The 15th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 12th-13th 2020

CYBER SECURITY - EVOLUTION AND OPPORTUNITIES

ȘESTACOV Andrei, Lecturer, PhD candidate*
MIHALCEA Petru, Lecturer, PhD candidate**

*, ** Military Academy of the Armed Forces "Alexandru cel Bun"

Abstract:

The research is designed to protect data and security of the organization as well as to ensure the confidentiality of the employees and partners in the context of a dynamic information environment prone to large-scale cyber-attacks in which cybercriminals are using increasingly advanced methods to implement attack vectors that are undetectable and difficult to neutralize.

Whether we are talking about large or small companies, public institutions and government agencies, this study provides with a series of recommendations on the secure use of social networks, as well as a minimum set of measures needed to prevent cyber-attacks, in order to reduce the damage caused in case of attacks. At the same time, it will examine the best practices in the online environment, effectively analyze the privacy settings of mobile devices and present some top tips for the secure use of social networks.

The research conducted in this study complied with the following minimum set of measures in order to prevent cyber-attacks, but also to reduce the damage caused in the event of attacks.

Key words: cyber security, attacks, prevention and detection of intrusions, DoS, DDoS, e-mail passwords, tools.

1. Introduction

Today, cyber security is an extremely important focus for both individuals and public institutions. We had an example, when several companies in the Republic of Moldova were subjected to cyber incidents, in violation of the security policies of the e-mail service, being sent messages after which they made money transfers in the name indicated in the messages - in fact, to the attackers of the respective systems. In other words, there is a growing awareness of the danger of cyber incidents, because people from those companies have attended some important training and mentioned that they would participate in events on this topic, one of which is Moldova Cyber Week, to minimize the risks of cyber security attacks / incidents in order to be as protected as possible. In my opinion, this is related not only to one person, but to the interaction of all users of the information environment, who do and do not do IT, because today we all own various mobile devices with sensitive data, we have personal data anywhere and we must protect it [1].

Increased attention is paid to both the ability to respond to cyber attacks and to the prevention and detection of intrusions into information networks. Confronting the phenomenon of cybercrime is a priority for users of information systems, both in terms of intrusions into corporate networks or in personal data, as well as in the case of identity theft or fraud. Prevention and detection attacks are a necessity for public authorities, which must have the capacity to protect the critical infrastructure on which users of the information environment rely on in their daily work [2].

2. Analysis of current challenges present in the field of cyberspace

Cyber attacks are one of the biggest threats to humanity! Cyberspace possesses a number of threats that can target a state's critical infrastructure, and information technology becomes so unpredictable that it can easily get out of hand. This is exactly what we intend to avoid or at least monitor and control, through the exchange of good practices, public consultations, involvement and daily improvement. "Cyber security is also about diplomacy when it comes to responding to digital threats. Moldova, being one of the signatories of the Association Agreement with the EU, is closely following the actions of the European partners in this regard and is trying to implement good practices [3]. The trend at the regional level in this field is the consolidation of legislation and legal norms, capacities, partnerships, and we want Moldova to be part of this process."

Cyber security is a common responsibility. In today's world of technology, many government and private sector entities consider a cyber security information-sharing alliance between the government agencies and private enterprises to be the main course of defense action against cyber attacks.

Solid cyber security capabilities cannot be built on myths. Cyber security is certainly not someone else's responsibility, and every employee trained to meet cyber security challenges will certainly strengthen the institution's potential for development and trust in the eyes of customers and the community as a whole.

Cyber security is the sole responsibility of experts in the field. It is absolutely wrong to entrust cyber security and integrity solely to the team of cyber security experts, since hackers are increasingly hunting down the employees of companies, which of course have their devices connected to the network. Respectively, it is the duty of every employee to know the main rules and minimum requirements of cyber security in order to prevent and react correctly to a security incident.

According to IBM Security Services, 95% of cyber attacks are due to human error. On the other hand, according to ISSA data, 82% of employers report a lack of cyber security skills.

Another study in the field of cyber security is about the ability and training of IT specialists to provide 100% protection against cyber attacks. In reality, IT specialists as well as the rest of the employees, who perform several tasks simultaneously, will often look for the easy way to fulfill their duties, sometimes even due to non-compliance with security rules and precautions.

According to Varonis, 56% of IT experts believe that phishing attacks are their main security threat, and continuous education is an effective way to reduce this risk. At the same time, 77% of organizations do not have a cyber security incident response plan (IBM Security Services) [4].

Cyber attacks occur only in the virtual world. Many of the attacks were caused by a simple electronic information storage device placed in an unattended laptop. Physical access can play a vital role in everything related to unauthorized access to information.

For example, for the global shipping giant "Maersk", an infected computer disrupted the activity of an entire "empire" with international experience and fame, or the "Stuxnet" worm that wreaked havoc on Iran's "Natanz" nuclear facility, delivered by a flash drive that has been connected directly to one of the installation's computers. These examples are proof that a large part of cyber incidents do not only happen in the virtual world, but are actually caused by physical access to an unsupervised system.

A new ransomware threat, called Nemty Ransomware, was recently discovered by malware researchers at FortiGuard Labs. Nemty aims not only to encrypt personal data stored on devices but also to delete their backups to make impossible any procedure to recover them.

Ransomware is a malicious program that encrypts files stored on the victim's devices, and to decrypt them, criminals demand a ransom that is almost always monetary. Payment is requested in digital currency, hosted by the TOR network for anonymity, and to make the payment, the victim receives a configuration file containing the victim's identity and the file decryption key.

According to researchers, Nemty Ransomware has a well-known structure built into its binary code, as it was also used by GandGrab ransomware, and the distribution process uses the same method as Sodinokibi, a malware that has strong similarities to GandGrab.

The name Nemty Ransomware comes from the extension it adds to the name of the encrypted files. Throughout the run, the structure of Nemty ransomware is encrypted using a simple combination of base64 algorithm encryption and RC4 encryption.

Currently, researchers at FortiGuard Labs have published a report containing the full technical analysis. Here it is stated that Nemty Ransomware uses a combination of AES-128 in CBC, RSA-2048 and RSA-8192 mode unusual for file encryption and key protection.

The causes of this malicious program include access to user attachments sent via spam emails or from unknown sources, installation of unlicensed software applications, downloading files from compromised websites, connecting various external storage devices infected, etc. [5].

In such circumstances, security engineers come up with the following safety recommendations:

- ✓ Back up data on computing devices by storing them on a separate disk or cloud;
- ✓ Do not open attachments from spam or unknown emails;
- ✓ Do not open links that appear in spam emails or text messages from unknown and dubious sources;
- ✓ Use antivirus software and update it regularly;
- ✓ Keep your browser up to date and apply security fixes;
- ✓ Do not grant administrator privileges to applications that do not inspire trust.

3. Identifying good practices on preventing and limiting the effects of cyber attacks

Across Europe, the 9th edition of the European Cyber security Month (ECSM) kicks off, the European Union's annual campaign to raise awareness of cyber security by providing up-to-date information on cyber security through education and the exchange of good practice, coordinated by the European Union Agency for Cyber Security (ENISA) and the European Commission, and supported by the Member States.

Every year, the Republic of Moldova joins the European initiative to promote cyber security among citizens and to ensure their information and awareness about the risks and threats that may arise.

The broad topics targeted by the 2020 campaign address the need to change behaviors and identify opportunities to help users recognize the risks involved in new technologies.

This study aims at tools and training to strengthen the capacity to respond to cyber attacks in the field of cyber security for public and private sector personnel. Cyber Security supports the priority of creating and implementing a cyber security plan. It has become a condition for the proper functioning of government systems in the context of new technologies. Study aims to strengthen capacities and activities in order to inform and raise awareness of the risks and consequences of cyber security [6].

Cyber dangers affect not only privacy, but also the public image of society and the state. In recent years, we have witnessed several election campaigns in different countries, in which certain

cyber attacks have been launched, which is the reason why the question arises about the importance of international security in reducing these threats in the information environment.

Government institutions are developing and strengthening internationally recognized standards. Companies around the world are actively involved in this regard, as well as the EU, working on risk assessment, initiating studies and global standards, collaboration schemes between various international institutions and based on them provide recommendations for IT service providers, operators of mobile telephony, for equipment managers, reaching in common a goal and a transparent basis that gives us confidence in these tools for preventing and detecting intrusions into information networks.

Cyber security is in many ways a race between source and destination. The source constantly analyzes the weaknesses, which can occur in different contexts of information attack. Destination must reduce weaknesses, among them particularly important and intentional by people inside the information system and previously unknown information threats [7]. However, in the case of some of the known vulnerabilities, to which there are solutions, they cannot be implemented in many cases due to budgetary or operational constraints.

4. Types of cyber attacks

Essential types of cyber attacks today are carried out through malware applications, by denying services (DoS, DDoS), by affecting e-mail tools and web applications, and the last category being represented by APT (Advanced Persistent Threat) attacks.

Malware attacks are the most common form of cyber attack:

- ✓ Trojans are applications that give the impression that they are performing legitimate operations, but in fact they are trying to explore vulnerabilities in the computer system and to open ports in the computer system operation to allow attackers access to the system;
- ✓ Adware is a type of application that installs in the operating system and transmits in aggressively advertises the user;
- ✓ Spyware is a type of application that secretly captures various information about Internet user activity;
- ✓ Computer viruses are applications with often destructive effects, designed to infect a computer system. Viruses have two main characteristics: they self-execute and self-multiply in the infected system [8].
- ✓ Computer worms are applications with destructive effects that infect the computer system and spread through the Internet. Worms are looking for computer systems with vulnerabilities infect and perform harmful operations, after which it tries to spread further.
- ✓ Ransomware is a type of malware that restricts access to the system computer or infected files and request a ransom for the restriction to be removed.
- ✓ Some types of ransomware encrypt data on the system's hard drive while others may simply block the computer system and display persuasive messages the user to pay.
- ✓ Rogueware security software is an application that misleads users to pay money for removal of false infections detected in the operating system. Most often, this type of application claims to remove malware found on computers, but in reality installs applications with destructive effect.
- ✓ Scareware is an application that causes users states of fear, anxiety and purpose to market certain fake applications [9].

Denial of Service (DDoS) attack has the effect of compromising the functioning of some Internet services. One of the most common DDoS attacks is the packet flood attack which sends a large number of packets to the victim system which has the effect of blocking open connections and loading network traffic, leading to interruption of services provided by the attacked system.

Attacks on e-mail have increased exponentially in recent times. Depending for the purpose of cybercriminals, e-mail attacks are of several types:

- ✓ Email bombing is the repeated sending of an email with large attachments dimensions to a specific email address. This attack fills the space available on the server, making the email account inaccessible.
- ✓ e-mail spoofing consists in sending e-mail messages with the sender's address modified. This attack is used to hide the real identity of the sender for find out the confidential details or data needed to access an account.
- ✓ Email spamming is an attack that consists of sending unsolicited emails with usually commercial content. The purpose of these attacks is to attract the recipients emails to enter certain sites and buy more products or services or less legitimate. Email phishing is an attack whose scale is increasing, consisting of sending messages in order to get email recipients to provide information about bank accounts, credit cards, passwords or other personal details [10].

Conclusion

As we become increasingly dependent on Information and Communication Technologies, in our digital societies it is important to recognize the value of cyber security in terms of confidentiality, integrity, availability and non-repudiation of information, so we all have a responsibility in terms of cyber space. The Republic of Moldova, like many nations in the world, is developing such cyber security strategies, this initiative also involves working with other states to share information on various risks and threats, so that we can all be prepared for this. It is, first and foremost, about the risk management, because we cannot eliminate all risks. It is very important for states, individual organizations, for key sectors, such as the internet service providers or the communication, mobile telephony, to understand what are the best practices in the field and to develop compliance programs so that customers, companies, states and other users - to understand the extent to which major service providers address these risks and threats in the information environment, so as to be sure that services provided at government or private level will be at an appropriate level.

In the general context of the cyber security debate, at national and international level, the conceptual separation of the main vectors of action is fundamental: cyber defense, security and national defense, critical infrastructure and emergencies, international cyber cooperation and information governance. Isolating is not the ideal situation, but it is a reality, due to the complexity and diversity of cyber security as a whole.

The tools, roles and responsibilities of each national and international institution need to be set out clearly and responsible.

A major area of interest that may be in the future is cyber risk assurance that covers the risks of attacks on critical infrastructure.

The gaps in cyber security system can affect institutions and organizations on several levels, both financially and reputably. Information assurance against the risks present in the virtual space could financially protect against losses in the event of cyber attacks.

References:

[1]Hotărârea Guvernului cu privire la Strategia Națională de dezvoltare a societății informaționale „Moldova Digitală 2020" nr. 857 din 31.10.2013 // Monitorul Oficial nr. 252-257 din 08.11.2013;

[2] Regulamentul privind asigurarea securităţii informaţionale şi utilizare a resurselor sistemului de comunicaţii şi informatică ale Armatei Naţionale prin Ordinul MA nr. 114 din 12 martie 2015, Republicii Moldova;

[3] Hotărârea Parlamentului pentru aprobarea Strategiei securităţii naţionale a Republicii Moldova nr. 153 din 15.07.2011 // Monitorul Oficial nr. 170-175 din 14.10.2011;

[4] Carol Woodbury, IBM i Security administration and compliance, 2016, 38 p.;

[5] G. Held, K. Hundley, Arhitecturi de securitate, Editura Teora, 2003.

[6] Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone, Computer Security Incident Handling Guide, NIST Special Publication 800-61 2012;

[7] Hsiao S.B., Stemp R., *Advanced Computer Security*, CS 4602, Monterey, California, 2006;

[8] ISO 27002:2005, Codul de practică al managementului securităţii informaţiilor;

[9] ISO 27001:2013, Sistem de management al securităţii informaţiei: specificaţii şi ghid de utilizare.

[10] Serviciul Tehnologia Informației și Securitate Cibernetică, multiple informaţii, https://stisc.gov.md/ro;