CYBER SECURITY - AWARENESS & ZERO TRUST MODEL IN PUBLIC DOMAIN

Ionuț Ciprian Băjinaru[1]
George Căruțașu[2]

Abstract

Simplifying one's life is realizing, with an exponential growth, by evolution, so as technological evolution makes its presence more and more in each domain of human activities. It is obvious the fact that the development of the Internet and the continuous appearance of new technologies represents a way for social development. Even though, this opportunity brings around a new challenge, the one of assuring the security of the entire virtual space.

The movement towards virtual space, internet network and cloud computing shifts the tension of confidentiality of the public institutions and private also, towards security of the virtual world and equipment security and internal rules and standards. Once the 5G technology will be implemented in real world usage, no matter the provider, the possibilities of turning our life smart will be infinite. unifying and control of all home equipment with your own phone. Regarding all this, all these systems have to be protected of attacks by private or state actors.

So, it is extremely important to be aware of the impact of a cyber-attack and that the virtual space has transformed in the fourth tactic war space. Regarding this we keep in mind Jens Stoltenberg's declaration that even a cyber-attack can trigger article 5 from the NATO book, because an attack of the critical infrastructure can become of absolute importance.

Keywords: cyber security, cyber warfare, cyber-attacks, awareness, zero trust model

1. Introduction

Cyber security domain has become an inseparable part of what collective defense means in NATO way of thinking. The need of clear views of this subject has manifested ever since the Summit in Warsaw in 2016, by the increase in cyber-attacks of important institutions and private companies.

[1] PhD Student Ionuț Ciprian Băjinaru (The Polytechnic University of Timisoara, UPT), ionut.bajinaru@student.upt.ro

[2] Prof. PhD George Căruțașu (Romanian-American University, URA), carutasu.george@profesor.rau.ro

Implementing the virtual space in all the activities of the alliance, clarifies their view on policies of cyber security, and the availability of enforcing cyber operations in wide spectrum is not just a future project for NATO, but a necessity in this dynamic and insecure world of our days.

Cyber security state level or institutional represents a status of normality of digital information, resources and services offered by public and private companies. [1]

Responsibility for cyber security measures is guaranteed and regulated by Romania's Cyber Security Strategy and National Plan of Implementation of the National Security Cyber Security Network.

At national level the subject is transposed by European Directive which gives the idea of current importance of this problem: Directive UE 2016/1148 which reconfigures institutional architecture within the institutional area of control attributes and sanctions of the EU / Regulation 2016. Rigorous regulation on protection of the personal data of the citizens. [2]

According to this information, there is a stable framework, but all technological evolution changes largely the action plan on an incident, as well as transcribed procedures and regulations in laws.

Therefore, all that is the set of laws, regulations, policies, cybersecurity standards is very difficult to regulate and maintained. At the level of a state, consisting of cybersecurity, in a sum of public institutions and private entities, it really is a challenge in comprehensive cybersecurity.

We believe this is a real problem, but also a major necessity, the creation and application of cyber security policies in the scalable and adaptable public domain to the new challenges, generally applicable to a high degree of effectiveness, with niche valences according to the institution Application, also containing various scenarios:

1. Security policies
2. Standards and models
3. Awareness and promoting security culture
4. Risk management
5. Solutions for IT & C Networks and Systems

2. What we need to be aware in Cyber Security?

The concept of Cyber Security is, in a short definition, the security of all IT systems that a state, an institution, a person uses. What is most important is the close link that all these systems have, starting with the smallest unity, namely the individual or the end user.

In order to clearly determine the points we have to follow in this area, they are best highlighted in the Cybernetic Security Strategy of Romania and in the National Action Plan on the implementation of the national cyber security system, 2013. Thus, cyber security is It presents as the state of normality resulting from the application of a set of proactive and reactive measures to ensure the confidentiality, integrity, availability, authenticity and irreversibility of electronic information, public or private resources and services in cybernetic space. Proactive and reactive measures may include policies, concepts, standards and security guides, risk management, training and awareness activities, the implementation of technical solutions for protecting cyber infrastructures, identity management, consequence management. [3]

The cyber space is in fact the fifth battle territory in the 21st century, and the cyber security is a new meaning as the cybernetic component links the other battle, terrestrial, sea, air, space that was predominantly applicable during the war Cold.

The fully affected space in case of cyber conflicts is the global integrated communications and computer networks in which telecommunication infrastructures are also included. In addition, the virtual space includes the Internet and computer networks that cannot access through the Internet, which are separated, for example intranet. Cyber The space has as the main features lack of borders, dynamism and favors actions in anonymity, assigning a cyber-attack being a very complex process.

This concept of cyber security is organized on three layers, according to the unanimous opinion in the field, namely: staff of an entity, the processes that are carried out and technology used at all levels of that entity. [4]

So the first point in ensuring cyber security within an organization is staff and here is also the highest vulnerability. Creating an organizational culture is the best option to protect a computer system.

Cyber Security of staff is represented by behavior in the online but also internally, organizational, person. The uniqueness of a person can be used as a hackers' way of attack today, the fact that the equipment we use are increasingly connected, personally is a help and is at hand, but so a person becomes vulnerable, social media networks are connected, the phone is connected to the browser we use, so access to a single account can give access to all our equipment and possibly to an email account it uses within the organization where they work. Personified data that various accounts have can be used to get the passwords or answers of applications security questions. So it is advisable to hold an IT department capable of Cyber Security in the spectrum of staff training and, of course, respect for internal rules and legislation in force. [5]

Cyber Security at the level of activity refers to a code of conduct for any type of situation that may intervene, namely the steps that any employee must observe in the event of an error in the use of equipment. Documenting these procedures should clearly define roles, responsibilities and chain. Threats evolve, and a fair use can keep the organization safe.

Cyber Security at the technology is of course the widest branch that any entity has to develop. Investments in hardware technology (physical part of the equipment), as well as software (programs, applications) must be directly proportional to the value that the company represents, or the information it holds. Thus, the development of technology that technology has at these times can only come to the package with a level as high as possible vulnerabilities, referring to all uses of equipment for example, the frequency of electricity that enters a socket can become a signal that is repaid by a victim or attacker station, thus can destroy the information of storage units or may provide information to the attacker about the socket pattern if it can support high temperatures if it has sensors for current intensity or not, facilitating an attack of Hardware or a social-engineering type.

From an academic point of view, there is no unanimously accepted security definition, so a permanent revaluation of the methodology for analyzing this concept is relevant. The approach to establish a definition that includes the whole spectrum of threats, risks and vulnerabilities to security and to be accepted by all parties will be continuously as we are witnessing the complex phenomenon of globalization, the transformation of the national and international security environment given by the Technological innovations and not only, but also of the emergence of new asymmetric forms of war such as hybrid war, cyber war or human rights violations. The study of security and investing enormous resources for its insurance is not a novelty, the security being since the beginning of mankind one of the most precious things as it is even from Maslow's pyramid, where only physiological needs occupies a more important place. [6]

At the same time, although there is no current description of the cyber security or a framing of all offenses, as the field evolves, there is legislation at European level that should prevent incidents: The European Union adopted on July 6, 2016, the NIS Directive (Network Information Security) in order to increase the level of security of information and networks whereby this information circulates. The NIS Directive provides a legal framework for increasing the cyber security level by developing incidents response teams (CSIRT-Computer Security Incident Response Team) and a NIS competence authority. This directive encourages the exchange of information between Member States on the risks and threats that can affect a state. [7]

It is promoted security culture for our society in vital sectors such as the economy, critical infrastructure, the cyber espionage issue of the institutions and the exfiltration of data, targeting problems in areas such as energy, health, banking and digital infrastructures. Component undertakings of these sectors, which are identified by the Member States as providers of essential services for the company, will have to align the proposed concrete security measures and to transmit information on serious incidents, competent national authorities. Also, key digital service providers (search engines, cloud computing services and online markets) will have to comply with the new standards in terms of their own security requirements as well as users. [8]

In addition, there is a European Union Agency for this purpose in European territory to ensure compliance with cyber security. "The Commission has also proposed the creation of a stronger E.U. agency. Responsible for cyber security, starting from the existing structures of the European Union Agency for Networks and Information Security (ENISA). The role of the new agency would be to help Member States, EU institutions, as well as private enterprises to combat cyber-attacks. " [9]

Until now, ENISA has provided ITS security recommendations supporting the development of legislative articles and their implementation and has collaborated with operational teams across Europe. ENISA contributes to ensuring the information society of Europe by increasing awareness and developing and promoting a culture of network security and information in society, thus contributing to the smooth functioning of the internal market and implicitly to ensure national security.

On March 13, 2019, EU Ambassadors granted a mandate for the commencement of negotiations with the European Parliament in terms of the sharing of cyber security expertise. Negotiations will focus on two initiatives: the establishment of a peak knowledge base for cyber security, called the European Cyber Industrial, Technological and Research Center for cyber security and the establishment of a network of national coordination centers. [10]

From an international point of view, NATO declared the cyber space as an operational field as well as conventional spaces for wearing a war. This decision reflects the imminent adaptation to the evolutions of the 21st century and at the same time necessary in the history of 70 years of the Alliance and can be seen as part of a larger development in relation to the correlation of NATO measures with the current security needs that turn out once with the evolution of technology. In this respect, NATO members have decided to defend themselves from cyber-attacks in the identical procedural like against attacks launched in the other areas of war. NATO adapts to the evolution of the cyber line, being able to take pro-active measures against complex Cyber capabilities developed by both state and non-state actors. Cybernetic space is recognized as the integral part of today's wars, conflicts and crises today, but specifically is the basis of the current and future NATO operational security environment. [11]

Cybernetic field becomes an inseparable part in terms of the fundamental principle of NATO's collective defense. The need for concrete decisions at the 2016 Warsaw Summit and beyond it was led by the rapid growth of cyber threats and questions on the resilience of networks that is so much dependent on the society today. The incorporation of the virtual space into all other activities carried out by the Alliance, clarifies the cyber policy on Article 5, and the willingness to carry out cybernetic operations in broad spectrum is not just a future project for NATO but is a necessity in this dynamic, complex world and uncertain of our days. [12]

Declaration of cyber space as a conflict area states that cyber-attacks may be more easily used to justify the invocation of the Collective Defense Clause of Article 5, NATO. The Declaration also highlighted Member States that collective cyber resilience begins with its own countries, the cyber defense to be strengthened. Article 5 Specifies that only an armed attack on a Member State's security may rely on Article 5, and NATO is officially prepared to include complex cyber aggressions in the sphere of armed attacks. [13]

3. Asymmetric threat - Connection between Cyber Intelligence, Cyber Security, Cyber Warfare and Hacker Reinforcement.

Nowadays the damages that a war could cause is the most important reason that discourages the great powers from local conflicts, and excessive armed over-technology and modernization claims the idea that the next war will be the last.

Thus, large powers use other means to make their interests known or to sanction countries that do not respect international or geopolitical rules get too much zonal influence, namely hybrid warfare: destabilization of the population by Fake News and the media flooding False information, the imposition of sanctions from international fora or even cyber-attacks on government institutions. Although most of the time they are disguised in "personal" actions, most attacks are supported by a state actor.

In the cyber environment, the most frequent incidents are caused by crime, as each actor involved wants to take advantage of the vast possibilities offered by the virtual space. The defense of IT systems and networks is based on vulnerable protocols and emphasizes the detection of threats rather than eliminating them. Cyber-attacks are carried out with an unavoidable rapidity, putting a very high pressure on the technological and mental victim, because the part that defends must be successful in the specific actions undertaken, while the attacker needs to succeed once Defense systems or find breaches to achieve their goal. [14]

Cyber offenses being classified according to purpose and attackers: when the attacker is a state, the goal is spying or penetration and maintenance of access to the victim's defense systems called and APT (Advanced Persistent Threat), when the goal is financial resources Most of them are classical cyber criminals, namely hackers who have access to a private network of a company and make commercial espionage or encrypt all internal data asking various amounts for data recovery (Ransomware attack) or even copies all the company's data, not I am doing domestic damage, but they sell their data and customer data victim's data on Dark Web forums.

However, the technology is in full growing, and geopolitical realities are also changing, goals and even attackers can interleave, so a state actor that supports a hacker group can aim to obtain financial resources, etc.

The threat that a cyber-attack possesses is very strong from a functional point of view: the success of a cyber-attack can lead to ruin a whole economic branch of the victim state or to land the communications system or the energy.

Known cases: Stuxnet virus attack on Ukraine's energy network, malicious attack Petya throughout Europe.

Considering all these aspects, we can fit the phenomenon of cyber-attacks on an entity or state among asymmetric threats, considering the definition according to "asymmetry consists in refusing the rules of the fight imposed by the opponent, thus making any unpredictable operations." [15].

Thus, the most important aspect being the lack of any information on the moment, the target or the method of attack. So cyber-attacks and their use as a hybrid war form are very well motivated:

1. The cyber war is cheaper, because it does not require the involvement of troops or weapons in the classical sense;
2. The cyber war can be worn remotely, so without any movement that could be a logistic, physical or additional cost;
3. The starting costs of a cybernetic war are relatively low. At first, a computer is sufficient with internet connection, but later financial resources can become important depending on the ultimate goal;
4. Most attack instruments are cheap and at the disposal of each person, hackers can find pieces of program in lines on the Internet that they can later change;
5. The proliferation of cyber-type attacks cannot be controlled;
6. Attackers can take advantage of the latest innovations in the technological field;
7. Cybernetic space offers attackers anonymous because it is very difficult to watch the origin of an attack, the attackers operating behind false IP addresses or foreign servers;
8. The cyber war offers the ability to manipulate and disrupt the opponent, and is not necessary to carry out combat operations to achieve interests;
9. The cyber war allows state actors to achieve political and strategic objectives without actually beginning an armed or other conflict;
10. A cyber war takes place at a remarkable speed, the time between the launch of an attack and the experience of its effects is very low. This generates much more risks for decision-makers, especially in times of crisis.
11. The victim of a cyber-attack in the case of an institution must invest considerable resources for neutralizing threats. Teams specialized in software and hardware are needed, and these people are very difficult because they prefer the private environment.
12. The vulnerabilities of countries increasingly dependent on the interconnection of network information systems increase with the implementation of new technologies and can become targets for cyber opponents.

All these reasons transform the cyberspace into the most efficient and effective weapon that any state can have, as the required code lines can be written even on a phone.

4. ZERO TRUST POLICY - The new cyber security model

The increased need for cyber security and recrudescence of cyber-attacks have determined substantiation, especially in private environment, of a new cyber security concept, called "Zero Trust" - "Zero Trust".

This concept is a strategic initiative policy aims at preventing computer security breaches by eliminating the concept of "trust" in the network architecture of an organization. The basic principle of this policy "Never Trust, Always Verify" (never to trust, always check) is representative, being built to protect digital media by segmenting the network, both by preventing the lateral movements of the attacker's potential and by offering a pattern of level 7 threat to the OSI theoretical model, protecting high-level applications from the technologies present in the institution. [16]

The "Zero Trust" model was created by the need to secure network infrastructure, being the successor of traditional internal security models. These traditional models function, and many are still working on the erroneous principle that all infrastructure users are responsible for network, they are reliable, and their identities are not compromised, while maintaining network anonymity.

According to the new concept, any model aims at trust in the human component is from the very beginning an erroneous model, a proven aspect of many successful cyber-attacks through social engineering. This assumption is based on a perfectly natural human trait to overcome the different conditions and limitations imposed by infrastructure security rules, especially on the social component, either in a controlled digital framework.

Thus, the punishment or internal normative conditioning of the behavior of employees / network users denies a fundamental human trait (to challenge and interpret the rules and try to circumvent them), not being long-term viable and / or a larger group of people. [17]

In this respect, on the traditional model, once entered into the network, a malicious user can insert or exfiltrate any type of data, moving sideways in network architecture research. Given that the initial point of the attack is, most often, completely different from the target location, the internal network could be compromised by different ways of access, and the institution's trust policy will foster the presence of foreign or domestic malicious entity, not being prepared for defensive actions.

Therefore, in antithesis, the "Zero Trust" policy is not meant to increase confidence in the institution's internal system, but to completely remove it to build a alert thinking model for an inevitable security breach, regardless of the architectural model of the network.

The initiation of the approach is to identify a protection zone. This area is made up of services, data, assets and critical apps for the network and institution. Once this area identified, organization traffic is analyzed on that area. Identifying users and services using this plan is the pre-tackling of internal cyber security policies by using the Zero Trust. The institution is obliged by this method to keep track of all access points in the critical plan to cover its assets in the case of a security breach. The advantage is both the identification of vulnerabilities as well as the actors that can exploit them by tracking the network of network transit and analyzing disturbing factors.

From the time building "Zero Trust" policy around the protection area, it must be monitored and maintained in real time for possible non-included dependencies as well as for ways to improve policy.

Complementary security policy according to the "Zero Trust" method, it is also noted the advantage of outsourcing responsibility for securing individual applications to the companies that have built them.

A good argument to opt for this outsourcing is the security budget allocated to large firms such as Google, Apple, Slack, and the like. The security component, though impressive at the individual level in each of these, is eclipsed by the whole community. In other words, by managing the different security micro services at the level of each company, a high-level security specialization is achieved, impossible specialization to be achieved at a macro level within a single institution, either with substantial resources.

With regard to the cost of implementing a Zero Trust method, although the initial cost may be substantially, it is amortized within a relatively short term, given the possibility of accessing any network device, including personal devices of users. Also, the cost of the software is low, no longer the renewal of licenses for different operating systems, file management software such as the Microsoft Office package or VPN connectivity server management for remote work.

One of the greatest policy benefits "Zero Trust", apart from the security component, is the dynamics of architecture. The method is not dependent on a location, but involves the constant presence everywhere, so it cannot be imposed in a particular place, but must be proliferated throughout the working environment. In this respect, there will be certain files that can be accessed by certain users based on well-defined conditions that cannot exit the pattern established when drawing the defining lines for the security area mentioned above. A happy consequence of this policy is thus the freedom of movement of responsible staff within the institution, which manages to access the services and tools needed to carry out the activity anywhere in the world at any time. In this case, the above-mentioned traffic analysis will serve as the basis of all possible system vulnerabilities, observing atypical behaviors, influence factors and possible risk spaces to be managed in accordance with the needs of the institution at the initial assessment.

5. Conclusions

In the context of the latest cyber information, certain projections or trends in cyber security are preferable. We believe that technologies related to artificial intelligence and Machine Learning will become the main weapons in the following cyber-attacks, as the full range of information systems used becomes overcome to the power of these technologies.

Also, on the background of the pandemic, remote technological and labor developments, the new industrial system, the economic system will move to the 4.0 model where most people employed will be replaced by a previously scheduled industrial apparatus, which respected and repeats the chosen parameters. Thus, IOT (Internet of Things) will be increasingly exploited, and the remote work developed and the threats appear. [18]

The problem of the pandemic from a cyber point of view is the lack of a culture of safety and security regarding the general concept applied "work from home". More and more APT formations are appearing, with a clear financial purpose, starting ransomware attacks, which are also the most profitable for attackers. The most affected infrastructures by these attacks are medical institutions, already subjected to a multiplied stress compared to a normal period. This risk is also transposed among employees in most areas, in the context of the current restrictions and laws imposed. Phishing attacks have multiplied 11 times in 2020 compared to 2016, doubled from 2019. In addition, 75% of the companies in the world have been attacked by phishing attacks, 96% started by means of an e-mail, precisely because of this an organizational culture in the private environment, but especially in the environment of state institutions is absolutely necessary. Regarding the costs RISKIQ estimates that minute by minute in the business environment is lost about 17.000$ due to cyberattacks across the broad spectrum. [19]

The development of 5G networks (the fifth generation of Internet transfer speed) will take place worldwide and will increase the Internet speed at least 10 times. Therefore, 5G technology will facilitate interconnection of devices with each other, which will increase the number of cyber-attacks.

Thus, we believe that the cyber-space, the package with all its opportunities and risks, will become the next bathing field for international hegemony, and the actors involved will be in a larger number, attracted by the opportunities generated by the development of cyberspace.

Bibliography

[1] Mihai, I.C., Ciuchi, C, Petrică, G.M, Provocări actuale în domeniul securității cibernetice – impact și contribuția României în domeniu, Studii de strategie și politici – SPOS 2017, Nr. 4.

[2] Directive (Eu) 2016/1148 Of The European Parliament And Of The Council - 6 July 2016.

[3] Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică. (2013). Guvernul României.

[4] „What is Cyber Security? Definition and Best Practices" - https://www.itgovernance.co.uk/what-is-cybersecurity

[5] " What Is Cybersecurity? " - https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-works

[6]Diakun-Thibault, Nadia. (2014). Defining Cybersecurity. Technology Innovation Management Review. 2014.

[7] Mîrzac, A.L., & Stanciu, R. (2018). Legile securității cibernetice. Sysadmin Adjectiv-Gardienii datelor personale.

[8] ALBESCU, Alexandra & Perețeanu, Georgiana-Cristina. (2019). Cultura de securitate cibernetică în România. Revista Română de Informatică şi Automatică. 29. 75-84. 10.33436/v29i4y201906.

[9] [10] Reforma securității cibernetice în Europa, 2019 - https://www.consilium.europa.eu/ro/policies/cybersecurity

[11] Limnéll, J. (2016, June). Challenge for NATO-Cyber Article 5. Center for Asymmetric Threat Studies

[12] Brent, L. „NATO s role in cyberspace" - https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm

[13] Limnéll, J. (2016, June). Challenge for NATO-Cyber Article 5. Center for Asymmetric Threat Studies

[14] https://www.veracomp.ro/stiri/super-producatorul-care-da-un-sens-sintagmei-zero-trust-security

[15] Cf. Thomas POULIN, Les guerres asymétriques: conflits d'hier et d'aujourd'hui, terrorisme et nouvelles menaces», http://www.grotius.fr /guerres-asymetriques.

[16] https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture, 2021.

[17] Marsh, S. & Dibben, M.R. (2003). The Role of Trust in Information Science and Technology. Annual Review of Information Science and Technology (ARIST)

[18] Ion, M., Căruțasu, G., Tehnologiile smart, descriere de ansamblu și cadru legislativ, Romanian Cyber Security Journal, nr. 1, 2020.

[19] Maddie Rosenthal - Must-Know Phishing Statistics - https://www.tessian.com/blog/phishing-statistics-2020/#the-most-targeted-industries - 15.11.2021