Cybersecurity and Cyberattacks in Organizations: a Case Study

Ricardo Martins

Lusófona University, Porto – Portugal
ricardoolimart2001@gmail.com

Abstract. Nowadays technologies are an increasingly an indispensable factor for the daily life of an organization. Currently these are used to store the most sensitive data of an organization such as login data, banking information and personal data of employees, in addition to the storage function, these are also used to optimize tasks, increase productivity and product quality. Therefore, the increase in attacks has been having an exponential growth in recent years because of these factors mentioned above it is becoming more profitable for the attacker to carry out attacks against organizations either for their own benefit, or to sell the information obtained illicitly to competitors or in the market or even just to cause damaged. This paper presents different types of cyber-attacks that can be carried out against organizations and will be analyzed at the World panorama, in Europe and in Portugal, and later will be addressed a case of study for each of them, also reports the cybersecurity issues that should be addressed by the organizations.

Keywords: Cyberattacks, Cybersecurity, Technologies, Organizations, Threats

1 Introduction

Technologies increasingly play a more important role in companies, and for many of them, the use of technologies is essential for the proper functioning of the organization and, therefore, we have been witnessing an exponential increase in cases of cyberattacks on organizations as they stop attackers are increasingly profitable to make these attacks as technologies increasingly represent something of high importance, but many organizations devalue security issues related to technologies as somehow an investment in the security area will not bring financial return and moreover it requires a possibly high investment [1]. As organizations devalue investment in the security area, they become vulnerable to cyber-attacks and, especially, these are successful. Nowadays, intruders have several techniques and tools to carry out cyberattacks and, therefore, companies should try as much as possible to be careful, that is, they should take measures to avoid suffering attacks of this kind since the occurrence of these attacks on a company, can be devastating for the company whether for ransom or reputation issues [1]. The purpose of this document is to investigate the ways most used by hackers to carry out attacks on organizations and describe how these attacks work, it also aims to investigate the cybersecurity policies adopted by

organizations and finally it will be investigated the evolution of cyberattacks and cybersecurity at global, European and national level. In general, this paper will describe the main objectives by which cyberattacks are carried out, then the most frequent threats in the organizational environment will be mentioned, then what a security policy should contain and the importance of cybersecurity it has i nowadays, that is to say, the points that must be specified in it, afterwards and related to the security policies, some good practices that must be carried out by the organizations will be described and finally the evolution of cyberattacks and cybersecurity will be detailed in the world, in Europe and in Portugal and a case study of a real cyberattack will be presented for these three. The first chapter (introduction) outlines the topics from which this document will be implemented. The second chapter presents the description of the focal terms of this paper, such as cyberattack, cybersecurity, and politics. The third chapter introduces the objectives of executing cyberattacks, that is, the purposes of executing these crimes against organizations, since this will focus on the main methods of attacks against organizations and will include a description of the modus operandi of each of these methods. In the fourth paragraph, an effective analysis of how organizations can protect themselves from the attacks mentioned in the previous point will be carried out, in addition to this, it will also describe the best practices for drawing up a correct and objective security policy. The fifth paragraph will scrutinize the way in which cyberattacks, and cybersecurity is evolving at a global, European, and national level, then a case study will be described for each of these three, that is, a case of a cyberattack will be detailed. and the way the organization mitigated and dealt with it. In the sixth paragraph, the writing of the document will be concluded, and a detailed opinion will be presented in a succinct manner on how cyberattacks and cybersecurity have evolved in the World, European and national panorama, and the opinion will be presented in line with the points elaborated in this document.

2 Definition of cyberattack, cyber security and security policy

Cyberattacks are attacks carried out in the technological context, in other words, it is an act of modifying, destroying, exposing, stealing sensitive information and data and obtaining unauthorized access to a certain medium [2]. Cybersecurity is the measures defined by the organization to protect its technologies against cyberattacks, these include the development of policies and guidelines, analysis of risk management, awareness and training of employees and definition of the best tools and technologies to protect the organization's technology against attacks, on the other hand, protection measures are good practices aimed at all organizations and must be implemented by them to obtain a secure organizational technological environment[3].

3 Targets of cyberattacks

In short, cyberattacks have four main purposes, these being [4]:

Intrusion -The intrusion has the function compromise the integrity, confidentiality or availability of a system resource. This type of attack can irreversibly change information.

Access to confidential information - Towards of an attack, attackers may have access to certain information considered sensitive.

Loss or theft of information Following an attack, information may be erased, or information may be stolen by the attacker.

Personification- Occurs when the attacker tries to impersonate someone else.

3.1 Most frequent attacks

This section will present the main attacks by hackers against organizations and will also present the main ways to mitigate them and the main measures by which organizations should be guided to protect themselves from these attacks.

Some examples of the most frequently executed attacks are:

3.1.1 Distributed denial of service (DDoS)

DoS (Denial of Service) is an attack whose function is to interrupt a service or completely prevent the use of the system by legitimate users [5]. Regarding the attacks themselves, there are eight attacks that are used most frequently, these are [6]:

Sin Floods (SYN Flood) -This attack aims to flood the network by sending a high volume of packets (500-589 million packets per second).

WS-Discovery - It is a multicast discovery protocol and therefore it is used by IoT devices to discover the different nodes in a network.

Reflected and Amplified Attacks-These attacks have the method of sending a message to users to present the possibility of delivering a larger payload than usual.

BIT-AND-PIECE These attacks affect the telecommunications sector and the services that provide the internet and aim to overload a service.

Multi-Vector DDoS Attacks - This attack combines different types of existing DDoS attacks to cause more impact.

Some actions to mitigate these attacks are: the use of DDoS protection services, use of methods to quickly identify infections, use and cloud services and frequently carry out risk analyzes to assess security techniques, technologies and network services [6].

3.1.2 Spam

Spam is the mass sending of unsolicited messages. Spam is not itself a means of attack, it is used as a means to distribute attacks such as ransomware and trojans [7].

Some ways to avoid receiving spam emails are: implementing a method to filter content and locate existing malicious content, keep hardware, firmware and software up to date, not log in via links received by email, develop procedures to handle sensitive data, use secure email gateway and perform filters maintenance frequently, implement security techniques and finally frequently update the whitelist, reputation filters and blacklist. [8]

3.1.3 Phishing attack

Phishing is a technique used to trick people into sharing their confidential data unlawfully [9]. We can organize phishing attacks into two categories [10]:
Make the attack-To carry out an attack, several ways can be used, such as email spoofing, sending attachments, URL spoofing, website spoofing and spear phishing.
Collect the data obtained in that attack-The techniques used to collect the data obtained in the attack can be divided automatically into two groups, the collection is performed by filling out false forms by the victim, keyloggers (records and sends to the attacker the keys clicked by the victim) and manual collection which is performed through human observation (social engineering) and social network analysis.

To mitigate phishing attempts, simply educate staff to learn how to deal with phishing attempts, implement standards to reduce spam emails, verify website domains, and verify forms before filling in personal data [9].

3.1.4 Web based attacks

Services provided by the Web are subject to different types of attacks such as [11]:
SQL Injection - This attack has the function of executing queries/changes on websites in an improper way.
XML Injection Attack - This attack's main function is to change the XML logic of an application/site.
XPath Injection Attack - This attack occurs when user input data is used maliciously.

The most frequent attack in this category is SQL Injection. This is a technique used by hackers to perform improper SQL queries/changes on the database server [12].

To mitigate these attacks, developers must take into account the security of the application while developing it, as attacks often occur due to design flaws, it is also important to implement web application firewalls, use input validation methods, encrypt communication and API binding, provide correct authentication mechanisms, authorization and perform vulnerability assessments on applications. [12]

3.1.5 Malware

Malware is a general term used to describe all malicious software intended to wreak havoc on a computer system. [13]

The best-known different types of malwares are [13]:

3.1.5.1 Trojan Horse

This type of malware disguises itself in the system together with a legitimate program and so the victim installs the program thinking that he is installing something legitimate and after all he is installing something legitimate with a virus attached and once installed and given permissions can perform activities in the background.

3.1.5.2 Virus

This type of malware attaches itself to a legitimate program or system document and spreads from one computer to another via internet downloads or email attachments for example.

3.1.5.3 Worm

Worm is very similar to a virus, it only has the particularity of spreading from computer to computer without human interference, unlike the virus, it can be executed through a keylogger or through activity monitoring programs.

3.1.5.4 Ransomware

Ransomware is the most prevalent type of cyberattack currently, this type of attack has as its main objective to hijack the files and resources of the victim's machine and then ask for a ransom, in order for the latter to regain access to those resources or files. Ransomware can be differentiated into three distinct categories such as [14]:

Locker -This ransomware's main function is to block the computer's functions.
Crypto- Crypto encrypts files on the victim's device but does not interfere with computer functions. This can use three different schemes to encrypt documents, namely: symmetric encryption, where the key to encrypt documents is included in the ransomware, then we have asymmetric encryption, but this has a condition given that it is slower than the previous one and that's why it becomes a problem to encrypt large files, finally we have hybrid encryption, this uses symmetric and asymmetric encryption.
Scareware- Scareware uses pop-up ads as a means of attacking, as a way to trick users into downloading certain software.

Some actions to mitigate these attacks are: keep backups that follow the 3-2-1 rule (3 copies in two different formats and one of those copies off site), have cyber insur-

ance policy, have a security operations center in the organization, implement content filtering to filter out unwanted attachments, invest in employee training, and perform frequent antivirus tests [15].

4 Security Policies for Organizations

We have witnessed a growth in the importance of technology in organizations and therefore they must pay special attention to the care they must take and transmit to the organization's technology users. A security policy is intended to delineate and regulate the rules by which people belonging to it must obey whenever they are IT. use the systems. A good security policy must comply with certain requirements such as: information security policies, ie the way in which information must be managed according to existing laws, regulations and the business, the organization of information, in other words, the levels of access for which a certain type of information will be available, the management of human resources that is related to the organization of information and also contains the levels of access to computer systems, asset management, ie, the organization must have someone who is responsible for the computer field and this must be documented, physical security and environment, that is, it must contain the rules for the physical use of the computer components, security of operations, that is, rules must be defined on how the organization's network should be used and, finally, the management of security incidents, that is, it must be documented how to act before, during and after a cyber-attack [4].

After the security policy is elaborated, it must be ensured that some measures are complied with, such as [16]:

Assign management responsibility-Someone within the organization should have the role of ensuring that adequate resources are used.

Gaining Employee Acceptance- Communication with employees about cybersecurity issues by administrators.

Carry out cybersecurity audits -Audits should be carried out regularly by people with adequate knowledge and experience.

Data Protection- Make employees and suppliers work in accordance with the RGPD

Publish cybersecurity policies - Cybersecurity rules and policies for OS employees should be defined and published

Provide Appropriate Training - Provide cybersecurity awareness training to all employees.

Ensure effective third-party management - Ensure that all providers with access to data or sensitive parts of systems respect the agreed security levels.

Develop an incident response plan - An incident response plan must be developed, this plan must contain clear and documented guidelines, roles and responsibilities.

Protect access to systems - Encourage employees to use passwords with at least 3 random words combined in a sentence, this must be long, with upper and lower case

letters, must also have numbers and special characters and must not contain personal information. At passwords must not be reused elsewhere, cannot be shared with peers, and must use 2-factor authentication.

Secure devices - Use firewalls, ensure remote access software is up to date, ensure remote access only to verified IP addresses, restrict remote personnel access to only necessary systems, and ensure monitoring and alerts are enabled to alert you to suspicious activities. Improve physical security - Encourage users of company devices to be careful with them such as being careful where they leave them and using strong passwords.

Secure backups - Backup should be done regularly and automatically whenever possible, kept outside the organization's environment, should be encrypted especially if moved between locations, and the ability to restore data from backups should be regularly tested.

Working in the cloud - When choosing a cloud service, you must obtain information about it, such as how it complies with European Union regulations and the type of treatment used with personal data.

5 Cyberattack analysis

In this chapter, an analysis of the evolution of cyberattacks in the World, European and Portuguese panorama will be carried out. Three real cases of executions of cyberattacks against organizations will also be described.

5.1 Analysis of the World Panorama

Regarding the global scenario, cyber-attacks have experienced an exponential growth in relation to the values of previous years and a lot because of the COVID-19 pandemic, which the whole world has faced. The pandemic is indirectly related to the increase in cases of attacks, since the technological area, with the progression of the pandemic, became a very important and indispensable factor in the daily lives of organizations and, therefore, it became a profitable business for the hackers. The most performed attacks worldwide are through malware, ransomware, spear-phishing and spam emails, these attacks lead to violations of the organization's privacy, affect the company's reputation, lead to lost revenue, and generally lead to interruption of the services of the organization. company., then there is website theft, which is based on the hacker gaining administrative control of the website, which can lead to service disruption, loss of reputation, loss of customer confidence, and loss of revenue. As the pandemic came on suddenly and so organizations had to adapt very quickly and they had to make technology an indispensable factor for the proper functioning of the organization, and that is why we have been witnessing an increase in importance and increasing cybersecurity measures worldwide [17].

5.1.1 Cyberattack on Colonial Pipeline (USA)

Colonial Pipeline is a company that contains the largest pipelines in the US [18]. The type of attack used in this case was through a Ransomware, more specifically the hackers used a Trojan called DarkSide [19]. This type of Trojan is created by DarkSide and then sold to people interested in buying it, and a fee is charged either for the executed attack or a monthly fee. Darkside is a ransomware-as-service (RaaS) in other words, it is an organization in which they develop ransomware and then deliver it to cybercriminals to carry out attacks on organizations, the hackers who developed it receive an income [20]. Regarding the attack itself, this took place on May 7, 2021, the actors of the coup encrypted the data and demanded payment in cryptocurrencies, they also stole 100GB of company information to use as blackmail [21]. Regarding the modus operandi of the attack, the hackers used a password from a VPN service account that was no longer in use but still had active access, this password was made public along with a set of other passwords on the darkweb. The data breach happened on April 29 and was only discovered on May 7, when it was communicated to the company that they had been attacked, the company decided to pay the attackers approximately 3.8 million euros (US$ 4.4 millions) in cryptocurrencies right after the attack for the attackers to return the stolen data by them [21]. In terms of impact, the company lost part of the money it paid, the US government was later able to recoup a part, but in addition to this, it restricted the availability of fuel, which led to prices increasing enormously at gas stations and furthermore it caused embarrassments in the gasoline stations. This attack could have been avoided if the company in question gave more relevance to security issues, given that a policy for the use of multifactor authentication was in place [21]. Basically, multifactor authentication involves adding one more level of protection to a login, as for the login to be executed, the user who intends to do so will have to use two pieces of information found in different places [22].

5.2 Analysis of the European panorama

In relation to cyber-attacks that occurred in the European space between 2020 and 2021, these increased mainly due to the pandemic state in which we live. Between 2020 and 2021 we observe that attack through Ransomware continues to dominate the list of attacks preferred by attackers on the other hand, malware continues to decline even though in 2021 its affluence has increased compared to the year 2020, since the attack by DDoS became more "competent" and targeted in the year 2021. The pandemic forced the adoption of technology on a large scale, and so cybersecurity experts needed to adapt existing defenses to a new infrastructure paradigm being that the main objective was to minimize the organizations' exposure to cyber-attacks. In addition, specialists had to deal with the adaptation of organizations to a new modus operandi as they had to adapt and modify all their work patterns, and IT security professionals had to respond very quickly to the challenges introduced by the pandemic [23].

Between 2020-2021 cyber threats did not affect a single industry, that is, attacks were made to systems that are used by different industries, but targeted attacks were also carried out, that is, attacks aimed at harming an organization in concrete [23].

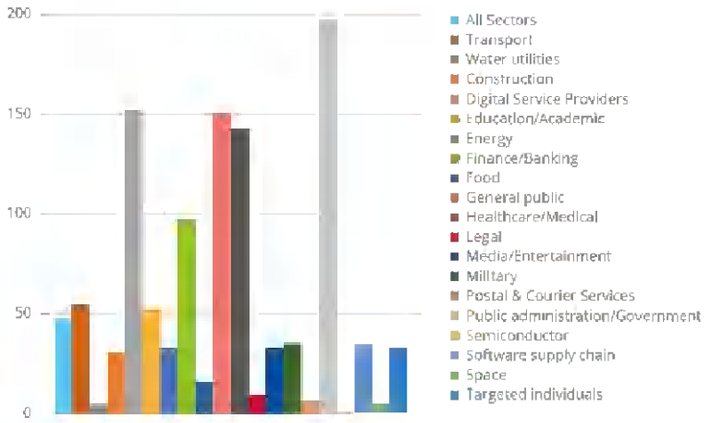

Fig. 1. Incidents by sector between 2020 and 2021 [23]

5.2.1 Cyberattack on Oloron Sainte-Marie (France)

Oloron Sainte-Marie is a hospital located in the Pyrénées-Atlantiques region and on March 8, 2021, was the target of a ransomware attack [24]. The attack carried out by the hackers encrypted the hospital's data and demanded a payment of 44120 euros (approximately 50000 dollars) in Bitcoin. The attack executed by the hackers encrypted the hospital's data and demanded a payment of 44120 euros (approximately 50000 dollars) in Bitcoin. Regarding the attack itself, the screens went blank, and a message appeared on them with a ransom demand of 12000 euros (approximately 13600 dollars), the municipality decided not to pay the ransom and a part of the data was erased from the disk [25]. This attack ended up affecting the proper functioning of the hospital because the computer system was down and, therefore, the users' data and prescriptions were no longer available and had to be executed on paper, this attack affected the medical interventions performed to the users [26]. To mitigate this attack, the hospital managers conducted an audit of the hospital's computer systems [26].

5.3 Analysis of the Portuguese panorama

Regarding the national panorama, we can say that we have been witnessing an increase in threats and conflicts in cyberspace in Portugal, in 2020 the number of cybersecurity incidents underwent a large increase compared to the values of 2019, and the exponential growth of these incidents occurred to from March 2020, which coincides with the beginning of the COVID - 19 pandemic. During the year 2020 there was an increase in phishing/smishing attempts, but there was also an increase in other forms of swindling. people being more isolated and also because of the growing need for people to use more technological means due to the pandemic. The main attack is the malware infection since the fact that people have to use more technological means

due to the fact that they are telecommuting favored the attackers to the point that they were able to take advantage of the technical vulnerabilities that arose from it. Despite the increased risks, national cyberspace managed to increase or at least managed to maintain capacity in 2021 in compared to the year 2020, but it is possible to state that in the year 2021 threats continue with an emerging trend compared to the year 2020. It is inevitable to talk about cyber-attacks without mentioning the influence that the pandemic situation had on their increase. For this increase there are two reasons being these, the social confinement, and the mandatory mass adoption of digital technologies. During the period of confinement, phishing was the most used cyber-tack by attackers. In Portugal, the main victims of cyber-attacks are SMEs (small-medium enterprises), Sovereignty Bodies, Public Administration and the sectors of Banking and Education and Science, Technology and Higher Education [27].

5.3.1 Cyberattack on Portugal Energy (EDP)

EDP Comercial is a company belonging to the EDP Group that operates in the free energy market, both nationally and internationally [28]. The type of attack used in this case was through a Ransomware, more specifically the attackers used a Trojan called by Ragnar Locker which is intended for cyber-attacks against organizations [29]. Regarding the modus operandi of this ransomware, it starts by implementing Windows XP virtual machines to encrypt the victim's files, the implementation of the virtual machine allows attackers to prevent the Trojan from being detected by security mechanisms, after closing the barriers of the company's security and device management services, then it warns the company that it was attacked and publishes evidence of the attack on the dark web to show the company in question that it has very important documents belonging to it, and then the attackers present it to the injured a ransom value in Bitcoin and a deadline [30]. Regarding the attack itself, this one took place on April 13, 2020. This attack encrypted part of the company's servers and in addition apparently, 10TB of sensitive company data was stolen. The attackers exposed evidence on dark web that they had sensitive company data and gave it 20 days to proceed with the payment of 1580 bitcoins (approximately 10 million euros at the time), if the company did not make the payment, they threatened to return public documents and deliver the information to the competition. EDP did not pay the attackers the 1580 bitcoins and therefore, and surprisingly, they eliminated the decryption keys from the company's servers and computers, that is, the attackers in doing this gave up trying to profit from the attack since made it impossible to recover the assets affected by the attack. In terms of impact, the company lost much of its reputation as it lost sensitive data, which contained government information, customer data, investor data, among others and in addition there is still a risk that hackers have sensitive information in their hands and may still try to take advantage of them. In addition to the aforementioned impacts, the company still had to replace the hacked servers. Regarding security issues, an investment of 50 million euros was made in computer security, to make mitigations, "maximum permissible downtimes for applications" were implemented, redundant disaster recovery systems, creation of a team to monitor the

security of the company, cyber-attack insurance, and employee training in security principles [29].

6 Conclusion

To conclude, throughout this paper the main attacks carried out against organizations were described, a set of measures by which companies can be guided to mitigate the occurrence of cyber-attacks was also presented, and a global, European, and national analysis of the evolution was presented. of cyber-attacks and finally three case studies of cyber-attacks were presented. Regarding the analyzes presented, we can observe that these all focus on a factor called COVID-19, in the three scenarios presented, the pandemic factor led to an exponential growth of attacks and therefore it is noticeable that organizations did not give much relevance to more technologies. specifically in the area of cybersecurity, mainly in the training of its employees, which only happened when they had to perform more functions virtually, if they had been trained before in the technological areas, the number of incidents would probably be lower, on the other hand we can say that attacks orchestrated by hackers are evolving and so it will become increasingly difficult to defend against them as there are several ways to exploit system vulnerabilities and also, for a hacker, just find a small vulnerability to be able to breach the system while, on the other hand, the team that takes care of the organization's computer field has to look for and fix several vulnerabilities that may exist, so the attacker's job will always be easier than the work of the defense. Organizations will always be able to try their best to prevent the occurrence of attacks, for that they have to create a good security policy and encourage technology users to follow them. In short, organizations should invest in cybersecurity investment since, increasingly, the most important and confidential information is stored in digital format and therefore care must be increased since the occurrence of a cyberattack can completely ruin an organization either in monetary terms or in matters of customer trust.

7 References

1. Astani, M., Ready, K.J.: Trends and Preventive Stratregies For Mitigating Cybersecurity Breaches in Organizations. Issues in Information Systems.Volume 17, Issue II. pp. 208-214 (2016)
2. Iakovakis, G., Xarhoulacos, C.G., Giovas, K., Gritzalis, D.: Analysis and Classification of Mitigation Tools against Cyberattacks in COVID-19 Era. Hindawi. Volume 2021, 1-21 (2021)
3. G. Cains, M., Flora, L., Taber, D., King, Z., S. Henshel, D.: Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. Wiley Online Library. Risk Analysis, 1-27 (2021)
4. Oliveira, V, dos Santos, V.D.: Cibersegurança e Inteligência Artificial: Como garantir a segurança de um Sistema de Informação. NOVA Information Management School – Instituto Superior de Estatisitca e Gestão de Informação, 1-91 (2021)

5. Ivaki, N.: A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification. WSEAS Transactions on Computers. 1-11, (2008)
6. ENISA, "Distributed deniel of service- ENISA Threat Landscape" (2020)
7. Spinello, R.A.: Ethical reflections on the problem of spam. Ethics and Information Technology. 1. 185-191 (1999)
8. ENISA, "Spam – ENISA Threat Landscape", (2020)
9. ENISA, "Phishing – ENISA Threat Landscape", (2020)
10. Basit, A., Zafar, M., Liu, X., Javed, A.R., Jalil, Z., Kifayat, K.: A comprehensive survey of AI- enabled phishing attacks detection techniques. Telecommunication Systems (2021) 76, 139-154 (2020)
11. Mouli, V., Jevitha, KP.: Web Services Attacks and Security – A Systematic Literature Review. Procedia Computer Science. 93. 870-877 (2016)
12. ENISA, "Web-based attacks", (2020)
13. Mat, S.R.T., Razak, M.F.A., Kahar, M.N.M., Arif, J.M., Mohamad, S., Firdaus, A.: Towards a systematic description of the field using bibliometric analysis: malware evolution. Scientometrics (2021) 126, 2013-2055 (2021)
14. Beaman C., Barkworth A., Akande, T.D, Hakak, S., Khan, M.K.: "Ransomware: Recent advances, analysis, challenges and future research directions. Computers & Security, Volume 111, pp. 1-22 (2021)
15. ENISA, "Ransomware – ENISA Threat Landscape" (2020)
16. ENISA, "Cybersecurity guide for SMEs – 12 steps to securing your business", (2021)
17. Okereafor K,. Adelaiye O.: Randomized Cyber Attack Simulation Model : A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. IJRERD. Volume 05 - Issue 07, pp. 61-72 (2020)
18. Colonial Pipeline, https://sr2448.colonialresponse.com, last accessed 2021/10/20
19. Kaspersly, https://www.kaspersky.com/blog/pipeline-ransomware-mitigation/39907, last accessed 2021/10/20
20. CISA, https://us-cert.cisa.gov/ncas/alerts/aa21-131a, last accessed 2021/10/20
21. Bloomberg, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password, last accessed 2021/10/20
22. Microsoft, https://www.microsoft.com/pt-pt/security/business/identity-access-management/mfa-multi-factor-authentication, last accessed 2021/10/21
23. ENISA, "Enisa Threat Landscape 2021" (2021)
24. LaChaîneTV7, https://www.sudouest.fr/pyrenees-atlantiques/oloron-sainte-marie/bearn-l-hopital-d-oloron-sainte-marie-victime-d-une-cyberattaque-1558161.php, last accessed 2021/11/02
25. TECHVAIR https://www.techvair.com/2021/09/oloron-sainte-marie-sanitation-service.html, last accessed 2021/11/15
26. Insider Paper, https://insiderpaper.com/frances-oloron-sainte-marie-hospital-cyberattack/ last accessed 2021/11/02
27. CNCS, "O relatório em 15 minutos – Cibersegurança em Portugal" (2021)
28. EDP, https://www.edp.pt/quem-somos/, last accessed 2021/11/10
29. Expresso, https://expresso.pt/economia/2020-04-18-EDP-imune-a-crise-mas-nao-aos-hackers, last accessed 2021/11/11
30. National Cyber Security Center Hungary, https://nki.gov.hu/en/it-biztonsag/hirek/virtualis-geppel-tamad-a-ragnar-ransomware/, last accessed 2021/11/15