SARA Law **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2821 – 4161 (Online), ISSN 2810-4188 (Print), ISSN-L 2810-4188
N°. 1 (2022), pp. 235-243

PREVENTION OF COMPUTER CRIME THROUGH KNOWLEDGE OF THE CONCEPT OF CYBER SECURITY

I.-A. POP

Ionuț– Andrei POP
European Police Union "Europol" - vice president
Expert P2 - Publisind Federation within the project "Strengthening the professional capacity of employees through digitalization", contract POCU 860/3/12/142833
Email: ionut.andrei.pop@gmail.com
ORCID ID: https://orcid.org/0000-0002-9219-7650

Abstract

The purpose of this article is to make the reader aware of the concept of cyber security and of the importance of establishing cyber data protection systems that we currently manage. Cyber-attacks have experienced a continuous upward trend in recent years, being targeted at both personal computer systems, computer systems managed by companies or computer systems managed by state institutions, as such cyber security has become a necessity for any user, provider, or consumer of cyber data.

Key words: *cybersecurity, cybercrime, cyber, security, crime, data, protection.*

INTRODUCTION

To understand the concept of cyber security, we must look at the evolution of digital technologies in recent years. It is easy to see that on all levels (personal, business, economic, financial, entertainment, state, etc.) the digitization trend has an accelerated crescendo.

Digitization has the potential to offer solutions for many of the challenges faced by the society we live in today and offers opportunities among the most varied, such as: changing the work paradigm from a spatial or temporal perspective (now you can work from anywhere at any time, you have you only need a computer device with a high-speed internet connection), the promotion of new educational methods and techniques (online school), the expansion of the commercial potential of companies through online commerce, the facilitation of citizens' access to public services of the state through the digitization of government institutions/ state, etc.

At the European level, the Council of the European Union gave an additional impetus to accelerate the technological transition, and to determine the member states to enter the process of institutional digitization, processes financed by the European Council through the National Recovery and Resilience Plans[1] (consilium.europa.eu).

At the European level, the first steps have been taken to protect citizens, companies, and institutions by establishing new mandatory rules on cyber security for products with digital elements throughout their entire life cycle[2] *(digital-strategy.ec. europa. I).*

1. WHAT IS THE CONCEPT OF "*CYBERCRIME*"

The Internet is an important part of our daily lives. We listen to music through streaming apps, read books using e-books, and watch our favorite video content. The Internet is also the main place where we shop, organize our lives, and perform important daily tasks such as paying bills and managing bank accounts.

However, no matter how carefully integrated the online environment is in our daily lives, cybercriminals are always nearby. We can find them on our favorite websites, in our emails, on social media platforms, video streaming.

In its simplest form, cybercrime includes anything illegal that takes place on the Internet through a computer or similar device. It is most related to hacking, but can also be used in financial fraud, data theft, harassment.

Cybercriminals are intelligent people with extensive knowledge of how online systems work. Not only are they capable of exploiting websites, encoding dangerous attacks like ransomware, and destroying other people's devices, but they are also adept at convincing unsuspecting victims to do what they want, willingly provide personal or financial information.

It is very likely that most people who are active in the online environment have already faced cybercrime attempts. It is very likely that in the e-mail address of each user there are e-mails marked as spam, which have corrupted content (virus) or which urge the user to various actions, which once executed will provide the cyber-criminal with all the data he needs for to complete their cyber-attack[3] (uk.norton.com). Phishing, ransomware, and data breaches are just a few examples of today's cyber threats, while new types of crimes and cyber-attacks are constantly emerging. Cybercriminals are increasingly agile and more organized, exploiting new technologies, adapting their attacks, and acting in new and increasingly novel ways[4] (*interpol.int*).

[1] https://www.consilium.europa.eu/en/your-online-life-and-the-eu/
[2] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[3] https://uk.norton.com/blog/how-to/what-is-cybercrime-how-it-works-and-how-to-stop-it
[4] https://www.interpol.int/Crimes/Cybercrime

Cybercrime goes even further as it can also include malware, or malicious software, which can wreak havoc on a user's life by encrypting all important files so they cannot be accessed, or by remotely installing a file to steal personal information such as passwords and credit card numbers.

Cybercrimes know no national borders, the victims and the technical infrastructure are spread globally, in several jurisdictions, in different legal systems, bringing many challenges to criminal investigations and prosecutions.

2. THE MAIN TYPES OF CYBER SECURITY THREATS

1. ***Phishing*** is the practice of sending fraudulent emails that look like emails from reputable sources. The goal is to steal sensitive data such as credit card numbers and login information. It is the most common type of cyber-attack. You can help protect yourself through education or a technology solution that filters out malicious emails[5] (*ncsc.gov.uk*).
2. ***Social engineering*** - Social engineering is a tactic attackers use to trick you into revealing sensitive information. They may request a cash payment or gain access to your confidential data. Social engineering can be combined with any of the other threats to get the person to click on links, download malware, or trust a malicious source[6] (*imperva.com*).
3. ***Ransomware*** - Ransomware is a type of malicious software. It is designed to extort money by blocking access to your files or computer system until the ransom is paid. Paying the ransom does not guarantee that files will be recovered or that the system will be restored[7] (*checkpoint.com*).
4. ***Malware*** - Malware is a type of software designed to gain unauthorized access or cause damage to a computer[8] (*rapid7.com*).
5. ***Backdoors*** - any malware, virus or technology used to gain unauthorized access to an application, a system, a network, bypassing all implemented security measures. Unlike other types of viruses/malwares, backdoor attack elements reach the core of the targeted application and often drive the targeted resource as a key driver or administrator[9] (*wallarm.com*).
6. ***Formjacking*** - Formjacking attacks are designed and executed by cybercriminals to steal financial and banking details from payment forms that can be captured directly on the payment pages of e-commerce sites [10] (*loginradius.com*).
7. ***Cryptojacking*** - is a threat that embeds itself in a computer or mobile device and then uses its resources to mine cryptocurrencies. Cryptocurrency is

[5] https://www.ncsc.gov.uk/guidance/phishing#section_2
[6] https://www.imperva.com/learn/application-security/social-engineering-attack/
[7] https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/
[8] https://www.rapid7.com/fundamentals/malware-attacks/
[9] https://www.wallarm.com/what/what-is-a-backdoor-attack
[10] https://www.loginradius.com/blog/identity/what-is-formjacking/

digital or virtual currency, which takes the form of tokens or "coins". The most well-known cryptocurrency is Bitcoin, but there are about 3,000 other forms of cryptocurrency, and while some cryptocurrencies have ventured into the physical world through credit cards or other projects, most remain virtual [11] (*kaspersky.com*).

DDoS (distributed denial-of-service) attacks - Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves several connected online devices, known as a botnet, which are used to flood a target website with fake traffic, causing it to be blocked for a period[12] (*imperva.com*).

3. GROWING THREATS PROMPT NEW LEVELS OF ACTION

3.1. Growing threats

The high-profile cyber-attacks in industries and governments last year increased the need for cyber security and generated an essential risk management for most people with executive functions in the business environment as well as around state institutions. Growing threats during the pandemic have added business risks to manufacturers from the point of view of ransomware[13] (*csis.org*). Most Western companies report phishing or ransomware security incidents in the past 12 months

82% of Western companies have already taken steps to increase their budgets by committing to invest more in cyber security in 2022, with almost a quarter allocating financial resources, at least 10% more than in 2021. An expanding attack surface from the connection of operational technology (OT), information technology (IT), from the perspective of external networks, it was found that they require more security measures. Outdated systems and technology were not suited to the sophisticated challenges of today's online environment from a security systems perspective[14] (*Devin Partida, 2021*).

As threats also increase with workforce displacement, the need for cyber security inside and outside organizations is ever greater, literally vital, in today's business architecture. It is vital for the cyber security of companies that they designate point persons responsible for cyber security procedures, being an essential responsibility at the company level. Zero-trust security measures that require authentication and restrict access can be part of prevention. Vigilance

[11] https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking

[12] https://www.imperva.com/learn/ddos/denial-of-service/

[13] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[14] Devin Partida, "Who's responsible for cybersecurity in industrial and manufacturing settings?," *Occupational Health & Safety*, August 24, 2021.

requires retooling, employee training, and oversight within and across departments[15] (*Gerry Grealish, 2021*).

3.2. The main protective actions against cyber attacks

In today's world, cyber security must be treated with maximum attention, responsibility, and professionalism, especially in the context where the traffic of personal or confidential data is continuously increasing. With ever-increasing threats to individuals, businesses, or state institutions, having a robust security solution is essential.

There are simply too many security threats to ignore the risks – from ransomware to phishing, they can all affect the integrity and privacy of a computer system. Prevention is key and, in this article, we are trying to identify some common and effective ways to prevent cyber-attacks.

a) Continuous documentation and training of employees on security risks

One of the most common ways in which cybercriminals have access to computer data is through employees or even the user of the computer system (in the case of natural persons). They will send fraudulent emails impersonating a person in the target's organization or entourage and request either personal details or access to certain files. Links often look legitimate to the uneducated eye, and it's easy for anyone to fall into the trap. Therefore, employee awareness is vital.

One of the most effective ways to protect ourselves against cyberattacks and all types of data breaches is to implement a system of ongoing employee training on cyberattack prevention[16] (leaf-it.com).

Verification actions:

- Checking links before accessing them
- Checking the e-mail address in the received e-mail
- If a request seems strange, it probably is, as a result, it is necessary to verify and confirm the request through a phone call (or any other means of direct communication) with the person concerned before acting on the "*request*"

b) Keeping software and systems fully up to date

Often, cyber-attacks occur because the systems or software used are not fully updated, leaving weak points that become security breaches. Consequently, cybercriminals will exploit these vulnerabilities to gain access to the network. Once they have entered, it is often too late to take measures to counter, stop or limit the attack.

To counter this, a smart move is to invest in a patch management system that will handle all software and system updates, keeping your system resilient and up to date.

---

[15] Gerry Grealish, "The pace of government won't fix cybersecurity," Industry Week, September 3, 2021.

[16] https://leaf-it.com/10-ways-prevent-cyber-attacks/

c) Terminal protection

Protection of all devices (*terminals*) interconnected in the internal network, protects the networks by making it difficult to connect remotely, through Internet networks, to the devices. Mobile devices, tablets and laptops that are connected to internal networks provide access points and pose security threats. These paths must be protected with specific endpoint protection software [17] (*cybermagazine.com*).

d) Installing a Firewall

Placing your network behind a firewall is one of the most effective ways to defend against any cyber-attack. A firewall system will block any brute force attacks made on the network or systems.

A firewall helps protect your computer systems by blocking unauthorized network traffic or access. It also provides an additional layer of protection against malware and viruses, which hackers commonly use to gain access to systems.

That being said, it is recommended to install and enable a strong firewall on your networks. One can start by enabling the basic firewalls that come with most computers (*Windows Firewall and Mac Firewall*) as well as on your Internet router. While it might not seem like much, it certainly deters a hacker from accessing your network's data and computer systems[18] (*purplesec.us*).

e) Frequent data backup

In the event of a cyber-attack, you must have data backups to avoid data loss and significant financial losses.

Cases of ransomware attacks have been on the rise in the recent past. Cybercriminals use ransomware to encrypt data and block access to computer systems, making it virtually impossible to modify or access any data. The hackers then force the victims of the attack to pay a certain amount (in the form of a ransom) in order to be able to access the data and systems again. Ransomware attacks can occur even if the latest protection systems are installed, or a firewall or antivirus is active.

One way to avoid such inconveniences is to perform regular data backups as often as possible. In this way, a backup solution will be implemented in case an attack happens and data is lost. Plus, it's much easier to restore data from a clean backup than paying a hacker for a decryption key[19] (*mightygadget.co.uk*).

f) Controlled access to computer systems

One of the attacks that can occur on computer systems can be of a physical nature. The possibility of unauthorized access by plugging a USB key containing infected files into one of the computers on the network, allowing it to access or

[17] https://cybermagazine.com/cyber-security/top-10-ways-prevent-cyber-attacks
[18] https://purplesec.us/resources/prevent-cyber-attacks/
[19] https://www.wallstreetins.com/blog/post-2/

infect the entire network, must be eliminated. Installing a perimeter security system is a great way to stop cybercrime as much as break-ins (*wallstreetins.com*).

g) Security of Wi-Fi networks

Any device can get infected by connecting to a Wi-Fi network, if this infected device has unrestricted access to the entire network, then the entire system is at serious risk.

Securing Wi-Fi networks and hiding them is one of the safest actions you can take to protect your computer systems. With wireless technology developing more and more every day, there are thousands of devices that can connect to a Wi-Fi network that they can compromise[20] (*mightygadget.co.uk*).

h) Establishment of personal accounts for employees.

Each employee needs their own login for each application and program. Multiple users logging in under the same credentials can put the network at risk.

Having separate logins for each staff member will reduce the number of attack fronts. Users log in only once per day and will only use their own set of login credentials[21] (*upguard.com*).

i) Access management

Controlling access to established policies and data can also help protect your most valuable information and data. With an access management system in place, staff can only be assigned the data they should be accessing, making everything inaccessible.

In addition, access management records every action that staff take while accessing these files as well. This also means that one can grant or deny the ability to access, copy, print or even delete files. With this approach, the authorization required to access certain files and data must be identified. Although it may seem a bit harsh, enforcing administrator rights and blocking staff from accessing or installing applications or data will go a long way towards increasing your resilience against cyber-attack[22] (*mightygadget.co.uk*).

j) Establish strong and different passwords for each device

Having the same password set up for all devices or apps can be dangerous. Once a hacker discovers the password, they will have access to everything on the computer system and any application used. Password cracking technology has advanced a lot, and simple passwords are a major vulnerability. Instead, complex passwords should be used, and multi-factor authentication strategies implemented to deter cybercrime. Also, password sharing between employees should be

[20] https://mightygadget.co.uk/10-ways-to-prevent-cyber-attacks/

[21] https://www.upguard.com/blog/reduce-cybersecurity-risk

[22] https://mightygadget.co.uk/10-ways-to-prevent-cyber-attacks/

discouraged so that even if one desktop is hacked, the rest remain secure[23] (*upguard.com*).

CONCLUSIONS

Data plays a critical role in the commission of many cybercrimes and generates the main vulnerabilities to cyberattacks. Even though data offers its users (individuals, private companies, organizations, and governments) countless opportunities, these benefits can be (and have been) exploited by some for criminal purposes. More precisely, the collection, storage, analysis and sharing of data allow the commission of a wide range of cybercrimes, especially when these operations are carried out by neglecting, voluntarily or involuntarily, the legal means of protection by establishing optimal security protocols.

In addition, the aggregation, analysis, and transfer of data is occurring at a scale that governments and organizations are unprepared for, creating several cybersecurity risks.

Privacy, data protection and security of systems, networks and data are interrelated. With this in mind, to protect against cybercrime, security measures are required that are designed to protect user data and privacy and prevent cyberattacks.

BIBLIOGRAPHY

https://www.consilium.europa.eu/en/your-online-life-and-the-eu/ ;
https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act ;
https://uk.norton.com/blog/how-to/what-is-cybercrime-how-it-works-and-how-to-stop-it ;
https://www.interpol.int/Crimes/Cybercrime;
https://www.ncsc.gov.uk/guidance/phishing#section_2;
https://www.imperva.com/learn/application-security/social-engineering-attack/;
https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/;
https://www.rapid7.com/fundamentals/malware-attacks/;
https://www.wallarm.com/what/what-is-a-backdoor-attack;
https://www.loginradius.com/blog/identity/what-is-formjacking/;
https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking;
https://www.imperva.com/learn/ddos/denial-of-service/;
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents;
Devin Partida, "Who's responsible for cybersecurity in industrial and manufacturing settings?," *Occupational Health & Safety*, August 24, 2021;
Gerry Grealish, "The pace of government won't fix cybersecurity," Industry Week, September 3, 2021;

[23] https://www.upguard.com/blog/reduce-cybersecurity-risk

https://leaf-it.com/10-ways-prevent-cyber-attacks/;
https://cybermagazine.com/cyber-security/top-10-ways-prevent-cyber-attacks;
https://purplesec.us/resources/prevent-cyber-attacks/ ;
https://www.wallstreetins.com/blog/post-2/;
https://mightygadget.co.uk/10-ways-to-prevent-cyber-attacks/;
https://www.upguard.com/blog/reduce-cybersecurity-risk.