PUBLIC LAW

Cyber Security Audit of Critical Infrastructure at National Level - from Necessity to Legal Imperative

Adrian Constantin APOSTOL[1]

Abstract: *Offensive actions in cyberspace against both state institutions and citizens continue to have a significant presence in the dynamics of national security risks. The trend is upward, with the threat evolving both in terms of the number and complexity of cyber-attacks. The recent evolution of cyber-attacks in our country places the cyber threat among the most dynamic current threats to national security, the issue of cyber security becoming a priority for all actors involved.*

Keywords: *audit; cyberspace; cybersecurity; vulnerability; cyber attack*

I. Introduction

We have recently witnessed the resurgence of cyber-attacks on the IT&C infrastructures of the Romania as well as of our traditional allies, attacks with uncertain genesis, very difficult to attribute, being almost as difficult to repair the damage caused. Since early 2022, the wave of attacks that have mainly targeted Ukraine, but also other European countries including Romania, in areas vital to the functioning of a society - financial, military, energy, communications, health, etc., has foretold the conventional war that has changed the course of recent history, starting with February 24, 2022.

In this context, cyber security and our digital autonomy have become a topic of strategic importance for the European Union or the North Atlantic Treaty Organization of which Romania is a part, and as the level of threat increases, there

[1] PhD Student, Doctoral School of Socio-Human Sciences, Management "Dunarea de Jos" University of Galati, Romania. Corresponding author: adrianconstantin2003@yahoo.com. This article was presented at the International Conference "Exploration, Education and Progress in the Third Millennium", that took place in Galati, Romania, on the 12-13th May 2022.

is a need to intensify efforts to protect our information systems and our digital infrastructure against cyber-attacks.

Cyber security is not just about utilities, defense or health systems, but also about the protection of personal data, business models and intellectual property. In short, cybersecurity aims to protect democratic societies, our independence as European citizens and the way we live together.

An imperative of today's society is to adopt an adequate and flexible legislative package, to implement a set of proportionate and combined measures, limited to cybersecurity, to ensure the normality of the digital information space at national level. In this perspective, the responsibility for ensuring cyber security lies with all the entities involved, requiring the involvement of both public and private institutions and civil society.

At the level of public institutions, it is important to implement proactive, preventive and reactive measures that may include security policies, concepts, standards and guidelines, risk management, training and awareness activities, implementation of technical solutions for cyber infrastructure protection, management identity, and consequence management. Institutions must also ensure that these measures are complied with by end-users, by exercising prudent conduct in the online environment.

At the same time, in order to be effective, the actors involved in ensuring cyber security must know the impact and effects of a possible cyber-attack, the sensitive data transmitted within their own computer systems, the exposure of their own IT&C systems to risks and enter into partnerships with other entities in order to increase their own cyber security.

However, the first wall of protection against threats in the virtual space is represented by the user, so all the staff of an institution must be trained in the sense of a prudent professional behavior from a cyber safe perspective.

Given the evolution of the international security environment and the increasing relevance of cyberspace to national security, has emerged the need for effective institutional management of cybersecurity threats from cyberspace.

Progress has been made over time in creating and developing effective resilience mechanisms and responding to cyber threats by aligning with relevant European legislation and regulations, namely:

- the establishment of the National Cyber Security Directorate (DNSC - former CERT.RO) and the Cyber Security Operational Council (COSC), entities provided by the Romanian Cyber Security Strategy, which ensures the format of cooperation to ensure cyber security between public authorities and institutions with responsibilities and capabilities in the field;

- designation[1] of the Romanian Intelligence Service as a national authority in the field of cyber intelligence, having the mission to prevent and counter threats in the virtual environment with an impact on the national security of Romania.

At the same time, important steps were taken in the direction of aligning the Romanian institutions with the European norms regarding the assurance of cyber security (NIS Directive), completed in 2018 with the adoption of *Law no. 362/2018 on ensuring a high common level of security of computer networks and systems*, which entered into force on 12 January 2019. The law transposes the so-called NIS Directive (*Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a common high level of security of networks and information systems in the Union)* and aims to:

✓ increasing the level of preparedness of EU states to deal with cyber security incidents and respectively increasing the degree of trust of citizens in the Digital Single Market;
✓ establishing a unitary set of measures and requirements to ensure cyber security;
✓ creating a framework for notifying cyber security incidents;
✓ establishing an institutional framework for cooperation, under the coordination of the Government;
✓ initiating a process of identifying essential service operators and registering them in the Register of Essential Service Operators (ROSE);
✓ establishing rules on the audit of OSE and FSD networks and systems, the establishment of public, private or sectoral CSIRT / CERT teams as well as rules on training in the field.

The legal norm specifically addresses:
A. Essential Services Operators (ESOs) in 7 sectors of economic activity:
✓ energy;
✓ transportation;
✓ banking sector;
✓ financial market infrastructures;
✓ health sector;
✓ supply and distribution of drinking water;
✓ digital infrastructure.

A. Digital Service Providers (FSD) in three categories, namely: online markets, online search engines, Cloud Computing services.

The NIS Directive has helped to improve cybersecurity capabilities at national level by requiring Member States to adopt national cybersecurity strategies and designate cybersecurity authorities. At the same time, it has helped to strengthen cooperation between Member States at Union level by setting up various forums to facilitate the exchange of strategic and operational information and improving the cyber resilience of public and private entities in seven specific sectors *(energy, transport, banking, infrastructure, financial markets, healthcare, drinking water supply and*

[1] by CSAT Decision no. 053/16.05.2008.

distribution and digital infrastructure) and within three digital services *(online markets, online search engines and cloud computing services)*, requiring Member States to ensure that essential service providers and digital service providers set cybersecurity requirements and report incidents[1].

Cyber security, as an ever-changing area, required that the European Commission has been in the process of revising the NIS Directive since 2020. Following this process, the NIS 2.0 proposal has been launched for debate and approval in the European Parliament.

The NIS 2.0 directive makes a number of major changes: it will be addressed to all medium and large organizations in a number of predefined sectors, including small entities, depending on the critical level for the economy or society.

The main innovations of the NIS 2.0 Directive are the following:

- the language of the directive changes, dividing the entities between **essential** and **important** ones, to which a different supervisory regime applies *(the essential ones are ex-ante and the important ones are ex-post)*
- the categories of sectors approached were extended;
- The implementation of security requirements imposed on companies becomes the legal responsibility of managers;
- addresses the security of "supply chains" and relations with suppliers;
- simplifies reporting obligations;
- introduces stricter surveillance measures for national authorities;
- includes more stringent law enforcement requirements;
- harmonizes the sanctions regime in all EU Member States.

The NIS 2.0 proposal currently covers ten sectors for essential entities: ***energy, transport, financial-banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration*** and ***space***. The new Directive also provides for a number of sectors for important entities: ***postal and courier services, waste management, chemicals, manufacturing, digital service providers***.

Under the proposal, each Member State would adopt a national strategy to ensure the resilience of critical entities and to conduct regular risk assessments. These assessments would also help to identify critical entities that would be subject to obligations to strengthen their resilience to non-cyber risks; obligations include risk assessment at the entity level, implementation of technical and organizational measures and incident reporting[2].

The year 2022 brought to the fore, since its inception, cyber security as a necessary condition for the normal functioning of Romanian modern society, by adopting on January 7 the "Cyber Security Strategy of Romania, for the period 2022-2027", as

[1] https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0014.02/ DOC_1&format=PDF.

[2] https://dnsc.ro/citeste/directiva-nis-2-0-UE.

well as the "Action Plan for the implementation of Romania's Cyber Security Strategy", for the period 2022-2027, a framework document whose stated purpose is to establish the main guidelines and general approaches in the field of cyber security.

In essence, the framework document promotes an up-to-date vision, adapted to current needs in the field, to help the whole of society: public administration authorities and institutions and private entities, academia, citizens. By implementing and applying the provisions of the Strategy by all relevant actors, the national security objectives and the commitments assumed by Romania at NATO and EU level will be fulfilled, creating in the context the necessary premises for the development of the business environment, national economy and education or research area.

II. Cybersecurity Audit

According to Chapter V of Law 362/2018, by cybersecurity audit we mean the activity through which a systematic assessment of all policies, procedures and protection measures implemented at the level of computer networks and systems, in order to identify malfunctions and vulnerabilities and providing remedial solutions.

Thus, each network and systems operator with an impact on national security, including those designated by the legislation transposing the NIS Directives, following the inclusion in ROSE, must develop procedures for testing and auditing the level of cybersecurity, as an integral part of the risk assessment process, and to constantly update the hardware and software technologies used in the infrastructure. At the same time, cybersecurity authorities and institutions with responsibilities for ensuring cybersecurity need to encourage and support the implementation of cybersecurity policies and measures by creating a unified framework, providing the necessary training and coagulating a community of experts in the field.

With a periodicity of two years or whenever the situation so requires, in order to stop the significant manifestation of cyber security risks of a Critically Valued Infrastructure (IVC) of an essential service operator registered in the Register of Essential Service Operators (ROSE), a cyber security audit is required by an authorized auditor.

Reports from EU Member States' Supreme Audit Institutions report that by 2018, half of them had not performed an IT security audit, prompting concern about a new vision for this type of audit in the Union[1]. In fact, globally there is a growing concern for internal and external cyber security audits, both at the level of private and public institutions. Public authorities with responsibilities in the field of cyber security consider ISACA (Information Systems Audit and Control Association) documents

[1] Contact Committee of the Supreme Institutions of the European Union, *op. cit.*, p. 35.

according to which there are three lines of defense of cyber security: organization management, risk management and internal audit[1].

III. Methods and Steps for Conducting a Cyber Security Audit

The stage of preparing a cyber security audit involves conducting studies that reveal basic data about the beneficiary: the field of work of the organization, types of services offered, the area in which it operates. The type of data that is protected, its importance in the organization and the time required to perform the audit are also relevant. Another detail that needs to be checked is that of previous audits and their outcome.

The auditor will prepare a questionnaire containing questions related to control management, methods of authentication / network access, physical security, external access to the system, access to external networks, the existence of secondary plans - "contingency planning", etc. These questionnaires will be completed by the employees of the audited entity in order to evaluate the control and security policies that the company to be audited uses. In evaluating the answers received, we will consider the subjectivity of the answers, as a result these questionnaires will only be an introduction to the company's practices.

The cyber security audit involves the phased performance of activities aimed at identifying vulnerabilities and risks to the IT&C infrastructure managed by the requesting beneficiary, aiming at:

1. Physical Security

It is the most important component in maintaining security, which is often ignored by system administrators, as most believe that occasional proximity is sufficient.

There are a few factors that need to be considered for that system to be secure, namely:

- ➢ location on a straight, fixed surface and at a distance of at least 10 cm from the floor;
- ➢ protection from any source of excessive light, wind, water or extreme temperatures;
- ➢ a permanent monitoring in situations of heavy traffic in the premises where the system is located;
- ➢ the existence of an alarm and / or secure access system;
- ➢ securing the system terminal so that unauthorized persons cannot access it;
- ➢ observance of the delegation procedure from the terminal when leaving the premises;
- ➢ protection of power sources;

[1] ISACA (2017). *Auditing Cyber Security: Evaluating Risk and Auditing Controls*, p. 8, quoted by the Canadian Centre for Cybersecurity, *Cyber Security Audit Guide for the Government of Canada,* June 2020, p. 7, https://cyber.gc.ca/sites/default/files/2020-09/Cyber-Security-Audit-Guide_e.docx, accessed at 02.05.2022.

- ➢ securing or disabling parallel / serial / IR / USB / SCS / FW ports;
- ➢ securing external memory media;

2. The Security of the Network to which the System Belongs

After checking the physical security, the network security will be checked, as a system operating in a network is more susceptible to an external attack than a "stand alone" system. The security of a network is much more difficult to assess because it requires an in-depth knowledge of both the various levels and components of the system and the services that interact with the system in question.

- ✓ special attention will be paid to ***securing the physical network*** (cable, router, switch, proxy, firewall, etc.) so that it cannot be accessed or modified without authorization;
- ✓ physical access to the network infrastructure is allowed only to authorized persons;
- ✓ people who manage the physical network must have a high degree of trust;
- ✓ networked systems are both physically and electronically secure;
- ✓ the network must be protected by a properly configured proxy and / or firewall;

Regarding ***authorized network traffic***, attention should be paid to:

- ✓ the name, functionality, manufacturer and nature of the installed software applications;
- ✓ if the services that interact with the network do not allow "by default" unauthorized access to the system;
- ✓ the existence of some limitations of the users, in order to prevent the leakage of sensitive information related to the security of the system in question;
- ✓ if authorized users can run command/shell lines to remotely access the system;
- ✓ if there are software applications that can interact with each other (conflict), generating security breaches;
- ✓ the existence of system logs with all the activity produced in the network;
- ✓ the obligation to periodically change the passwords by the users;
- ✓ encrypting network traffic;
- ✓ permission to use chat clients such as Yahoo Messenger, gTalk, Skype, on the network;

Regarding ***unauthorized network traffic***, proceed to:

- ✓ periodic verification of the existence of unauthorized attempts to connect to the system;
- ✓ checking for unauthorized programs running on the system in question, which could allow remote connection;
- ✓ verification of the existence of abnormally high activity in the network, produced by the system in question.

Regarding ***wireless network traffic***, it will be evaluated:

➢ if the connection to the WIFI network is made by password; what type of encryption is used?

➢ if the data traffic is encrypted;

➢ if access with external devices in the WIFI network is allowed.

3. Protocols / Services

It is the most laborious stage of a cybersecurity audit: computers are made to process and depending on the purpose of the system in question, it can run different types of software applications. Since all these applications are written by different programmers, at least one of them is likely to contain a vulnerability, as each programmer understands security in his own way, paying attention to it differently.

✓ In general, it is acceptable to consider that software applications that come pre-installed in a new system have reasonable security, but you should always check if the manufacturer has released updates (especially security - “Security patches”) or other relevant information on the specific configuration of the system in question.

✓ It will be checked, for each software application installed in the system in question, if there are both known security breaches and methods to use them (exploits). If the manufacturer has a newsletter announcing these issues, the network administrator must subscribe to it. Check that the applications have been set up correctly during installation.

✓ If the installed application can access sensitive data, it is checked if the user in question is authorized to work with this program.

✓ If there are “daemon” type applications (constantly running), it should be checked how it reacts to attacks such as “buffer overflow” or “denial of service”. It is also necessary to perform a “stress test” to see how the system reacts in situations of use at maximum parameters.

4. User Security

User security varies depending on the nature of the system in question. In some cases, the system is isolated, having the functions of a server, with few users. In other cases, hundreds of users can log in to that system, all with direct and simultaneous access. The importance of user security is directly proportional to their number and type, but it should not be ignored that it is enough for a single user to try to gain unauthorized access for the whole system to be compromised.

Recommended security measures:

- Development of a standard method for creating and maintaining user accounts: clear and concise rules, brought to the attention of each user;
- If we are in the scenario “one system - more users”, we must set the level of resources that each user can have (number of logs, the size of the allocated memory space, etc.);

- There is a possibility to limit the way a user connects to the system, by securing login terminals, running services such as "tcp_wrappers" or "identd", if he has direct access through protocols such as telnet, to verify that the user connects from the system it claims to be;
- Storing logs with user activity, connection time (date and duration), where you logged in, applications you ran, commands, etc.

5. Data Storage Security

Security of data storage is usually not seen as a risk, as it is assumed that people may or may not have access to it. There are many ways to gain access to this data illegally, and your system administrator needs to be aware of it. Thus, it will be assessed whether:

✓ the user has access only to what is relevant to his work;
✓ the user's account is limited, he has no administrator right on the system he works on;
✓ the administrator is aware of the users' rights policy.

6. Passwords

The password is the central component of any security scheme. There are several basic rules that need to be followed:

✓ Each user must have a complex password;
✓ The password must contain at least 6 characters and be a combination of letters, numbers and special symbols. The password does not have to be a name, noun, idea or any common word;
✓ There must be a password change policy. The user will not keep the password for more than a few consecutive months, and at the time of the change the new one must not have been used before;
✓ Passwords are not written down or stored in a place that can be accessed by unauthorized persons. It is preferable to memorize it.

7. The Human Factor

Since security also depends on people, not just technology, social engineering is one of the most dangerous and effective methods of attack. Fraud is a common method of penetrating the security of a system, so human factor testing is necessary in the context of a cybersecurity audit. This identifies how employees comply with certain security policies.

Types of social engineering:

- "Piggybacking": The auditor will dress in the same types of clothes that employees wear and sit at the entrance to the premises. He will wait until an employee comes and unlocks the door, then enters after him. This scenario is used to test whether an employee allows access to unauthorized persons inside enclosures equipped with code / card / key access systems.

- “Computer technician”: The auditor tries to convince an employee that he is either from the service department or from a company specialized in computer troubleshooting. Its purpose is to steal the device in which the confidential information is present.

- “Bribery”: The auditor tries to bribe an employee, giving him a large sum of money for certain information.

- “Phishing”: Sending fake e-mails that appear to come from officials. The purpose is to obtain confidential information.

- “Payroll”: The auditor intentionally leaves a CD labeled in such a way as to arouse the curiosity of an employee (“Employee Salary List”, “Current Year Promotions List”, etc.). The CD contains a malicious application that once run will be able to install a virus / Trojan, etc.

There are several options for action, depending on the specifics of each beneficiary.

8. Disaster Plan

It is a set of rules, policies and technologies that ensure the continuity of the organization in the event of a major problem. When a critical situation arises, this plan will help to quickly and temporarily restore an acceptable level of activity. The following are relevant:

- If there is a data backup policy;
- If there are power generators;
- If there is an alternative method of communication both inside and outside the company

IV. End of Audit

Once the evaluation has been completed, the auditor will engage in a discussion with the organization's director and security personnel, in which context he or she will communicate what he or she has discovered and whether there are issues that require urgent remediation. After a period, the auditor shall submit a formal report containing all the tests performed, together with their results.

V. Control of the Application of Legal Provisions; Sanctions

The National Directorate of Cyber Security (DNSC) exercises control over compliance with legal provisions on ensuring a high common level of security of networks and information systems, within the limits of legal powers of monitoring or verification.

However, prior to the imposition of a sanction, in the event that a digital service provider or essential service operator discovers an obligation under the law, or an act issued by DNSC under Law 362/2018, DNSC shall transmit to the entity in cause a notification informing him of the infringement found, the mandatory measures to be taken to remedy the deficiencies found and set the time limit for compliance as well as the applicable sanction.

But not the amount of the fine - which varies from 3000 lei to 5% of turnover, in case of serious deviations - should be the main motivating factor for the decision makers of the entities covered by the legal norm, but the awareness of the risks involved: exposes the organization by ignoring the activities necessary to protect its own IT&C infrastructure and its users; damage caused by cyber-attacks (Malware, Ransomware, Distributed Denial-of-Service, Web-based Attacks, Social Engineering, Cyberspionage), data theft and even interference in democratic processes, such as interference in electoral processes and misinformation campaigns[1].

VI. Bibliography

Curtea de Conturi a României, Auditul sistemelor informatice. Manual/Court of Accounts of Romania, IT systems audit. Manual, Bucharest, 2012, https://www.curteadeconturi.ro/uploads/25529564/77241a13/330b7f07/6c1123fc/16ba70a5/2eeb2cdf/0fbfb694/38bf227f/MANUAL_AUDIT_IT.pdf.

Curtea de Conturi a României, Ghidul de audit al sistemelor informatice/The Court of Accounts of Romania, Audit guide for IT systems, Bucharest, 2012, https://www.curteadeconturi.ro/uploads/b3578fec/2e705397/8f5ff376/123728f6/08da8783/a7cf8c9a/974875d0/4f7867de/GHID_AUDIT_IT_.

Canadian Centre for Cybersecurity*, Cyber Security Audit Guide for the Government of Canada,* June 2020, p. 7, https://cyber.gc.ca/sites/default/files/2020-09/Cyber-Security-Audit-Guide_e.docx.

Contact Committee of the Supreme Institutions of the European Union, *Audit Compendium. Cybersecurity in the EU and its Member States*, December 2020, pp. 9-12, AuditCommitehttps://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EN.pdf.

[1] Contact Committee of the Supreme Institutions of the European Union, *Audit Compendium. Cybersecurity in the EU and its Member States*, December 2020, pp. 9-12, AuditCommitehttps://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EN.pdf, accessed on 02.05.2022.

Legislation

Order no. 599/2019 on the approval of the Methodological Norms for the identification of essential service operators and digital service providers.

Order no. 1323/2020 for the approval of the Technical Norms regarding the minimum requirements for ensuring the security of networks and IT systems applicable to operators of essential services.

Decision no. 88/2020 on the approval of the List of European and international standards and specifications.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems in the Union.

https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016L1148.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cyber Security) and on the certification of cyber security for information and communication technology and repealing Regulation (EU) no. 526/2013 (Regulation on cyber security).

https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32019R0881.

Law no. 362/2018 on ensuring a common high level of security of networks and IT systems.

http://legislatie.just.ro/Public/DetaliiDocument/209670.

Emergency Ordinance no. 119 of July 22, 2020, for the amendment and completion of Law no. 362/2018 on ensuring a common high level of security of networks and IT systems. http://legislatie.just.ro/Public/DetaliiDocument/228369.