Information Security of Power Plants

Dinar Nabiullin[1,*], *Rustem* Vildanov[1]

[1]Krasnoselskaya st., 51, Kazan, Rep. Tatarstan, 420034, Russia

Abstract. The article deals with the main problems of the information security of power plants. Possible probabilities of hacker attacks on individual objects in the energy sector have been investigated. Possible attack scenarios and ways to prevent them are also discussed.

1 Introduction

With the development of digitalization in the power industry, the number of hacker attacks on industrial facilities has increased dramatically. In this regard, the question arose about measures to counter cyber-attacks, such as the creation of laws and regulations for information security. Methods have been proposed to prevent information attacks on critical infrastructures.

2 Information security in the energy sector

With the advancement of digitalization, energy is becoming an increasingly complex, interdependent, and dynamic industry. The problem of information security in this segment is not yet so acute, but in 5-10 years, this problem may become paramount in various segments of the energy sector. Information security will undoubtedly play an important role in improving the efficiency of the technological process since the failure of devices in operating systems reduces the reliability, uninterrupted generation, and distribution of energy resources. The main task is to analyze weaknesses at certain power plants, as well as access control, accounting, and information security in the company. Speaking about technological objects, one should take into account the specifics of the APCS, SCADA (Supervisory Control and Data Acquisition), and DCS (Distributed Control System). When creating an information security system, it is necessary to carefully study the protected object and technological processes and take into account many possible factors.

3 Initiating a cybercrime

A cyber-attack can be divided into 4 stages:

1) preparation for the attack;
2) penetration into the system;
3) distribution;
4) sabotage.

Preparing for an attack: Preparing for a cyber-attack includes identifying a specific target (power plant), searching for the maximum amount of information about it, identifying weaknesses in the security of objects. Then a strategy is developed, penetration tools are created from previously created or new, specialized ones, then they are tested on models. Monitoring is carried out for the presence of open ports through which penetration into the system is possible.

Penetration into the system: at this stage, an attacker injects a Trojan horse or worm into a private host (server) that can cause irreparable damage to equipment. In this case, the malicious code enters the closed network. Malicious software can be injected in different ways:

1) Downloading a program under the guise of specific documentation in the form of PDF or DOC, as a result of downloading the file, a macro is triggered (automatic opening of the file on the computer).

2) Using social engineering, an attacker can convince an employee to install a certain program that includes malware.

3) Zero-day vulnerability - [1]. Day zero refers to a recently discovered software vulnerability. Since the developer has just learned about the vulnerability, this also means that there was no official patch or update to fix the problem. Day zero refers to the fact that developers have zero days to fix a problem that has just been identified and may have already been exploited by hackers. Once the vulnerability becomes known to the public, the vendor must promptly fix the problem and protect its users.

Distribution: here the attacker tries to deploy his program as much as possible inside the device, paying special attention to especially important points - production servers. The work is performed under the administrator's name, thus remaining unnoticed by the security system [2].

Sabotage: This step is the key to deleting important files or managing the programmable logic controllers and SCADA systems. Critical files, manipulation of devices, monitoring and espionage, sabotage, as well as

[*] Corresponding author: dinar91121mail.ru

neutralization of electrical equipment [3]. The creators of these threats are highly skilled and have a deep understanding of industrial control systems and communication protocols in the power industry. These attacks can be carried out not deeply by "individuals", but by entire groups acting in the interests of the enterprise or the state. It is not possible to fully identify attackers by IP address, since most IP addresses are hidden from strangers.

4 The first appearance of cyber-attack in the energy sector

One of the first known and most powerful cyberattacks was carried out in 2010 on Iranian enterprises, in particular at nuclear power plants [4].

It is the first known computer worm that intercepts and modifies the information flow between Simatic S7 PLCs and workstations of Siemens' Simatic WinCC SCADA systems.

Thus, the "worm" can be used as a means of unauthorized data collection (espionage) and sabotage in the process control systems of industrial enterprises and power plants. Then the most dangerous and colossal attacks followed, these are BlackEnergy attacks [5]: BlackEnergy was used for cyberattacks on users with the help of a Trojan horse, cybercriminals delivered a special component "KillDisk" to computers of dispatchers of the electric network, specializing in destroying files on disk. Win32 / Industroyer: Win32 / Industroyer has a high level of expertise and a deep understanding of industrial control systems and communication protocols in the power industry.

It is unlikely that anyone would be able to write and test such software without access to the specialized hardware used in the target environment. Each attack had its own uniqueness and consequences; therefore, the attack was “targeted” [6,7].

5 Methods for preventing cyber attacks

Before launching a cyberattack, hackers fully study the infrastructure of the power plant, as well as each vulnerability and method of implementing the attack [8]. Therefore, in order to prevent cyber-attacks, it is necessary to carry out measures to check computers, relay protection devices, SCADA systems for operability and to check for "abnormal" activity in computer processes. It must be assumed that systems remain safe from cyberattacks as long as the entire technological structure is kept secret from outsiders. It can be assumed that without detailed specifications, attackers will not be able to manipulate the equipment (and will not even try to do it). This approach to information hiding will block all opportunities for cyberattacks on individual devices or networks [9].

Another way to improve security and protection against illegal entry or deliberate distortion of information is:

a) development of a corporate standard for ensuring information security (a series of international standards, including information security standards published jointly by the International Organization for Standardization (ISO) and the International Organization for Standardization) [10].

b) restriction or exclusion of the use of wireless and remote access to APCS without authorization and authentication. In this case, we are talking about unauthorized access to the system using the telnet protocol, where you can authorize and enter the system having access to the internal IP address and port.

c) measures to organize the protection of information in the field of industrial safety [11].

Main goals:

1) Prohibiting employees from downloading unknown files from third-party resources.

2) Drawing up a plan of explanatory work on the cybersecurity of industrial enterprises [12].

3) Creation of a log of unstable computers.

Conclusion

The article examines the state of information security of power plants, draws attention to the fact that the problems of cybersecurity in the energy sector are aggravated by the spread of the concept of intelligent energy systems. An increasing number of power plants are using virtual private network (VPN) connections or a web interface to remotely control electrical equipment. Thus, it is necessary to secure the authentication by changing the login password to a more complex one. Security updates are critical to preventing cyber-attacks by closing vulnerabilities that can provide access to the system without the need to provide login IDs and passwords. Methods for the implementation of information security are considered, attention is drawn to the need to take measures to ensure information security of power plants at the state level. The authors put forward optimal solutions to the problems of information security of power plants: 1) limiting the use of wireless and remote access to the SCADA system without authorization and authentication; 2) awareness of employees about the presence of cyber threats for programmable logic microcontrollers, relay protection, and APCS; 3) monitoring computers and devices of program logic controllers for the presence of abnormal processes in the system.

References

1. B. Genge, I. Kiss, and P. Haller, A system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures, International Journal of Critical Infrastructure Protection, Elsevier, Vol. 10, pp. 3-17, (2015).

2. G.N. Ericsson, Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure, (2010).

3. Todd Baumeister, Literature Review on Smart Grid Cyber Security, (2011).

4. R. McMillan, “Siemens: Stuxnet worm hit industrial systems,” COMPUTERWorld, Sept.14, (2010).
5. M. Nefodova, BlackEnergy. URL: https://xakep.ru/2016/01/05/blackenergy/
6. Athanasios Dagoumas, Assessing the Impact of Cybersecurity Attacks on Power Systems, (2018).
7. Jason F. Clemente, Cyber security for critical energy infrastructure, September (2018).
8. A. Anwar, A. Mahmood, "Cyber security of smart grid infrastructure", The State of the Art in Intrusion Prevention and Detection, CRC Press, Taylor & Francis Group, USA, January (2014).
9. B. Genge, P. Haller, I. Kiss, A Framework for Designing Resilient Intrusion Detection Systems for Critical Infrastructures, International Journal of Critical Infrastructure Protection, Elsevier, vol. 15, pp. 3-11, (2016).
10. Richard Bejtlich, The Practice of Network Security Monitoring: Understanding Incident Detection and Response, (2013).
11. B. Genge, P. Haller, I. Kiss, Cyber Security-Aware Network Design of Industrial Control Systems, IEEE Systems Journal, IEEE Systems Council, Vol. 11(3), pp. 1373 – 1384, (2017).
12. Grishina, NV Informatsionnaya bezopasnost’ predpriyatiya. Textbook / N.V. Grishina. - M .: Forum, 2015, 55 p.