Defining the Resilience of Critical Systems to Cyber-Attacks

OSHAKBAY DANA, AKHMETOVA ZHANAR
Information Security Department
L.N. Gumilyov Eurasian National University
Nur-Sultan, st. Satpayev 2
KAZAKHSTAN

Abstract: - The article presents the features of the definition of critical systems, as well as the definition and types of use of the critical system in Kazakhstan. In this article, the stability of critical systems to cyber-attacks was studied, was defined the cyber resilience of critical systems to cyber-attacks. There is given the methods how cyber resilience to cyber-attacks could be implemented.

Key-Words: - critical system, critical systems design, cyber-attack, critical systems resistant to cyber-attacks, cyber resilience, critical system model.

Received: June 13, 2019. Revised: March 14, 2022. Accepted: April 11, 2022. Published: May 6, 2022.

1 Introduction

In recent years, great attention has been paid to security-critical systems, due to their importance and criticality in many types of confidential information, both civilian, military, and information that ensure viability. Today, critical systems are used in a variety of areas that are computerized to improve production or maintenance efficiency, critical systems can be nuclear power plants, aircraft and aerospace vehicles, air traffic control, ground transportation systems like trains and cars, medical electronic devices and patient monitoring, chemical plants, fire protection systems on oil/gas platforms, telephone switching networks, robots in production systems and hazardous environments, military vehicles [1]. These applications are characterized by the content of critical information and high risk, in this regard, the issue of providing critical systems resistant to cyber-attacks is becoming more and more important. Failure of the listed critical systems can lead to large financial losses.

2 Critical systems

To ensure the continuous and safe operation of critical systems, it is necessary to determine the resilience of critical systems to cyber-attacks.

Critical systems are security-critical systems that have stochastic behavior, according to the stochastic nature of the external world, due to hardware failures that can occur stochastically security-critical systems are stochastic and have probabilistic type [2]. The definition of a critical system is the state of the system, which must be highly reliable and maintain this reliability as it develops, without requiring prohibitively high costs. Reliable security methods are used for critical systems [2]. Consequently, critical systems are usually developed using well-proven methods, rather than newer methods that have not been the subject of extensive practical experience.

There are three types of critical systems:

- Critical security system: Failure and attack in critical security systems results in injury, death or environmental damage.
- Critical systems: failures in critical systems lead to non-fulfillment of expected behavior and work, for example, the navigation systems of a spacecraft.
- A business-critical system: damage in these systems leads to large financial losses and financial risks as a banking accounting system [3].

According to the Cybersecurity and Infrastructure Security Agency, the types of critical system infrastructure are divided into the following sectors:

- communications sector;
- chemical sector;
- transportation systems sector
- commercial facilities sector;
- critical manufacturing sector;
- industrial control systems;
- defense industrial base sector;
- emergency services sector;
- energy sector;
- financial services sector
- food and agriculture sector
- government facilities sector
- healthcare and public health sector
- information technology sector

- nuclear reactors, materials, and waste sector
- water and wastewater systems sector.

Cybersecurity of critical systems, industrial electronics, and life support systems is becoming increasingly important as the Internet of Things is used in life. Serious vulnerabilities have been identified in embedded secure and critical devices, such as insulin pumps, pacemakers, etc. Researchers have developed exploits for these devices that demonstrate that patient safety can be compromised remotely by cyberattacks.

3. Defining the critical systems in Kazakhstan

In Kazakhstan, critical systems are defined by the list of critical information and communication infrastructure facilities approved by the Decree of the Government of the Republic of Kazakhstan dated September 8, 2016 No. 529, which are regulated in the rules and criteria for classifying information and communication infrastructure facilities as critical information and communication infrastructure facilities. In these rules, a critical system is defined as critically important objects of information and communication infrastructure [4]. Those critical systems are objects of information and communication infrastructure, the disruption or termination of the functioning of which leads to an emergency situation of a social and (or) technogenic nature or significant negative consequences for defense, security, international relations, the economy, certain areas of the economy or the vital activity of the population living in the relevant territory, including infrastructure: heat supply, electricity supply, gas supply, water supply, industry, healthcare, communications, banking, transport, hydraulic structures, law enforcement. This list of critical system objects includes at least one of the following criteria:

- critical facilities /systems affect the continuous operation of particularly important state facilities, the consequences of a malfunction of which is to stop the activities of particularly important state facilities;
- affects the continuous and safe operation of strategic facilities, facilities of economic sectors, the consequences of the failure of critical systems will be the shutdown of the activities of strategic facilities, as well as the emergence of man-made emergency threats;
- affects the sustainable functioning of the object of informatization of "electronic government" and other information and communication services, has the consequences of a social situation.

The influence of the object of information and communication infrastructure on continuous operation is particularly important, in this regard, the following rules apply to critical systems:

- to monitor the provision of information security of critical systems facilities;
- to ensure the connection of information security monitoring systems to the technical means of the security monitoring system;
- notify about information security incidents;
- transfer backup copies of electronic information resources to a single platform for backup storage of electronic information resources.

The purpose of this Concept is to achieve and maintain the level of protection of electronic information resources, information systems and information and communication infrastructure from external and internal threats, which ensures the sustainable development of Kazakhstan in the conditions of global competition [4].

End users are considered the weakest link and the primary vulnerability within a network. Since end-users are a major vulnerability, technical means to improve security are not enough. Organizations could also seek to reduce the risk of the human element. This could be accomplished by providing security best practice guidance for end users' awareness of cyber security. Employees could be taught about common threats and how to avoid or mitigate them a cyber security risk mitigating end user program could consist of a combination of multiple approaches including cyber security awareness, cyber security training, and cyber security education. According to, and adopted from, see the below table that provides a comparison of the approaches [5].

A cyber-attack is a malicious and deliberate attempt by an individual or organization to hack into the information system of another individual or organization. Usually an attacker is looking for some benefit from disrupting the victim's network. There are the most common types of cyberattacks:

1. Malware, malicious software as spyware, ransomware, viruses, and worms, which breach with vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can do the next:

- blocks access to key components of the network, also known as ransomware;
- installs malware or additional harmful software;
- furtively obtains information by transmitting the data from the hard drive of the computer, also known as spyware;
- disrupts certain components at the system.

2. Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, the given communications that appear to come from a reputable source usually performed through email. The reason is to steal sensitive and confidential information like credit card and login information or to install malware on the victim's machine. This is a common type of cyber-attack that every company should care about in order to be aware.

3. Man-in-the-middle attack, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data. One type of man-in-the-middle attack is unsecure public network, attackers can insert themselves between a visitor's device and the network. Without knowing, the visitor passes all information through the attacker. The second type of attack is when malware has breached a device, an attacker can install software to process all of the victim's information.

4. A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. For the given type of attack the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a distributed-denial-of-service attack.

5. A Structured Query Language injection occurs when an attacker inserts malicious code into a server that uses Structured Query Language and forces the server to reveal information it normally would not. An attacker could carry out a Structured Query Language injection by submitting malicious code / data into a vulnerable website searching mechanism. Learn how to defend against Structured Query Language injection attacks.

Cyber-attacks to critical system have become increasingly reliant on connectivity, their vulnerability to attack and exploitation has risen accordingly. World-changing events in the last year have forced organizations to adapt and rely heavily on remote access to ensure continuity.

Considering how devastating cyber-attacks on critical infrastructure can be, it's worth looking at successful attacks to learn how to prevent similar ones in the future. The common types of cyber-attacks on critical infrastructure are:

1. the Triton malware attack;
2. Taiwan's state-owned energy company;
3. cyber-attack to Israeli water systems;
4. Nippon Telegraph and Telephone;
5. Iranian Cyber Attack on New York Dam;
6. Unnamed American Water Authority;
7. Colonial Oil Pipeline.

4. Cyber resilience

To increase the resilience to cyber-attacks of critical systems, it is necessary to build an effective strategy that includes components of a variety of solutions in the field of computer security. A strategy to ensure the resilience of critical systems to cyber-attacks may include the following ways to strengthen information security in the information and communication infrastructure of a critical system:

- artificial intelligence and machine learning;
- ensuring the security of critical system data;
- ensuring the security of the critical system application system;
- identity and access management;
- provision for the management of incident management operations.

Artificial intelligence and machine learning are an effective method of ensuring cyber resilience. Given the huge amount of data in critical systems generated by security solutions, the use of systems that can analyze behavior and risks and automate responses can significantly enhance an organization's ability to intelligently adapt to vulnerabilities and attacks. One of the main reasons why Artificial intelligence should be used in cybersecurity is the ability of AI to learn and evolve from mistakes. Apart from this, Artificial intelligence has many advantages and applications in various attacks, cyber security being one of them. One of the buzzwords within the Data Innovation is Internet of Things. Long-standing time is Web of Things, which is able change the genuine world objects into shrewdly virtual objects. Achieving a good level of security in Internet of Things is not an easy task due to low powered, resource efficient and autonomous nature of IoT devices. Internet of Things devices are also designed for limited functionality and the recent outburst in the requirement of Internet of Things devices has led to the production of insecure devices. Apart from that, since Internet of Things is a rather new field, there is a lack of experience among certain companies producing Internet of Things devices.

Confidence in information and systems, the security is key if society is to benefit from the potential efficiencies that the Internet of Things can bring. And public confidence is just as important for the SCADA systems that keep aircraft in the air as it is for the information technology platforms that underpin mobile banking.

Information security monitoring center (Security Operations Center, SOC) is a structural unit of the organization responsible for operational monitoring of the information technology environment and

prevention of cyber incidents. SOC specialists collect and analyze data from various infrastructure objects of the organization and, if suspicious activity is detected, take measures to prevent an attack. The information security-monitoring center can exist both as a separate division of the company, and as a team of specialists from different departments who combine SOC tasks with other responsibilities. In addition, SOC functions can be outsourced to specialized companies that carry out remote information security monitoring and response.

The functions of the security-monitoring center may differ depending on the size of the enterprise and its organizational structure. Most often, the scope of responsibility of the SOC includes active monitoring of the environment and collection of incident data, analysis of suspicious events, threat response, recovery after an incident, incident investigation, maintaining a register of resources and compliance management.

The security of application systems and critical system applications begins with the process of developing an application for a critical system that meets the requirements for the development of critical infrastructure application systems. Testing of a critical infrastructure application system should be scalable and flexible for integration with other critical system information infrastructure systems. It's required to comprise processes for simple navigation through the system. The network management, cyberattacks, model-based detection, probabilistic forecasting methods, and uncertain linear systems are studied. It's also possible to highlight the main points that have been studied in this article as a deception-based security system for planning and integrating deception, models for understanding the actions of attackers during attacks, quantitative indicators for measuring the effectiveness of attackers and defenders.

Identity and access management, which allow access to critical systems and data. It's needed to abide by with the requirements for an identity with the exact access level. It's required to expand patterns for identification and identification when abnormal patterns appear. Solutions to ensure incident management of critical systems should expand the productivity of resources. Security management, automation and response systems and security information and event management systems are necessary to ensure the safety of critical facilities. Resistance to cyber-attacks increases the level of cybersecurity in an organization and its skill to define priorities, taking into account the risks when designing a critical system resistant to cyber-attacks. Information security incident management centers filter the misleading positives, notify about threats of security incidents.

One of the approaches widely used in the field of information security and the identification of information security threats is the General Vulnerability Assessment System, which is used to assess the severity of vulnerabilities after they are detected. This method prioritizes remediation and mitigation efforts so that priority is given to the most critical vulnerabilities. General Vulnerability Assessment System performs this assessment using a combination of predefined weights and subject matter expert assessments to quantify the exploitability and impact for a particular vulnerability and provide an overall assessment of the criticality of the vulnerability.

The reason for the disagreement of attacks to critical systems is the complexity of critical infrastructure. The necessary device infrastructure, as power technology and distribution, is becoming additional complex and reliant on networks of connected gadgets. Simply many years in the past, electricity grids and other crucial infrastructure operated in isolation. Today some distance greater interconnected both in terms of geography and throughout sectors. As the us power grid state of affairs highlights, the failure of one critical infrastructure should result in a devastating chain reaction. The vulnerability of critical infrastructure to cyber-attacks and technical screw ups has grown to be a large subject. And fears have been given credence through current occasions.

4 Conclusion

The digitalization is becoming part for different critical system infrastructure. Therefore the enhancing the resilience to cyber-attacks is important part to prevent the cyber risks. Information on the design of critical systems resistant to cyber-attacks that will be used for the analysis of the study will be used for the conclusion and further work on the dissertation research on the topic of probabilistic models in the design of critical systems resistant to cyber-attacks.

References:

[1] Barboni A., Francesca Boem, Thomas Parisini. Model-based Detection of Cyber-Attacks in Networked MPC-based Control Systems. [URL: https://www.sciencedirect.com/science/article/pii/S2405896318324091?via%3Dihub

[2] P. Popov. Stochastic Modeling of Safety and Security of the e-Motor, an ASIL-D Device.

URL:
https://openaccess.city.ac.uk/id/eprint/12518/.

[3] Symbat, I., & Yesseniyazova, B. M. (2019). Cyber Security Issues in Digital Kazakhstan. In NISPA Organization. URL: https://www.nispa.org/files/conferences/2019/e-proceedings/system_files/papers/cyber-security-issues-issabaeva.pdf.

[4] Friedman, A., Moore, T., & Procaccia, A. (2010). Cyber-sword v. cyber-shield: The dynamics of us cybersecurity policy priorities. Under Review. // URL: https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/Friedman+cyberwar-governance+sword+shield_0.pdf

[5] Decree of the Government of the Republic of Kazakhstan dated June 30, 2017 No. 407 On Approval of the Cyber Security Concept ("Cyber Shield of Kazakhstan") // URL: https://adilet.zan.kz/rus/docs/P1700000407.