated in an emulated environment for network security training? *Journal of Sensor and Actuator Networks*, 6(3):16, 2017.

[16] Allan Cook, Richard G Smith, Leandros Maglaras, and Helge Janicke. Scips: Using experiential learning to raise cyber situational awareness in industrial control system. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 7(2):1–15, 2017.

[17] Bil Hallaq, Andrew Nicholson, Richard Smith, Leandros Maglaras, Helge Janicke, and Kevin Jones. Cyran: A hybrid cyber range for testing. *Security Solutions and Applied Cryptography in Smart Grid Communications*, page 226, 2016.

[18] Leandros A Maglaras and Jianmin Jiang. OCSVM model combined with K-means recursive clustering for intrusion detection in SCADA systems. In *Heterogeneous Networking for Quality, Reliability, Security and Robustness (QShine), 2014 10th International Conference on*, pages 133–134. IEEE, 2014.

[19] Zibusiso Dewa and Leandros A Maglaras. Data mining and intrusion detection systems. *International Journal of Advanced Computer Science and Applications,*, 7(1):62–71, 2016.

[20] Rongxing Lu. *Privacy-enhancing aggregation techniques for smart grid communications*. Springer, 2016.

[21] Mohamed Amine Ferrag, Leandros A Maglaras, Helge Janicke, Jianmin Jiang, and Lei Shu. A systematic review of data protection and privacy preservation schemes for smart grid communications. *Sustainable Cities and Society*, 2018.

[22] Allan Cook, Michael Robinson, Mohamed Amine Ferrag, Leandros A Maglaras, Ying He, Kevin Jones, and Helge Janicke. Internet of cloud: Security and privacy issues. *arXiv preprint arXiv:1711.00525*, 2017.

[23] Andy Wood, Ying He, Leandros A Maglaras, and Helge Janicke. A security architectural pattern for risk management of industry control systems within critical national infrastructure. *International Journal of Critical Infrastructures*, 13(2-3):113–132, 2017.