The 13th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 8th-9th 2018

CONTINUOUS FIGHT AGAINST CYBER-ATTACKS ON SENSITIVE DATA, BANKING AND FINANCIAL SYSTEMS

NITESCU Silvia Elena PhD. candidate
LUCA Mihaela Paraschiva PhD. candidate

"Lucian Blaga" University/ Doctoral Economic Studies/ Sibiu/ Romania

Abstract:
This paper considers the subject of cyber-attacks as one of the most worrying security issues that countries are confronting nowadays.
We describe the evolution of this concept, the main types of cyber-attacks and relevant examples in history and present days. We analyze the measures implemented by different countries and companies in order to counter-attack this form of aggression and its impact from an economic point of view.

Key words: security, cyber attacks, financial systems

1. Introduction

The use of technology has brought enormous advantages within all the fields of all industries. But in the same time the technological development comes together with a series of vulnerabilities speculated and exploited by actors as the states and other forms of organizations.

Cyber aggressions may affect the integrity, the confidentiality and the availability of the informatical systems. In the same time, they can lead to unavailability, degradation, the destruction and the malicious control of a system or IT structure, can destroy the integrity of data or can steal sensitive, confidential and restricted data, in order to use it in different scopes.

Cyber-attacks together with other conventional or nonconventional methods are part of a mix of instruments that international actors whom dispose of enough developed capabilities, start and maintain these forms of complex attacks, in order to gain strategical and financial advantage. Virtual space has become a battlefield. The states and the corporations have to constantly invest in this cyber-defense field in order to keep up with the newest protection methods. This is the reason why the world states finance alliances, and international organisms in order to develop ways of maintaining under control this dynamic phenomenon, and to protect the final users, who are the victims in this cyber war, together with all the companies and corporations that suffer great losses. [1]

This article is about the way cyber-attacks have constantly developed throughout history and about the constant and united fight that all countries have to sustain in order to fight against all forms of cyber aggression.

2. Types of Cyber-attacks on banking and financial system

Digital money, sensitive data and financial institutions are elements that have to be defined in order to understand the context of cyber-attacks.

Electronic money (also e-Money or **digital money**) are traditional currency in a digital format. They are issued by the government, are regulated and legal tender in the country of issue. The supply of money is fixed and controlled by the state (European Central Bank Report, 2012).

The following personal data is considered '**sensitive'** and is subject to specific processing conditions: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.[2]

Financial institution: any institution that collects money and puts it into assets such as stocks, bonds, bank deposits, or loans is considered a financial institution.

In order to complete their goals, the cyber attackers developed various programs and software which target storage devices, emails, login and password information, social network profiles, payment channels, important programs used by the institutions:

- **Viruses and worms** are computer programs that affect the storage devices of a computer or network, which then replicate information without the knowledge of the user.
- **Spam emails** are unsolicited emails or junk newsgroup postings. Spam emails are sent without the consent of the receiver — potentially creating a wide range of problems if they are not filtered appropriately.
- **Trojan** is a program that appears legitimate. However, once run, it moves on to locate password information or makes the system more vulnerable to future entry. Or a Trojan may simply destroy programs or data on the hard disk. Denial-of-service (DoS) DoS occurs when criminals attempt to bring down or cripple individual websites, computers or networks, often by flooding them with messages.
- **Malware** is a software that takes control of any individual's computer to spread a bug to other people's devices or social networking profiles. Such software can also be used to create a botnet a network of computers controlled remotely by hackers, known as herders to spread spam or viruses. Scareware Using fear tactics, some cyber criminals compel users to download certain software. While such software is usually presented as antivirus software, after some time these programs start attacking the user's system. The user then has to pay the criminals to remove such viruses.
- **Phishing** attacks are designed to steal a person's login and password. For instance, the phisher can access the victim's bank accounts or assume control of their social network. Targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.[3]
- **Fiscal fraud** -By targeting official online payment channels, cyber attackers can hamper processes such as tax collection or make fraudulent claims for benefits
- **State cyber-attacks** -Experts believe that some government agencies may also be using cyber-attacks as a new means of warfare. One such attack occurred in 2010, when a

computer virus called Stuxnet was used to carry out an invisible attack on Iran's secret nuclear program. The virus was aimed at disabling Iran's uranium enrichment centrifuges.

- **Carders Stealing** bank or credit card details is another major cyber-crime. Duplicate cards are then used to withdraw cash at ATMs or in shops. [4]

3. History of cyber-attacks from all over the world

All cyber-attacks start with a motivation, which is important to understand in order to properly protect the organizations and their customers. Cybercrime groups, scammers and even state sponsored APT groups have two key motivations for attacking a financial institution:

- ***The financial motivation***: high payoffs and the relatively low risk of detection are inspiring criminals to "go online". The probability of getting caught hacking a bank is considerably lower than physically robbing it.
- ***The Cyber Warfare / Cyber Terrorism motivation***: It is a way of creating fear, just like a terrorist attack. In the same time it conducts to financial damage. This is considered an act of war.

Some of the most significant cyber-attacks in history:

a) The Morris worm is one of the first network worms distributed over the Internet. Written by a graduate student at Cornell University Robert Tappan Morris and launched on November 2, 1988 at the Massachusetts Institute of Technology. The damage from the Morris worm was estimated at about $ 96.5 million. [5]
b) The computer virus "Chernobyl", also known as "Chih" and CIH, was the first malicious program that was able to damage the hardware of the computer—the Flash BIOS chip. The virus first appeared in June 1998, and since then its epidemic has not stopped.
c) The Mafiaboy virus, which spread in 2000, is one of the first full-scale DDoS attacks (distributed denial of service) via the Internet servers of large companies. Attacking several well-known sites, including Yahoo, Fifa.com, Amazon, Dell, eBay and CNN, began a Canadian high school student. The damage amounted to approximately $ 1.2 billion.
d) ZeuS—Trojan program, which appeared in 2007, is the first case in the history of malicious software distribution through social networks. Facebook users were sent several photo messages, which were redirected to sites with the ZeuS virus. Then the Trojan program was introduced into the system, intercepted the user's registration data, which made it possible to steal funds from the accounts of customers of leading European banks. The virus attack affected Spain, Italy, Germany and the Netherlands. Attacks were not only the victim's personal computer, but also mobile devices.[6]
e) StuxNet is the first military-use virus and the first really used cyber weapon. He attacked the industrial systems that controlled the production processes in 2010. StuxNet disabled Iran's nuclear facilities, physically destroying the infrastructure: then up to 20% of Iran's nuclear centrifuges could suffer (one of the Iranian enterprises in the photo).
f) The Lazarus virus in 2014 led to a large-scale leak of personal data from Sony Pictures employees, e-mails and unreleased film studio films. The losses of the company were

estimated at $ 100 million (of which $ 83 million—due to the loss of the films being prepared for rental). It is believed that the attack on the servers of Sony was carried out by the cyber group Lazarus, associated with the government of North Korea.[7]

g) The famous virus-encryptor WannaCry in May 2017 attacked 200,000 computers in 150 countries around the world. The damage was estimated at $ 1 billion. The virus penetrated computers with a Windows operating system, where no updates were installed, encrypted the contents of hard disks and demanded $ 300 for users to decrypt. However, two months later Hutchins was arrested in the US on charges of spreading another malicious program—Kronos. With the help of this virus in 2014–2015. Cyber-fraudsters successfully stole bank card data. [8]

In Romania, cyber criminals are mainly aiming to obtain financial gains from online sales and banking systems, by means of cyber operations, employing a wide variety of methods, including phishing, spamming, social engineering, skimming, carding, as well as hacking techniques against targeted computer networks or personal workstations. Next to state and crime involvement, hackers may have a large variety of motivations ranging from sheer misplaced (usually juvenile) assertiveness to some forms of ideological-type convictions.

- Operation PENE - organized crime group specialized in electronic frauds, comprised by 24 that defrauded almost 350 persons from the US, Canada and UK, causing losses of over 8mil. USD
- Operation PĂUNESCU - a crime group led by Mihai-Ionuţ Păunescu whose purpose was launching cyberattacks against various financial/banking institutions in the US, like United States Postal Services and Bank of America, causing losses of approx. 240 mil. USD.
- Anonymous Romania, starting January 2012 launched a high number of cyber-attacks against national public institutions. They have also been involved in initiating cyber-attacks on foreign entities from the US, Czech Republic, Serbia, Poland and Brazil. Anonymous Romania also supported Anonymous International in attacking various IT systems outside Romania. [9]

4. Concrete measures taken to counter continuous cyber attacks, actors involved

Many cybersecurity incidents, either intentional or accidental ones, in recent years, showed an increase in threats from cyberspace. On the public agenda of governments infrastructure protection at the state level has become a priority.

The **European Union** has taken a number of concrete measures to enhance the level of preparedness in cybersecurity field [10], such as:

➢ It has adopted the *European Strategy for Cybersecurity* [11], with objectives derived from the European regulations in the field, contributions from Member States and private sector as well. All 28 European Union Member States have developed national cybersecurity strategies. Both European strategy and national strategies for cybersecurity have common objectives, namely: a unified approach to cybersecurity, collaboration and continuous updating of policies and concrete actions to reduce cybercrime, developing capabilities for cyber defense to ensure the security of European cyberspace;

- On April 27, 2016, the Parliament and the European Council adopted the *Regulation on the processing of personal data and the free movement of such data* [2], which establishes the rights guaranteed to persons whose data are processed, as well as the obligations personal data controllers have;
- It adopted on July 6, 2016 *NIS Directive* No. 1148 (Directiv on Security of Network and Information Systems) on security of network and information systems [12]. The Directive establishes measures to be taken by each Member State on:
  - adopting a national strategy on security of networks and information systems;
  - establishing the competent authority, respectively of a single point of contact at national level on the security of network and information systems;
  - ensuring receipt of incident notifications in accordance with NIS Directive.
- On December 20, 2017, the EU institutions have established a permanent *Response Center to Cybersecurity Incidents (CERT-UE)* [12] for all institutions, bodies and agencies of the European Union, strengthening the existing operational group, transforming it into a permanent and effective team, responsible for ensuring a coordinated response of the European Union to cyber attacks against its institutions.
- In October 2018, the European Council called for adopting a common approach to EU in the field of cybersecurity, following the reform package proposed by the European Commission [13], namely:
  - creating a stronger European Union agency responsible for cybersecurity;
  - establishing a wide cybersecurity certification system at the level of the entire European Union for products, services and processes of information and communication technology (ICT). This proposal is known as the "law on cybersecurity".
  - rapid implementation of the Directive on NIS.

Romania has adopted by Government Decision No. 271 of 2013 *Cybersecurity Strategy and National Action Plan on Implementation of the National Cybersecurity System* (SNSC) [14]. The purpose of the strategy is to establish and maintain a secure cyber space, by complying with the National Defense Strategy and the National Strategy of critical infrastructure protection.

The national cybersecurity system has the role of "overseeing coherent implementation of all measures to prevent and respond to cyber attacks against public institutions or private companies and brings together public authorities and institutions with responsibilities and capabilities in the field" and it includes:

- public authority with expertise in the field, such as Romanian Intelligence Service, Ministry of Defense, Ministry of Interior, Ministry of Foreign Affairs, Ministry for information Society, Special Telecommunications Service, Foreign Intelligence Service, Protection and Guard Service, National Registry Office for State Classified Information, Secretary of Supreme Council of National Defense;
- participants from the private, professional and business sector.

The main national bodies responsible for cyber security are:

- Supreme Council of National Defense – the authority coordinating SNSC activity at strategic level;
- Romanian Government through Ministry of Communications and Information Society - it ensures the coordination of the other public authorities in order to implement

government strategies in the field.

In the spirit of commitments assumed, in order to comply with the requirements of the European Strategy for Cybersecurity, Directive NIS and public - private partnership in the area of cybersecurity, Romania has constituted an interinstitutional working group coordinated by the Ministry of Communications and Information Society, for updating and promoting the draft of Cybersecurity Act and for transposing NIS Directive.

5. Impact on economy, investments in software development, training human resources, development of public administration departments, the emergence of entities within or outside their companies, incurred losses and impact on economic indicators

Worldwide, estimates show that losses caused by cyber risks are amounting to almost 0.5% of world GDP and are about twice more than the average annual losses caused by natural disasters.

The Geneva Association, in the study published in the April 2018 *Understanding and Addressing Global Insurance Protection Gap* [15] considers cyber risk as the biggest challenge facing modern economies.

According to the *Report on Cyber Threats Evolution in 2016* [16] published by the National Center for Response to Security Cybernetics Incidents (CERT-RO) "Romania is both a country generating cybersecurity incidents and with the role of proxy (transit) for attackers outside the national space through the use of vulnerable or compromised information systems that are part of national cyberspace".

The number of cyber security alerts nationally processed by CERT-RO has evolved as follows:

Year	**Number of alerts**
2013	43.231.599
2014	78.769.993
2015	68.206.856
2016	110.194.890
2017	138.217.026

Table 1

The evolution of cyber attacks in 2017 compared to 2016 is as follows:

	2016	**2017**
Total unique IPs involved in at least one cyber security alert processed by CERT-RO	2.92 mil (38.72%)	2.89 mil (33.71%)
Alerts aiming information systems infected with botnet malware (it has mechanisms that allow attackers to remotely control infected systems)	14.12 mil (12.81%)	8.17 mil (5.88%)
Domains web.ro reported as compromised	10.639	1.709

Table 2

Of total alerts processed by CERT-RO:

- 115.6 mil (83.63%) targeted vulnerable, outdated, insecure, poorly configured information systems;
- 14.33 mil (10.32%) targeted compromised information systems.

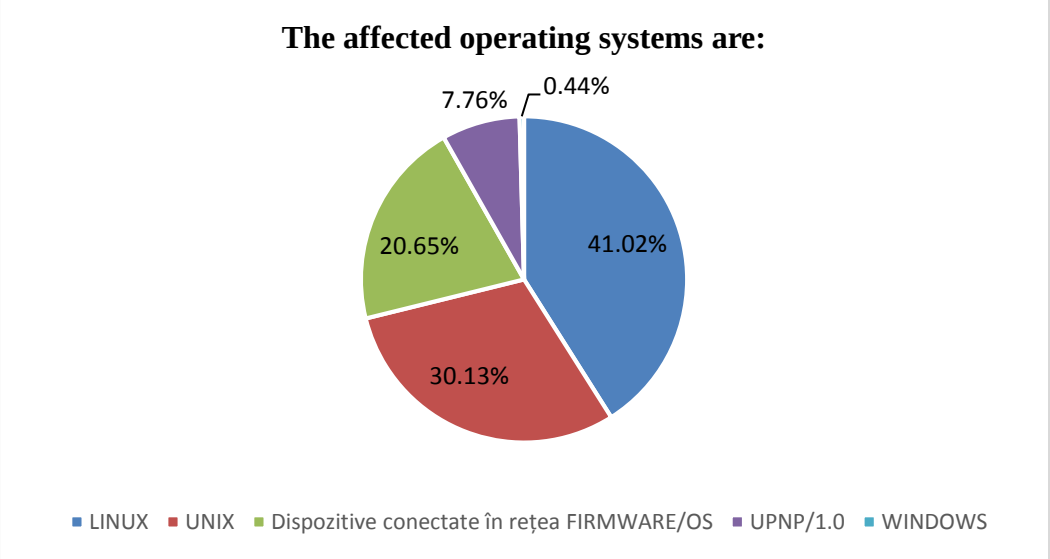

Fig.1

According to the study *Global State of Security Survey* [17] conducted by Pricewaterhouse Coopers (PwC) in 2018, on a total of 9,500 executive and IT directors in 122 countries, many organizations fail to ensure the protection of data confidentiality: only 51% of executive directors have a statement of personal data of employees and customers and only 53% perform compliance audits on customer and employee data management.

Companies involved in PwC study adopt advanced authentication technologies, such as:

Biometrics	60%
Software tokens	59%
Hardware tokens	55%
Cryptographic keys	53%
Multifactor authentication	51%
National IDs and ePassports	50%
Smartphone tokens	48%
Other	20%

Table 3

A percentage of 46% of those who contributed to performing the study said they plan to increase investment in advanced biometric authentication technology this year in order to increase data security.

Reducing the risks of cyber attacks involves responsibilities from both the heads of the institutions and companies and their employees. An important role will have cyber insurance.

Financial Supervisory Authority (ASF) maintains in *Report on Thematic Analysis on Cybernetic Risk Insurance* " [18] the development of cyber insurance products, both through policies at national and sectorial level". To this end, in 2018, InsurTech Hub working group was established within ASF, which proposed the establishment of a strategy in this area that shall provide know-how and shall provide specific educational programs for implementing the strategy. Currently, of the 16 insurance companies in Romania only two hold cyber risk insurance products

in their portfolio.

It requires awareness that insurance can take the risks to which public institutions, private sector, professional or business are exposed, at the same time representing a means of supplementing the cyber risk management framework. In addition, European requirements regarding cyber risks must be implemented at national level, as well as educating the Romanian companies on cyber risks.

6. Conclusions

Cyber attackers are constantly gaining know-how and trying new emproved methods to reach their objectives. There is a neverending war that all countries have to fight against this current. Only when all strategies come toghether in this fight, there is the chance to be able to prevent major demage.

After the analysis of the information above, there result the following actions to be taken to better manage the risks of continuous cyber attacks:

- involving high specialized up to date with specific legislation professionals wihin the state and all companies dedicated departments;
- a common platform where all professionals cand work together in order to fiind best solutions to be implemented in order to prevent and counter cyber attacks;
- actions to create awareness of the risks to which civil society, public, private or professional sectors are exposed to by the breach of minimum cybersecurity rules, and education on how to act in situations when they were targeted by cyber attacks;
- organizing media campaigns within the authorities public space, with responsibilities in cyberspace, focusing on legislative steps taken by them, as well as with concrete measures taken against those found to have launched cyber attacks, the ultimate goal being to increase confidence in the powers of authorities to effectively manage national cyberspace;
- the take-up and implementation at national level of the European requirements on actions to be taken to reduce cyber-related risks, which implies an updated national legislation on cyber security, transparency and cooperation at European level.

References:

[1]. Diana Olar, *Romania in fata inamicilor cibernetici*, 2017, http://intelligence.sri.ro/romania-fata-inamicilor-cibernetici/ (Romania facing cyber enemies, Intelligence.sri.ro /romania–face-cyber-enemies)

[2]. *Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)* (*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Regulation on data protection*)

[3]. https://www.phishing.org/what-is-phishing

[4]. Dr. Manisha M. More, Meenakshi P. Jadhav, Dr. K. M. Nalawade, 2015, *Online Banking and Cyber Attacks: The Current Scenario*
[5]. Timothy B. Lee, 2013, The Washington Post, https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its knees/?noredirect=on&utm_term=.5b631824ec8d
[6]. Resource Center Kaspersky.com, *Zeus Virus,* https://usa.kaspersky.com/resource-center/threats/zeus-virus
[7]. Kim Zeter, 2016, https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company/
[8]. https://medium.com/@LevelNetwork/10-major-cyber-attacks-in-the-history-of-mankind-cd6d53f5361c
[9]. Serviciul Roman de Informatii , *Cyber Threats, a Romanian Perspective*, 2013, https://info.publicintelligence.net/Romania-CyberThreats.pdf
[10]. Ioan-Cosmin Mihai (coordonator), Costel-Ciuchi, Gabriel-Marius Petrică, *Provocări actuale în domeniul securității cibernetice- impact și contribuția României în domeniu*, Institutul European din România, Studii de strategie și politici –SPOS 2017, (*Current Challenges in Cyber Security Field - Impact and Romania's Contribution in the Field*, European Institute of Romania, Strategy and Policy Studies) No. 4, page 38-55;
[11]. *ENISA (European Union Agency for Network and Information Security) Strategy 2016-2020*, January 2016, https://www.enisa.europa.eu/publications/corporate/enisa-strategy;
[12]. *Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune*, JO L 194, 19.7.2016; (*Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common security level of networks and information systems in the Union*)
[13]. *Reforma securității cibernetice în Europa*, www.consilium.europa.eu/ro/policies/cyber-security (*CyberSecurity Reform in Europe*)
[14]. *Hotărârea Guvernului Nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică*, of May 15, 2013, published in the Official Gazette of Romania, Part I, No. 296 of May 23, 2013; (*Government Decision No. 271/2013 for the approval of the Cybersecurity Strategy of Romania and the National Action Plan on the Implementation of the National Cybersecurity System*)
[15]. *Understanding and Addressing Global Insurance Protection Gaps, The Geneva Association, April 2018*, https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/understanding_and_addressing_global_insurance_protection_gaps.pdf
[16]. *Raportul privind evoluția amenințărilor cibernetice în 2017*, CERT-RO, 2017, https://cert.ro/vezi/document/raport-alerte-2017
[17]. *Global State of Information Security® Survey* 2018, PwC, CIO și CSO, April -May 2017,
[18]. *Raport privind analiza tematică referitoare la asigurarea de risc cibernetic*, https://asfromania.ro/files/analize/Asigurari_risc_cibernetic.pdf (*Report on the Thematic Analysis of Cyber Risk Insurance*)