ATLANTIS PRESS
Advances in Economics, Business and Management Research, volume 108
5th IPMA SENET Project Management Conference (SENET 2019)

Risk Management in Critical Information Infrastructures

Dejan Vuletić
University of Defence
Belgrade, Serbia
dejan.vuletic@mod.gov.rs

Jovanka Šaranović
University of Defence
Belgrade, Serbia
jovanka.saranovic@mod.gov.rs

Ivan Vulić
University of Defence
Belgrade, Serbia
ivan.vulic@mod.gov.rs

***Abstract* — We live in a time of great dependence on increasingly networked information and communication technologies, which besides numerous advantages, also have certain negative aspects. The paper gives a brief description and importance of critical information infrastructures and their vulnerabilities and protection. In the final part of the work are proposed strategies for risk management in the critical information infrastructures (information systems).**

Keywords—Infrastructures, networking, protection, risk, management

I. INTRODUCTION

The high dependence of society on information and communication technologies (ICT), cross-border connectivity and interdependence of information infrastructures makes modern society very vulnerable. In the past, servers were isolated without access to the Internet. Today, as a result of the development of ICT and the necessity of increasing efficiency, these infrastructures are becoming increasingly automated and interconnected. Due to attacks, natural disasters or technical errors, the consequences for the endangered system can be very serious and reflect on the safety, economy and functioning of the society as a whole.

With the development of information and communication technology, new forms of social activities have emerged that affect every segment of people's lives. Information and communication technology has resulted in numerous advantages, but it also has certain dangers for national security, economic stability and other aspects of human life, which can be caused by the threat of critical information infrastructures.

II. INTERNET OF THINGS

Information transmitted, processed, collected or protected by information and communication technology serves as a basis for making optimal decisions at all levels of decision making and contributes to the efficient use of the resources needed to make decisions. Information and communication technology enables access to vast numbers and sources of information. Information and communication technology provides a better understanding of the situation based on relevant information. Information is a key resource on which an organization's value is based.

An information society is one that is heavily used by information and communication technologies. Such societies and states are more vulnerable to possible attacks. This is especially characteristic of vital elements of society such as the defense system, the energy system and other information-dependent areas.

Information and communication technology has significantly increased the amount of information that is increasing enormously on a daily basis. The significant increase in the use of information and communication technologies has enabled numerous services for citizens and organizations, and has led to numerous changes in business and other segments of the functioning of society.

The Internet of Things (IoT) represents a large number of networked devices, mostly wireless technologies, in different environments (household, organization, city, etc.) and in various areas of social functioning (traffic, business, health care, etc.). The number of such connected devices is projected to increase globally in the next few years [1]. A large number of connected devices will provide numerous and new services that affect the quality of life of individuals and the functioning of different sectors of the organization, society and state [2]. In addition to its many benefits, IoT also poses a significant risk to the security of citizens and organizations, and of society as a whole[3].

With the increasing connectivity of many household devices, hacking into IoT networks could become a source of valuable intelligence for law enforcement investigations. For example, Cellebrite, the Israeli firm hired by the FBI to unlock the iPhone, is expanding its offerings to the Internet of Things [4].

Internet of Things allows objects to be observed and controlled remotely through existing network infrastructure. The IoT connects millions of everyday life items (street lighting, parking, street signage, hospital equipment, home devices, production lines, agricultural machinery, etc.) that are equipped with sensors, processors and communication devices. all with the aim of exchanging important data over computer networks (usually the Internet) and responding as needed in the most optimal way. It is a new concept of smart automation and smart monitoring using the Internet as a medium of communication.

IoT is most commonly associated with so-called smart office buildings and homes (adjusting the brightness, optimal room temperatures, smart TVs, various home appliances, using voice controls, etc.). IoT also includes certain devices that record an individual's parameters (pulse, blood pressure, body temperature, habits, etc.). IoT are becoming cheaper and more accessible to a large number of individuals and organizations. They are characterized by the ability to gather a large amount of information as well as the ability to interact and exchange data. The increasing number of connected devices makes the life of an individual easier, society more efficient and more organized, but at the same time more vulnerable in terms of security which reequires significant investment in their protection.

III. Vulnerabilities of Critical Information Infrastructures

Critical infrastructure means resources in the territory of certain countries whose disability or destruction can weaken national security, economic stability and affect other aspects of the normal functioning of those countries. Critical information infrastructures include services, computer networks and other systems based on ICT, which are important for the functioning of a particular country (economically, from the point of view of security, etc.). Critical information infrastructures are a narrower concept than critical infrastructures, i.e. they represent their inseparable part. They can be in both the state and the private sector.

Information systems are a critical segment of human society. The economic sector, defense, security, energy, telecommunications, industrial production, finance and other dependencies on information systems operating on local, national or global scale. Social dependence on information systems increases the consequences of attacks, accidents and falls, and the importance of ensuring the viability of their protection. Greater connectivity of information resources results in greater vulnerability of information systems.

If the information system is regarded as a system in which the connection between the system elements is achieved by the exchange of information, that informational system of the unforeseen situation can inflict irreparable damage, primarily by interrupting the information flows. The increased sensitivity of information systems is one of the causes of an increased number of incidents, many of which remain unpublished for various reasons. However, users are increasingly aware of the risk of system vulnerability and price in case of loss of data. Sometimes the main preoccupation of users and those who build the information system was how to make the system work faster and more efficiently, while today the main preoccupation is how to make the system work safer.

Numerous statistics and results of the research indicate that there is an increasing number of attacks on information infrastructures. The UK National Cyber Security Centre (NCSC) released its 2018 annual review. The statistics indicate that, from 1 September 2017 to 31 August 2018, the NCSC handled 557 cyber incidents and removed 138.398 phishing sites [5]. New research highlights the threat that connected devices pose to critical infrastructure. Academics in Israel warned that it would be possible to hack internet-connected irrigation systems, turning these on remotely in order to drain a city’s water reserves. A group of researchers from Princeton University found that a malicious botnet of water heaters and air conditioners could be used to manipulate the demand for energy by as much as 1%, leading to a blackout. The Port of San Diego confirmed that some of its internal systems had been affected by a ransomware attack. According to a spokesperson, the incident did not impact shipping functions and is being investigated by the Federal Bureau of Investigation. The issue of cybersecurity for port operations had received significant attention since 2013 when Belgian and Dutch authorities uncovered a criminal hacking operation in Antwerp that was used to facilitate narcotics trafficking, and several governments are taking action to further safeguard critical infrastructures [6]. These scenarios illustrate the challenge of securing critical infrastructure, suggesting that if industrial control systems are sufficiently hardened, attackers will shift their focus to connected devices with weaker security standards [7].

Given the degree of dependence of the modern society on information and communication technologies and the increasing trend of dependency, it is necessary for all states to adopt appropriate regulations and set up specific bodies in order to effectively manage the risks in critical information infrastructures [8].

IV. Protection of Critical Information Infrastructures

Critical Infrastructure Protection (CIIP) is defined as a set of measures that is necessary to deter or prevent the attack or provide a response in case of an attack on critical infrastructure. Protection of critical information infrastructures represents programs and activities realized by owners, users, operators, scientific research institutions, governments, regulatory bodies in order to maintain the performance of critical information infrastructures in the event of cancellations, attacks or incidents and minimize the consequences and time of recovery [9].

A secure environment implies that resources are protected from both external and internal unauthorized access. These resources may be material (hardware) or non-material (data, information) [10]. Protection of critical infrastructures is a complex problem. It is very important to know who are perpetrators and what tools they use, the motives, the ways in which the goals are chosen, the legal regulations on the national and international level. In addition, the joint operation of the private and public sector, cooperation between criminal services, Internet service providers, system administrators, judicial authorities is necessary. In protecting critical information infrastructures, the emphasis is placed on proactive action. In the event that in addition to the measures taken, there must be a trained person or team who will collect all relevant information about the incident that can lead to the perpetrator and prosecution of the case.

Heterogeneity is very important from the aspect of preventing the exploitation of system weaknesses. Elasticity (ability to restore) and robustness of the system (in the event of an attack there is no degradation or decline of the entire system), redundancy (multiplication of key components and information), rapid recovery and reconstruction, segmentation (that certain parts are autonomous) and central management of information resources are also very important.

The only effective way to reduce the threat is to use security technology in conjunction with security rules that define employee procedures, as well as with appropriate education and training. The system must maintain key features such as confidentiality, integrity, availability and reliability of information transmission. A key feature of the ability to survive information systems is their ability to maintain basic services during an attack, a fall in the system or an accident. Despite the efforts of those dealing with security, no degree of system strengthening can ensure with certainty that the system will be absolutely safe.

V. RISK MANAGEMENT IN ICT

The risk is probability that a particular threat will occur and lead to harmful consequences [11]. In the traditional terminology of risk analysis, an information resource is an object or element that is sufficiently valuable to be protected. System resources can be physically (computers, network infrastructure elements, facilities in which the equipment is located) or software (application software, operating systems). [12].

Risk management is an essential tool in protecting the organization's resources. It is a process achieving a balance between the cost of protection and the desired system efficiency. In computer systems, risk management implies the ability to balance between the price in the application of the protection measures and the risks to which the systems are exposed. A key component in risk management is a risk assessment in identifying and prioritizing risks in line with its potential impact on the organization's mission. Equally important is the procedure for determining appropriate protection measures to mitigate potential risk effects [13, 14].

The risk management area is based on two decisions of the management of the organization. The first decision is the determination of the minimum significance of the event occurrence rate, i.e. the probability of their occurrence, so certain ones are ignored, and certain attention is given to a considerable amount of attention. The second decision is to determine the maximum acceptable losses. Above this threshold, certain steps (e.g. risk transfer) must be taken to reduce losses [15, 16].

According to Microsoft, the following risk management strategy is proposed [17]:

- Acceptance of risk. After analyzing threats, system vulnerabilities and available countermeasures, the risk is assumed. This measure is used when, at particular risk, a minor harmful effect or damage is less than the cost of protection.
- Risk mitigation involves the application of additional measures to reduce the risk and motivation of the attackers. For example, by increasing the price of an attack (limiting users to accessing parts of the system can significantly reduce the attacker's profit).
- Risk transfer involves a partial or complete transfer of risk by a maintenance contract, insurance in the event of damage to the insurance institution.
- Risk avoidance. Some system functions are temporarily abandoned or some of the system components. Risk avoidance is temporary and aware of the degradation of the system. This measure is used if there is no other more cost-effective and more effective measure available.

VI. CONCLUSION

As the number of connected devices grows exponentially and they become integrated into public utilities and smart cities, every modern society will have extreme vulnerabilities. The probability of losing lives in a cyberattack that either intentionally or inadvertently causes health, transportation, energy, or environmental catastrophe is rising. The ability to rely on the origin and accuracy of data will become increasingly important for the resilience of critical infrastructures.

Society is increasingly dependent on information and communication technology, and this trend continues, which will lead to its increased sensitivity. Therefore, the protection of critical information infrastructures is a social problem that will grow at high speed in the foreseeable future. The risk management process can not eliminate all risks and ensure the absolute security of critical information infrastructures. By applying certain measures, the risk can be reduced to a level that is acceptable to the organization.

REFERENCES

[1] The Internet of Things: opportunities and threats (conference report). The Royal Society, 2017, pp. 4-5, https://royalsociety.org/~/media/events/2017/10/tof-iot/iot-conference%20report-final.pdf

[2] Understanding Internet of Things, GSM Association, July 2014, p. 3. https://www.gsma.com/iot/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf

[3] Internet of Things Tutorial, p. 1-2, https://www.tutorialspoint.com/internet_of_things/internet_of_things_tutorial.pdf

[4] Cyber weapons proliferation, https://www.iiss.org/blogs/cyber-report/2018/07/cyber-report-6-to-12-july

[5] Countering cyber threats, https://www.iiss.org/blogs/cyber-report/2018/10/cyber-report-19-to-25-october

[6] Securing critical infrastructures, https://www.iiss.org/blogs/cyber-report/2018/10/cyber-report-28-september-to-4-october

[7] Critical infrastructure exploits, https://www.iiss.org/blogs/cyber-report/2018/08/cyber-report-17-to-23-august

[8] J. Haller, A.S.Merrell, J.M. Butkovic and J.B. Willke, Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Software Engineering Institute, Carnegie Mellon University, Pittsburg, 2010, p.1.

[9] G. Lewis, Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation, John Wiley & Sons Inc. Hoboken, New Jersey (USA), 2006, p.4.

[10] M. J. Kizza, Guide to Computer Network Security, Springer, London, 2009, pp. 45-46.

[11] R. Opplier, Security Technologies for the WWW (e-book), Artech House, Norwood, 2003, ch 15.

[12] C. Douligeris and D. Serpanos, Network Security – Current Status and Future Directions, John Wiley & Sons, Inc., United States of America, 2007, p. 2

[13] D. Clark, Enterprise Security – The Manager's Defense Guide, Addison-Wesley Information Technology Series, Indianapolis, 2002, p. 178

[14] G. Stoneburner, A. Goguen and A. Feringa, Risk Management Guide for Information Technology Systems (Special Publication 800-30), National Institute of Standards and Technology, Gaithersburg, 2002. p. 4.

[15] Security Risk Management Guide, Microsoft Corporation, 2004, p. 10. http://www.microsoft.com/technet/security/topics/complianceandpolicies/secrisk/

[16] S. Bosworth and M. Kabay, Computer Security Handbook (fourth edition), John Wiley and Sons, New York, 2002, pp. 1034 -1035.

[17] M. Tulloch, Microsoft Encyclopedia of Security, Microsoft Press, Washington, 2003, pp. 387-389.