# Portugal Cyber threats Review: Targeted Health Institution

David Pinto

Lusófona University of Porto, Portugal
davidpinto15@gmail.com

**Abstract.** Over the years, there has been a larger improvement of technology, being present on most of the organizations, whether governmental or private, and being one of the fundamental components of their proper functioning, meaning that nowadays, big and most of medium corporations cannot work unless they have access to their servers and internet, showing how dependent they are to technology and how much impact an attack can have on their infrastructure.

Healthcare is no exception, given that technology is used from triage of the patient to their discharge, being used to save patients data, which medicines have taken or should take, all the medical history. This way, by storing all this data on servers, by becoming "online", health Institutions become potentials victims to attacks.

Throughout the paper, it will be done a review about the threats and attacks to Institutions in Portugal, focusing especially on the health Institutions, giving a real example of such attacks, how it was dealt with and ways to prevent and/or reduce them.

**Keywords:** Cybersecurity, Portugal, Threats, Attacks, Vulnerabilities, Healthcare, Information, Technology

## 1 Introduction

Technology and internet had a great advance in the last decades, given that is has been almost 30 years since the first medical record system based on a computer was proposed [1], till that date it was done manually. This advancement didn't affect just the way data is stored, it was also created new machines with the goal of facilitate the doctors work and improve the well-being and health of the patients. This way, Health Institutions became a new place for hackers to take advantage of, by having all their work fused with technology they have enabled themselves to possible cyberattacks.

Given that all the data about the patients is stored on a server, rather than some folders on a locker, it's natural that whoever wants access to this information, whether to use it themselves or to sell it to some companies, is willing to attack those infrastructures that contains it in order to seize it. Beyond their data, some patients require machines or electronic supports that are essentials for their health and well-being, such as implantable medical devices (IMDs), for example pacemakers or implantable cardioverter-defibrillators, which are electronic devices designed to treat abnormal physiological conditions within the body, which can vary from hearth failure to diabetes to Parkinson's disease, these devices can also fell victims to the

same hackers than seek your information, and even though technical security mechanisms has begun being developed it is not hack proof. [2]

However, things could be done to prevent or hinder the attacks, if the attack is successful there are measures to be taken in order to contain the data loss of patients and these attacks have consequences and cause damage.

All these questions will be addressed throughout this paper which focus on the theme threats to cybersecurity in Portugal, with special emphasis on health institutions. In section 2 is covered attacks and threats, giving examples, their consequences and the damage caused. Section 3, will be talked about vulnerabilities in health institutions, then a sub-topic about a specific attack to health institutions around the world and how Portugal fought against it and towards the end it will cover how health institutions operate in Portugal. Finally, conclusions are drawn in section 4.

## 2 Cybersecurity Threats and Attacks

Throughout the years, cybersecurity has had several definitions [3], also being in constant evolution, according to the author [4] cybersecurity is the prevention to the damage caused by the unauthorized usage of electronic information and of communication systems and the respective information contained therein, aiming to secure the confidentiality, integrity, and availability, including, as well, actions to restore the electronic information and the communication systems in the case of a terrorist attack or natural disaster, this definition leads to another, cybercrime, which is any criminal activity that involves a computer, networked device or a network, according to the U.S. Department of Justice it is divided into three categories, being them, crimes in which the computing device is the target, suck as in order to gain network access, crimes in which the computer is used as a weapon, like launching a denial-of-service attack, and crimes in which the computer is sued as an accessory to a crime, which happens when we store illegal data on our computer. [5]

Threats to cybersecurity could be classified into 3 types, naturals, non-intentional and intentional. The Naturals are due to hurricanes, storms, earthquakes, basically everything that it is not human related; The Non-Intentional involves all types of accidents, like spilling water on the server room causing damage to the server itself or the bad protection of a certain equipment; lastly, the Intentional, this one is more serious, because it’s the result of malicious actions by people. This last type will be the one given more emphasis since it’s the only that is considered a threat and the one that can hurt the corporations the most [6][7]. It can be categorized, as explained in this table 1. [8]

**Table 1**. Categories of attacks

| Category | Description | Sub-attacks |
|---|---|---|
| Malware | Malicious software used to launch specific attacks in the computer systems | Spyware, Ransomware, Backdoors. |
| Network attack | Active or passive monitoring of computer communications and network traffic | Phishing, Spoofing, Exploit. |
| Network intrusion attacks | Any unauthorized activity on the computer networks | Trojans, Worms. |
| Social engineering attacks | Using social media and phone calls, attackers apply human psychology trick to make users giving access to sensitive information | Phishing. |
| Cyber espionage | Snooping on confidential information of a user or organization without permission | Industrial, Economic, Corporate espionage. |
| Reconnaissance | By finding out weaknesses in the network systems and services, attacker gathers sensitive information about the network | Port scans, packet sniffers. |
| Network access attacks | By searching out malicious activities in the network authentication, FTP and web services, the intruder gets access to a network system to obtain confidential information | Eavesdropping, Denial of service, Identity spoofing. |
| Cyber terrorism | Use of internet for electronic terrorist activities like large-scale disruption of computer networks, high-profile national components, national critical infrastructures or important business operations | Sabotage, Website defacement and denial of service. |
| Cyber warfare | Major disruption to national critical and highly important infrastructures through malign use of digital information | Disruption of nation's public services, Financial Institutions. |

Now that we know the categories, here are so examples of possible attacks their explanations and some measures to prevent each attack:

- Phishing attack: the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.
- Backdoor: a backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access

to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.

- Botnet: a botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks.
- Clickjacking: A Clickjacking is a technique where cross-domain attacks are perpetrated by hijacking user-initiated clicks to perform unintended actions.
- Cross-Site Scripting: This is a type of attack that is responsible for computer security vulnerability, by injecting malicious scripts into the friendly and trusted web sites, these vulnerabilities can be used by attackers to bypass access controls.
- Eavesdropping: In Eavesdropping the attackers listens to the system's or network's conversation without their knowledge and uses that conversation for another attacker or enemy of that organization.
- Spoofing: Spoofing is an attack in which the attacker or program acts as if they are the actual, legitimate user of that system or network, hiding their originality from the network and impersonating the system admin or victim.
- Denial of Service: This attack has the goal of denying the user of resources and shutdown the services of the system by overloading its resources like bandwidth, TCP connection buffers and application/service buffer. [9] [10] [11] [12]

Even though attacks can happen to any institution, there are some measures that can be taken in order to prevent some attacks, here are some examples.

- Denial of Service: Filtering, Blackholing, Scale up Bandwidth, Outsourcing, Firewall and antivirus and Email filters.
- Spoofing: Network segmentation & access control, Physical Security, Packet filtering, Avoid trust relationships, Use cryptographic network protocols.
- Backdoor: Formatting hard disk, Use of file scanner, Setup Firewall.
- Eavesdropping: Access Control, CCTV installation, Securing the Area, Awareness Training.
- Phishing: Anti-phishing toolbar, Blocking of Pop-up, Updating of browser, Secure links, Back-up of data.
- Cross Site Scripting: Data Validation, Data Sanitization, Output Escaping.
- Botnet: Change of Passwords, Encryption. Put IoT devices on a separate network, Keep Firmware Up-to-Date, Turn off Universal Plug-and-Play.
- Clickjacking: Install a Spam & Virus Firewall, Filter Web Traffic and Block Malicious Sites, Periodically Logout Users, Update Internet browser and plug-ins such as Flash. [11]

Profile of the attackers, students, just to have some fun snooping on people's email, ex-employer, perhaps they were not too happy for being let go, so they decide to take revenge by attacking their former company, a sales representative, they do this so they can trick the other people into believing they are better than they really are or that they represent something/someone bigger/better than they actually do, a businessman,

to discover a competitor's strategic marketing plane, and finally a cracker, and in order to explain their motive we should explain who they are, although they can be compared to hackers, there are some differences, while hackers are normally seen as ethically correct, white hats that do their work in order to find loopholes and to restore the security of corrupted networks to build a secure system, and when they do it, it's with the consent of their hiring organization, crackers do it for personal gain, usually hackers have the knowledge and skill to create their own programs, unlike the crackers which prefer to use software available to them, their goal is to break the security of someone's computers and networks for the purpose of engaging in illegal activities. [7] [9] [10]

**Table 2**. Profile of attackers

| Profile of attacker | Goal |
|---|---|
| Student | Have fun |
| Ex-employer | Revenge |
| Sales Representative | Trick people |
| Businessman | Discover competitor's strategy |
| Cracker | Personal gain |

## 3 Targeted Health Institutions

Health institutions are some of the organizations we have to trust the most, it´s them that hold a lot of our personal and private information such as, name, date and place of birth, medical record and social security number, while having several flaws, like low budget, lack of IT organization and excessive use of legacy systems, because of it, they become one of the best and most frequent targets for hackers.

In the last years, medical fields have grown in terms becoming more technology dependents, electronic health records (EHRs), which are the digital versions of a patient's chart, have appeared, clinical systems have been automated, resulting in a evolved workflow that brings news and increased security challenges, the systems are interconnected and mobile devices are being used as remote accesses and data sharing, all these new aspects are in constant evolution, however, the cyber threats are also in constant evolution, hackers besides stealing the patient's data, can they can alter any patient medical records, compromise medicine inventory systems or even cutting off power supply resulting in the unnecessary risk of the patient's lives. [13]

Vulnerabilities are a key component on the impact hackers have since it makes their job easier. Vulnerability is a weakness that allows an attacker to compromise the availability, confidentiality or integrity of a computer system, these may be the result of a programming error, a flaw in the design or implementation or even a bad management which affects the security, it not only can affect software, but hardware as well. According to [14], the greatest vulnerabilities come from external attackers and sharing data with third-parties.[15] Attacks that focus on the network to

penetrated the service usually aim at three targets, web servers, databases and application software. The weakness with using a web service is that this one normally contains vulnerabilities that can be easily exploited by the attackers with the number of tools available to them that can scan web interfaces and highlight those vulnerabilities; To store all the information about the patients, medical services use databases servers, which, if not configured correctly are vulnerable to SQL injection, with the SQL injection the attacker has power over all the three goals of information security, confidentiality, integrity and availability, they can see, delete, steal or change information; For those who use application software, this is, those who use any software running on any device, a rigorous software vulnerability teste should be done to it, otherwise error in the code could be a weakness exploited by attackers. [16]

### 3.1 WannaCry Ransomware attack

The WannaCry attact in May 2017 affected multiple types of organization around the whole world, making thousands of hostages, and health institutions were not excluded from this with an exception.

The WannaCry malware is a self-propagating ransomware that spreads through internal networks and over the public internet by exploiting vulnerability in Microsoft's Server Message Block (SMB) protocol. It consists of two distinct components, one that provides ransomware functionality and another used for propagation, which contains functionality to enable SMB exploitation capabilities. The malware appends encrypted data files with the .WCRY extension, drops and executes a decryptor tool, and demands an amount of money to decrypt the data. [17]
Two days after the attacks have started to appear on several continents and organizations on 12 May 2017, SPMS (Shared Services of the Ministry of Health) issued a normative circular referring the same attack where the next protective measures were taken: The use of email was conditioned, only fax/phones were being used to communicate; Additional mechanisms of security were added to the use internet, these mechanisms could, in websites which held a reduced reputation, be conditioned; All the computers were to be shut down from the 14 to the 15 of May; On the 15 and 16 of May, the computers without internet connection should detect and report any anomalous situations to the computer services, the ones connected to the institution network would have to wait until the implementation of the recommended security measures; If any user detects any suspicious messages or change in the equipment operation, that person must unplug the computer down immediately, it must also report the situation to the computer services of that institution and the servicedesk of SPMS; All the suspicious email or file found on the pc must be reported to the computer services of that institution and the servicedesk of SPMS; If any worker from the National Health Service (SNS), Ministry of Health (MS) or any hospital had, in the distant or recent past, any situation with encrypted files and texts, with a ransom, that information should be immediately reported to the servicedesk of SPMS, informing the where, which and when it happened. [18] With this normative circular, the SPMS got ahead of the attack, and with it dodged being attacked like many other countries and institutions, from the 10 thousand machines

infected with the WannaCry ransomware in Portugal, the institutions that answered to the SMPS were not infected. [19]

### 3.2 SPMS

On this sub-topic, a few questions were made to someone in the Ministry of Health Shared Systems (SPMS), regarding the operation of health institutions in Portugal such as prevention measures or measures taken after an attack, given that the SPMS oversees the health Institutions in Portugal and the answers will be talked about here.

Ministry of Health Shared Systems is a concept to which a majority of corporations resort, hiring specialized services with the purpose of decreasing fixed costs on some activities.

The SPMS, EPE, as one of the central entities in the Ministry of Health has as mission the provision of shared services in the following areas – purchasing and logistics, financial services, human resources and systems and technology of information and communication – to the entities with specific activity in the health area. Regarding cybersecurity the SPMS, EPE should articulate with the GNS/CNCS (National Security Office/National Cybersecurity Center) in order to promote the articulation intra-institutional and interinstitutional with a view to ensure the cybersecurity of health information networks and systems, regardless of your location, depending on existing connectivity, such as keep up with, support and monitor the protection measures, detect, respond and recuperation of critical resources of SNS (National Health Service-). Thus, being that most of public hospitals are a public business entity, with administrative, financial and patrimonial autonomy, the protection and prevention measures from each of the health institutions are managed and enforced internally, performing the measures referred in normative circulars of SPMS or centrally provided services. Giving an example, the following normative circular, nº 07/2017/SMPS: Infrastructure reinforcement measures and systems operation, which is divided into 5 categories, that informs the responsibilities of the entities regarding network infrastructure, systems infrastructure, datacenters and system rooms, technical skills, security and operation, the SPMS responsibilities, measures to have in contingency and crisis situations, informing institutions about the topics a contingency plan needs to have, the SPMS contact mechanisms, actions and information to be submitted and the need to perform simulations and recommendations.[20]

According to the dispatch n. º 1348/2017, it was established that the SNS entities and the MS services and organisms are required to notify security incidents to SPMS, EPE, through their Responsible Notification Officer (RNO). This mandatory centralized cybersecurity notification procedure (NOCICS), predict to categorize cyber security incidents according to 9 classes, in accordance with the taxonomy used by the National CSIRT Network and National Cybersecurity center (CNCS) and where justified, the incidents are reported to the CNCS. [21]

According to the SPMS, the most frequent attacks are related to phishing, malware and intrusion attempts by exploiting vulnerabilities, often stemming from legacy web portal that were not developed using security best practices. However, the attack

surface amplitude is limited by the existence of RIS (Health Computer Network), which by default does not permit direct internet access.

## 4 Conclusion

With all the cybersecurity threats and attacks available, it's important, now more than ever to bet on a serious and sophisticated cybersecurity capable of protecting everybody's information, and also use the profile of attackers to determinate where and how they pretend to attack, so institutions can be prepared for it.

Even though by going offline, the health institutions in Portugal were able to not get infected by the malware, it should have not been their solution to the problem, by doing so they were showing how unprepared health institutes were in terms of cybersecurity in which a measure to stop the attack was shutting down everything from online.

With this work I've learned that for the number and importance of the information and lives health institutes are responsible for, their security should be better, just like the minds of the employees when it comes to opening suspicious emails or enter suspicious websites, however, the security has been improving over the years, showing that they realize the importance and want to keep it safer from every threat.

## References


1. Scielo, http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1415-65552001000100007, last accessed 2019/11/25
2. Denning, T., Borning, A., Friedman, B., Gill, B., Kohno, T. & Maisel, W.: Patients, Pacemakers, and Implantable Defibrillator: Human Values and Security for Wireless Implantable Medical Devices, pp.1-2 (2010)
3. Nicole M Tucker, Cybersecurity: Deciding the Effectiveness of the U.S.Comprehensive Cybersecurity Initiative, pp.1-2 (2015)
4. Cavalcanti, C., "Cyberdefense: Challenges and comparative legislation between Brazil and Portugal", pp.3-6 (2017)
5. SearchSecurity, https://searchsecurity.techtarget.com/definition/cybercrime, last accessed 2019/12/02
6. Breda, F., Barbosa, H., Morais, T.: Social Engineering and Cyber Security, pp.1-5 (2017)
7. Barbosa, H., Magalhães, R.: Cyber Espionage and Digital Privacy, pp.1-3 (2017)
8. Prasad, R, Rohokale, V.: Cyber Security: The Lifeline of Information and Communication Technology. 1st edn. 2020 edition Springer, pp.16-30 (2019)
9. European Commission: Cyberroad- Development of the Cybercrime and Cyber-terrorism Research Roadmap, n. º 607642 , pp.10-11 (2015)
10. Securitytrails, https://securitytrails.com/blog/hacker-vs-cracker, last accessed 2019/12/06
11. Dutta, L., Sumi, F. H & Sarker, F.: A review on Cyberattacks and Their Preventive Measures. International Journal of Cyber Research and Education, 1(2), pp.14-25 (2019)
12. Jamwal, K & Sharma, L. S.: Clickjacking Attack: Hijacking User's Click. International Journal of Advanced networking and Applications, pp.1-2 (2018)

13. Le Bris, A. & El Asri, W.: State of Cybersecurity & Cyber Threats in Healthcare Organizations, pp.10 (2006)
14. KPMG, “Health care and cyber security: Increasing Threats Require Increased Capabilities”, pp.1-2, (2015)
15. Symantec: ISTR Healthcare, vol.22, (2017).
16. Williams, P. & Woodward, A.: Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices: Evidence and Research, pp.309 (2015)
17. Kumar, M.S., Ben-Othman, J. & Srinivasagan, K.G.: An Investigation on Wannacry ransomware and its Detection, pp.1-2 (2018)
18. Circular Normativa nº01, Medidas excepcionais ciber-segurança: http://spms.min-saude.pt/wp-content/uploads/2017/05/Circular-Normativa-n%C2%BA1-SPMS-medidas-ciber-seguran%C3%A7a-v.2.pdf, (2017), last accessed 17/12/2019
19. exameinformatica, http://exameinformatica.sapo.pt/noticias/internet/2017-05-15-WannaCry-12-mil-computadores-infetados-em-Portugal, last accessed 16/12/2019
20. Circular Normativa n.º 07/2017/SPMS, Medidas de reforço de infraestruturas e operação de sistemas: https://spms.min-saude.pt/wp-content/uploads/2017/09/Circular_Normativa-N.07_2017.pdf, (2017), last accessed 20/12/2019
21. Despacho n. º 1348/2017, Diário da República n. º 28/2017, Série 2 de 2017-02-08, https://dre.pt/home/-/dre/106415139/details/2/maximized?serie=II&dreId=106415113, (2017), last accessed 20/12/2019