Adrian-Viorel DRAGOMIR
Doctoral School Industrial Engineering and Robotics,"Politehnica" University of Bucharest

WHAT'S NEW IN THE NIS 2 DIRECTIVE PROPOSAL COMPARED TO THE OLD NIS DIRECTIVE

Perspective, opinion and commentary

Keywords
NIS 2;
NIS Directive;
National competent authority;
Resilience, cyber-security;

JEL Classification
O32

Abstract

One of the most sensitive activities in the online environment is to ensure the security of information managed by entities, persons, or public institutions that are stored and traded through IT&C systems in the new technological context. New innovative technologies, in addition to their value, can also have negative sides with security in the digital world, and this is an increasingly common topic in the discussions in this area. Not all security incidents can be prevented, but proactive measures to mitigate their impact must be taken in any context. Information, like any critical resource of any organization, is one of the most important components for businesses operating in the European Union and therefore its protection requires particular attention. Sensitive information has become the target of increasingly numerous and diverse threats and attacks in both the public and private sectors. Cyber security measures can protect organizations from multiple threats to business continuity, data veracity, and increase resilience to cyber-attack and minimize the risk of information theft. In order to try to mitigate as many of the issues described above as possible, the European Commission has initiated the process of revising Directive (EU) 2016/1148 on the security of network and information systems (NIS Directive) since June 2020. On 16 December 2020, the Commission launched the proposal for a NIS 2.0 Directive which will be submitted for debate and approval in the European Parliament. One of the major changes brought about by the new Directive is that the Public Administration becomes a sector covered by the new Directive. Under the new regulations in the proposed NIS 2.0 Directive, the scope of activities covered by the national competent authority in the field of cyber security (CERT-RO cf. Law 362/2018) extends to this new sector, which will explicitly include ministries and agencies of the state, the territorial extensions of the central administration, as well as the structures of the local public administration.

INTRODUCTION

CERT-RO's obligation of institutional independence from entities established by the NIS 2.0 Directive given that the CERT-RO institution is the National Regulatory Competent Authority for the NIS Directive, it is necessary to maintain it under the coordination of the Prime Minister of Romania so as to avoid the situation that the regulatory authority is subordinated to the entities it regulates under the Directive. NIS 2.0 and implicitly of Law 362/2018, according to art.34 par.1 (Law no. 362/2019).
The most important thing that follows from this is that CERT-RO, as the competent authority at national level responsible for the implementation of the NIS Directive and the application of Law 362/2018, to maintain its institutional independence according to Art. 3. of GEO 90/2019. It ensures equidistance from all structures of the central public administration, avoiding the pressures of a public authority in case of subordination to a certain ministry and maintaining functional independence, as well as strengthening the position in the process of applying European cybersecurity rules in our country.
In addition, the coordination of the Prime Minister of Romania brings the necessary authority to fulfill the institutional responsibilities both at internal and European level.
We remind you that the subordination of CERT-RO to the former MCSI was the main cause for which Romania delayed by three years the adoption of the law transposing the NIS Directive, reason for which the infringement procedure against Romania in case no. 2019/2214.

NIS DIRECTIVE IN ROMANIA

The NIS Directive or the European Union Directive no.1148 / 2016 on measures for a high common level of security of networks and information systems in the European Union has its effects this year in Romania, with a strong impact on companies that do not comply. Fines can reach up to 5% of turnover.
So, if your organization is an operator of essential services such as medical, banking, drinking water supply and distribution, transportation or a digital service provider, it is very important to consider the practical ways in which you maintain a minimum level of security. cybernetics of the networks and computer systems that your institution uses.
NIS is the acronym for Network and Information Security but also the abbreviation of the title of the first European Directive on cyber security (Directive on security of network and information systems). Adopted by the European Parliament on 6 July 2016, the NIS Directive had to be transposed into the legislation of the Member States by 9 May 2018, following the identification of essential service operators, ie those companies to which the Directive applies, to be identified by 9 November 2018.

Why a cybersecurity directive was needed
In short, companies, regardless of their size, have become dependent on various computer systems and services, which has attracted the interest of cybercriminals. Security incidents have skyrocketed in recent years, so MEPs have said that all Member States should take this issue equally seriously.
This is in the context in which EU members had different levels of preparedness for cyber threats and unequally ensured the protection of consumers and businesses. However, the implementation of this directive seeks to bring all companies in the Member States to the same common high level of security of networks and information systems in relation to the associated risks.
The aim of the NIS Directive is therefore to protect European citizens by forcing companies in critical industries to adopt a set of standard measures and mechanisms through which they can ensure a high common level of cyber security. In addition, the Directive creates the necessary framework for Member States to work together to identify and eradicate cyber theft networks.

Transposition of the NIS Directive into national law
In Romania, the transposition of the NIS Directive was made in 2018, by Law no. 362/2018 on ensuring a high common level of security of networks and information systems. The normative act entered into force on January 12, 2019, but until July 2020, when the Government issued GEO no. 119 for amending and supplementing Law no. 362/2018, the implementation process of the Directive was blocked due to the legislative vacuum.
However, there are now technical rules on the minimum security requirements for networks and information systems applicable to essential service operators.

Who should apply the provisions of the NIS Directive?
Law no. 362/2018 on ensuring a high common level of security of networks and information systems targets two categories of companies.
Essential Services Operators (OSEs) from 7 sectors of activity vital for the economy:
1.1 energy;
1.2 transport;
1.3 the banking sector;

1.4 the medical field;
1.5 financial market infrastructures;
1.6 digital infrastructure;
1.7 supply and distribution of drinking water.
Digital Service Providers (Digital Service Providers), respectively:
2.1 online markets;
2.2 online search engines;
2.3 cloud computing services.
If you are a digital service provider, but you are in the SME category, most of the obligations we will mention during this article will not apply to you.
However, in order to be sure of the entity's status in relation to the NIS Directive, it is best to consult the Methodological Rules for the identification of essential service operators and digital service providers. You can find them in the Official Gazette, Part I no. 584 of July 17, 2019. Also, the List of essential services can be consulted in Decision no. 963/2020.
In the fields where the legislation on ensuring a high common level of cyber security is applied, non-compliance can attract fines between 3,000 lei and 5% of turnover.
Beyond the obligations introduced by law and even if this legal framework is not addressed to your entity, taking the appropriate measures to maintain a high level of cyber security is, in fact, the policy you pay to avoid material and image damage. in the event of a cyber-attack.
A recent analysis by SAS, the world leader in analytics, points out that there are prerequisites for 2021 to be the year of digital fraud.
So, if you have already invested in digitization or allowed teleworking, your organization has probably opened more doors to its IT network. Therefore, you should make sure that your entity's networks and IT systems remain secure and you do not risk financial losses.
According to the NIS Directive and implicitly the national legislation, in order to ensure the security of networks and information systems, as an essential service operator (OSE) and / or digital service provider (FSD) you have the following obligations:
Implement appropriate and proportionate technical and organizational measures to meet the minimum security requirements.
These minimum security requirements relate to Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act):

- access rights management;
- user awareness and training;
- journaling and ensuring the traceability of activities within computer networks and systems;
- testing and evaluating the security of computer networks and systems;
- management of network and computer systems configurations;
- ensuring the availability of the essential service and the functioning of computer networks and systems;
- management of the continuity of the operation of the essential service;
- user identification and authentication management;
- incident response;
- maintenance of computer networks and systems;
- management of external memory media;
- ensuring the physical protection of computer networks and systems;
- implementation of security plans;
- ensuring staff security;
- risk analysis and assessment;
- ensuring the protection of products and services related to computer networks and systems;
- vulnerability management and security alerts.

Implement appropriate measures to prevent and minimize the impact of incidents affecting the security of the networks and information systems used to provide essential services, in order to ensure the continuity of those services.
Establish permanent means of contact and designate those responsible for the security of networks and computer systems responsible for monitoring means of contact.
To ensure the immediate response to the incidents that occurred, to restore the operation of the service to the parameters before the incident as soon as possible and to carry out the security audit.
To interconnect within 60 days from the registration in the Register of essential service operators to the alert and cooperation service of CERT-RO, to ensure the permanent monitoring of the alerts and requests received through this service or through the other contact methods and to take as soon as possible the appropriate response measures at the level of its own networks and information systems.
In addition to all these technical issues, if your entity is an essential service operator or digital service provider, you must report CERT-RO all kinds of information, including if you have experienced incidents that have had a significant impact. on the continuity of the entity's essential services. At the same time, you must submit to CERT-RO controls in order to establish the degree of compliance with your obligations under this law.
In the fields where the legislation on ensuring a high common level of cyber security is applied, non-compliance can attract fines between 3,000 lei and 5% of turnover.
Beyond the obligations introduced by law and even if this legal framework is not addressed to your entity, taking the appropriate measures to maintain

a high level of cyber security is, in fact, the policy you pay to avoid material and image damage. in the event of a cyber-attack.
A recent analysis by SAS, the world leader in analytics, points out that there are prerequisites for 2021 to be the year of digital fraud.
So, if you have already invested in digitization or allowed teleworking, your organization has probably opened more doors to its IT network. Therefore, you should make sure that your entity's networks and IT systems remain secure and you do not risk financial losses.
According to the NIS Directive and implicitly the national legislation, in order to ensure the security of networks and information systems, as an essential service operator (OSE) and / or digital service provider (FSD) you have the following obligations:
Implement appropriate and proportionate technical and organizational measures to meet the minimum security requirements.
These minimum security requirements relate to:

- access rights management;
- user awareness and training;
- journaling and ensuring the traceability of activities within computer networks and systems;
- testing and evaluating the security of computer networks and systems;
- management of network and computer systems configurations;
- ensuring the availability of the essential service and the functioning of computer networks and systems;
- management of the continuity of the operation of the essential service;
- user identification and authentication management;
- incident response;
- maintenance of computer networks and systems;
- management of external memory media;
- ensuring the physical protection of computer networks and systems;
- implementation of security plans;
- ensuring staff security;
- risk analysis and assessment;
- ensuring the protection of products and services related to computer networks and systems;
- vulnerability management and security alerts.

Implement appropriate measures to prevent and minimize the impact of incidents affecting the security of the networks and information systems used to provide essential services, in order to ensure the continuity of those services.
Establish permanent means of contact and designate those responsible for the security of networks and computer systems responsible for monitoring means of contact.
To ensure the immediate response to the incidents that occurred, to restore the operation of the service to the parameters before the incident as soon as possible and to carry out the security audit.
To interconnect within 60 days from the registration in the Register of essential service operators to the alert and cooperation service of CERT-RO, to ensure the permanent monitoring of the alerts and requests received through this service or through the other contact methods and to take as soon as possible the appropriate response measures at the level of its own networks and information systems.
In addition to all these technical issues, if your entity is an essential service operator or digital service provider, you must report CERT-RO all kinds of information, including if you have experienced incidents that have had a significant impact. on the continuity of the entity's essential services. At the same time, you must submit to CERT-RO controls in order to establish the degree of compliance with your obligations under this law.
According to the Technical Rules on Minimum Requirements for Network and Information Systems Security for Essential Service Operators, your entity must look after four areas of security:

- governance - refers to the development and implementation of security policies at the organization level and is a matter of top management of the entity.
- protection - refers to the need to ensure the security of networks and computer systems. We are talking here about the administration and maintenance of resources, networks and computer systems and about controlling access to the elements / components of computer networks and systems.
- cyber defense - refers to the need to ensure the management of security incidents. How does your entity detect incidents that affect the security of networks and computer systems? How do you treat them?
- resilience - refers to the management of the continuity of essential services provided or, in other words, business continuity. In this regard, you need to ask yourself questions about how to manage crisis situations such as natural disasters. What do you do in case of security incidents that have a major impact on essential services?

The four security areas are in turn divided into categories of security activities, and for each of them security measures are established with one or more security requirements, which in turn contain control indicators.
In the process of implementing security requirements, OSE companies must also:

- identify risks if they do not implement security requirements;
- to plan the activities underlying the implementation;
- to establish those responsible for their realization.

AMENDMENTS TO THE NIS 2.0 DIRECTIVE

The NIS Directive 2.0 brings a number of major changes to the legislative framework applicable to the regulated area, including:

- increase from seven to ten regulated sectors for key entities: energy, transport, financial-banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration and space;
- introduction of a series of sectors for important entities: postal and courier services, waste management, chemicals, manufacturing, digital service providers;
- strengthen security requirements for businesses and address security of supply chains and supplier relationships;
- simplifying reporting obligations and introducing stricter surveillance measures for national authorities; stricter law enforcement requirements, while aiming at harmonizing sanctions regimes in all EU Member States;
- intensify the exchange of information and cooperation on cyber crisis management at national and EU level;
- the extension of the provisions of the NIS 2.0 Directive to public administration is an important step forward in ensuring the security and efficiency of activities in the field of administration, with beneficial effects on the citizen.

A novelty with major impact in terms of legislative, organizational implications and responsibilities in the field of cybersecurity is the inclusion of public administration institutions in the list of key entities on which extends the application of the new NIS 2.0 Directive and implicitly Law 362/2018.

According to Annex I of the proposed NIS 2.0 Directive, the sectors to which its provisions apply have been expanded on the basis of experience gained and observations made in the process of implementing the original NIS Directive, following proposals from all Member States, including Romania.

Newly added sectors include general government, which includes the following types of entities:

- Public administration entities in central governments.
- Public administration entities from NUTS Level 1 Regions.
- Public administration entities from NUTS Level 2 Regions.

In this context, taking into account the requirements of the European Union as well as the national needs in the field of cyber security, it is imperative to continue the direct coordination of CERT-RO by the Prime Minister of Romania.

This solution needs to be maintained as it ensures both the preservation of the institutional independence of CERT-RO and Romania's exit from the infringement procedure by the European Commission, related to the postponement of the correct implementation of the NIS Directive.

The word "Cyberspace" first appears in the literature in the early 1980s. The term was coined by William Gibson in his novel Neuromancer. Thus, Gibson's definition for Cyberspace was as follows: “A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding”. But Gibson did not think, at that time, to warn his readers how to be safe in this virtual space but with real dangers.

Cyberspace is delimited from the personal computer to the servers with huge databases of various public and private systems, as well as the networks designed to connect these systems. As long as this information can be accessed by anyone who has a device connected to the system and can be used more or less responsibly, it is necessary to ensure a secure cyberspace where risks and threats are known and countered. At present, cybersecurity is on the security agenda of all developed countries, as well as other non-state actors in the international arena.

The theories developed by the great strategist Thucydides prove to be as current as they were more than two thousand five hundred years ago: as predicted by the "father of international relations," human nature and people's reactions remain the same, regardless of age (Whitman, & Mattord, 2019). Thucydides also anticipated the importance of non-military factors, with which states can ensure and maintain their security, such as diplomatic, economic, social or psychological factors. Also in Thucydides' view, the great powers enter into partnerships with small states, for well-established purposes, and large states guarantee them, in turn, security. The concept of "strategy", which has its roots in military science, has been constantly developed and perpetuated, incorporating strategies in the economic, social, political or other more modern approaches (cybernetic), in order to obtain and maintain an advantageous geostrategic position of a state in its relations with other states and hold control.

In the current context, state actors are forced to re-analyze their classical approach to war and take into account new types of modern threats. An important emphasis is placed on the use of cyberspace in order to counter possible threats, prevent risks, and strengthen the position in international relations. This has led to the fact that under the umbrella of anonymity, some states use their own cyber capabilities for military and

industrial espionage, for surveillance and interception of communications, as well as for the manipulation of information and communications addressed to target actors. However, it is not only states that use such methods, but more and more frequently and with considerable power, non-state actors, especially terrorist or organized crime groups.

With the expansion of virtual space, cyber threats have grown and diversified. From this perspective, developed and technology-dependent states have begun to prioritize important resources in order to prevent and counter cyber threats. Following the terrorist attacks of September 11, 2001, the United States adopted in February 2003, for the first time, the National Strategy to Secure Cyberspace. This strategy was part of a complex of measures to strengthen national security and contained a set of priorities in the field of ensuring the security of the national cyberspace, which consist of:

- establishing a national system for reacting to cyber threats;
- adopting a program to reduce specific threats and vulnerabilities;
- creating an early warning program;
- human resource training programs with responsibilities in the field.

Cyber security is the practice of protecting systems, networks and programs against digital attacks. These cyber-attacks are aimed at accessing, changing or destroying sensitive information; extorting money from users or disrupting normal business processes.

Implementing effective cyber security measures is particularly difficult at present, as there are more devices than people, and attackers are becoming more innovative.

Over time, information technology has developed rapidly, advances have led to the implementation of these technologies in all areas. At present, the existence and functionality of human society is closely related to information technology, if not even dependent, in certain sectors critical to the normal operation of IT infrastructures. We could briefly appreciate that daily, professional, economic and political activities depend on information technology and its remote transmission.

An example of the transformation of today's society is the way goods are traded today, the parties involved no longer have to be face to face to trade goods, but only to communicate their contractual data through virtual space. It should also be noted that "confidential political, social, economic or personal data" are stored on the cyber infrastructure (Briony, 2003).

When we talk about technological advances, we must necessarily present them in correlation with the process of globalization, therefore we can conclude that cyber dependence has expanded globally, but this is especially noticeable among developed countries.

At the same time, the widespread use of information technology by all countries of the world, has led to the creation of a global network, practically the physical boundaries between the states of the world being overcome by computer connections. This global network is characterized by a transnational interconnection, so that in the event of a well-targeted cyber-attack, the negative effects can be devastating, it can reach a negative chain propagation effect, the consequences of the attack being felt by several state entities.

Therefore, at present, in view of the transnational interconnection, the security of a state entity no longer depends exclusively on itself, but is given by the security of the weakest link in the computer protection system.

Nowadays, if someone intends to cause damage, there is now the ability to undermine and deactivate a society without firing a gun or rocket, given that the military, business, transportation, communications, services of utilities, e-commerce, emergency services and financial services depend on the availability, integrity and confidentiality of the information circulating through these infrastructures.

A clear distinction must be made between the seriousness and implications of cybercrime and crimes committed in the real world. For example, a wallet theft, for example, involves the loss of identity documents and money from it. In this situation, the thief enjoys the money obtained without being able to use the identity documents for other purposes.

On the other hand, when we talk about breaking into a personal email address or a bank account, the consequences are long lasting and much more serious, the identification data are compromised and can be used for a long time, without the primary user knowing this thing. The cybercriminal has unlimited possibilities to use the stolen information, including its use for the purpose of committing other illegalities. In addition, unlike real-world crimes, where it is much easier to identify the perpetrator, in the case of virtual space it is much more difficult, cyberspace being characterized by lack of borders, dynamism and anonymity.

It should be noted that we are talking on a small scale, in this case a person, but serious problems arise when the victim of the cyber-attack is a legal entity, a multinational corporation and ultimately a national, global entity. We could talk about a structuring of cyber attacks on levels according to the target, severity and implications, as follows: home users, large enterprises, critical sections, national issues and global.

Home users - the target is a person, the implications are minimal and are limited to the person concerned.
Large enterprises - in this situation the target is no longer a single person, but several people belonging to an organized group (company, company, etc.) are targeted. The implications are greater affecting the proper functioning of that group.
Critical section - at this level, when cyber-attacks target a critical area (water supply, electricity, gas, etc.) the problem of cyber security becomes a national security issue, because the failure of the service endangers human life. We can conclude that at this stage cyber-attacks are somewhat beyond the economic sphere, moving towards the political sphere as well.
National issues - the target is a state entity, therefore the essential defense and functioning systems are attacked, which makes it impossible to guarantee national borders and protect citizens.
Global issues - the consequences of such a cyber-attack are vast and the major negative effects extend to several state entities, for example, if they are unable to function properly common missile defense systems, nuclear missile launch systems, stock exchange values, etc.
Another aspect that must be taken into account is the speed with which information circulates in the virtual space and the accessibility of this virtual space, and here I refer first of all to the anonymity generated by the internet and easy access to it. In addition, cyberspace is not under the strict control of any state structure, and is not regulated by law.
Second, the costs are relatively low, so anyone can quickly acquire the technical capabilities needed for a cyber-attack. As a consequence, internationally, the characteristics of cyberspace, anonymity, low price, rapid flow of information and asymmetry, "make the power differences between actors to be reduced."
For these reasons, in The Global Risks 2014 report on threats that can lead to the collapse of a state's central administration, cyber-attacks have been included on the short list of threats.
Cyber-attacks, according to this report, aim on the one hand the theft of information and its pecuniary capitalization, and on the other hand the theft of vital information that can lead to compromise and disruption of services.

CONCLUSIONS

Internet security refers to "the protection of Internet-related services and information technology systems, as an extension of network security in organizations and at home, in order to achieve the goal of security".

In short, internet security is responsible for the operation, availability and reliability of internet services. It differs from network security in that the Internet has billions of users, while a network that is not connected to the Internet has a fixed number of users. Therefore, in the event of an attack, it may be easier to detect the attacker in a closed-loop network than in the case of an attack from a network connected to the Internet.
It is very easy to download computer infection codes on the internet, hidden under a series of programs, toolbars, games, advertisements, etc., which can be accessed and downloaded for free. Infection of the computer with such a virus code leads to the destruction and modification of information from the PC / network, the installation of programs designed to facilitate remote control (remote control), the installation of programs to copy identity or monitor activity on that device.
Protection in such situations is provided by software programs designed to detect data theft (anti-phishing), to detect a dangerous code (anti-malware), to detect a suspicious page, etc.

REFERENCES

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148&from=RO, website consulted on 02.05.2021;
[2] Law no. 362/2019 concerning measures for a high common level of security of network and information systems, http://legislatie.just.ro/Public/DetaliiDocument/209670 , website consulted on 10.05.2021;
[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2019.151.01.0015.01.ENG&toc=OJ%3AL%3A2019%3A151%3ATOC, website consulted on 11.05.2021;
[4] European Council conclusions on cyber activities in 2018, https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/ro/pdf, website consulted on 20.05.2021;
[5] Whitman, M. E., & Mattord, H. J. (2019), Management of Information Security (6 ed.).

Boston, Maryland, United States of America: Cengage Learning
[6] Briony, J.O. (2003), *The potential contribution of ICT`s to political process. Electronic Journal of e-Government, vol. 1*, no. 1, 33-42;