Security Assessment of the Oeiras Municipality IT Infrastructure

José Pedro Ferreira Gomes

Thesis to obtain the Master of Science Degree in

Telecommunications and Informatics Engineering

Supervisor: Prof. Ricardo Jorge Fernandes Chaves
Prof. Nuno Miguel Carvalho dos Santos

Examination Committee

Chairperson: Prof. Rui Jorge Morais Tomaz Valadas
Supervisor: Prof. Nuno Miguel Carvalho dos Santos
Member of the Committee: Prof. João Pedro Faria Mendonça Barreto

January 2021

Acknowledgments

First, I would like to acknowledge the dissertation supervisors, Professor Ricardo Chaves and Professor Nuno Santos for their expertise, knowledge and cooperation that made this work possible.

I would also like to thank the entire IT Department of the Municipality of Oeiras that allowed this study and gave me all the conditions to carry it out.

A special thanks to André Lopes, Filipe Fernandes, Tiago Martins and Tomás Jacob, colleagues and friends that I made during my journey at the Instituto Superior Técnico, for their friendship, collaboration and support.

To my hometown friends, Pedro, João, Bruno and Renato for not allowing distance to alter the friendship that insists on lasting.

To my girlfriend, Mariana, for being my greatest support in these years of struggle, frustration, sacrifice and finally, conquest. For all the lost moments and because without her it wouldn't have been possible to get here.

To my grandmother who left while I was walking this road, who always asked me to study and graduate so that one day I could have a good life. Thanks for all your advice.

To my sister, for being my longest friend, for all the support and complicity she gave me throughout my life, for allowing me to be her daughter's godfather even though she knew I would be absent most of the time.

And finally, to my parents. To those who made this achievement possible from the beginning. Those who did not allow me to give up when this would be the easiest way, who always believed in me and made an effort so that I could get here. All the efforts I will never be able to compensate. Thank you both, for everything you always gave me.

Thank you all.

Resumo

A segurança da informação tornou-se uma preocupação primordial para as organizações. Devido à complexidade das modernas infra-estruturas informáticas, é difícil impedir indivíduos com más intencões de obter acesso ilegítimo à informação e/ou causar danos a dados ou serviços mantidos por empresas e instituições públicas. A cada mês que passa, o número de vulnerabilidades descobertas excede facilmente o número do mês anterior. Assim, numa altura em que os ataques informáticos são cada vez mais elaborados, qualquer entidade precisa de ter uma defesa física e tecnológica robusta. Neste trabalho, concentramo-nos numa organização específica – a Câmara Municipal de Oeiras – e o nosso objectivo é avaliar a segurança da infraestrutura informática desta entidade. A complexidade desta tarefa advém do facto da mesma ter crescido a uma escala considerável, sem seguir uma arquitectura de segurança abrangente e bem delineada. Como resultado, é actualmente difícil compreender até que ponto esta organização é vulnerável a potenciais ciberataques. Para abordar este problema, esta tese apresenta um estudo sistemático de segurança da infraestrutura informática do Município de Oeiras, que envolveu uma metodologia com três vertentes: (1) implementámos um SIEM interno para avaliar se este ajudaria a ganhar visibilidade dos eventos de segurança ocorridos na rede, (2) realizámos uma análise manual de vulnerabilidade utilizando ferramentas de *pentesting* comummente utilizadas, e (3) realizámos um estudo de campo para avaliar a consciência social dos empregados. Identificámos várias vulnerabilidades e fornecemos um conjunto de recomendações para melhorar a segurança desta infraestrutura informática.

Palavras-chave: Cibersegurança, Vulnerabilidades, Ferramentas de avaliação, SIEM, Infraestrutura, Engenharia Social, Segurança da Informação.

Abstract

Information security has become a primary concern for organizations. Due to the complexity of modern IT infrastructures, it is difficult to prevent individuals with malicious intent to gain illegitimate access to information and/or cause damage to data or services maintained by enterprises and public institutions. With each passing month, the number of vulnerabilities discovered easily exceeds the number of the previous month. Thus, at a time when computer attacks are increasingly elaborate, any entity needs to have a robust physical and technological defense. In this work, we focus on a specific organization – the Oeiras Municipality – and our goal is to assess the security of the IT infrastructure of this entity. The complexity of this task comes from the fact that this infrastructure has grown to a considerable scale without following a comprehensive, laid out security architecture. As a result, it is currently difficult to understand to what extent this organization is vulnerable to potential cyber-attacks. To address this problem, this thesis presents a systematic security study of the Oeiras Municipality IT infrastructure which involved a three-pronged methodology: (1) we deployed an in-house SIEM - Security Information and Event Management - to assess whether it would help to gain visibility of the security events ocurred in the network, (2) performed a manual vulnerability analysis using commonly used pen-testing tools, and (3) conducted a field study to assess the social awareness of employees. We identify several vulnerabilities and provide a set of recommendations to improve the security of this IT infrastructure.

Keywords: Cybersecurity, Vulnerabilities, Scanning tools, Information Security, SIEM, Infrastructure, Social Engineering.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

The world relies on technology now more than ever before. As a result, digital data creation has grown exponentially. Nowadays, businesses and governments store a great deal of that data on computers and transmit it across networks to other computers. Unfortunately, devices and their underlying systems have vulnerabilities that, when exploited, undermine the health and objectives of an organization [1].

Devices, as well as human beings, play a fundamental role in cybersecurity. Cybersecurity is referred mainly as information security, and the practices of ensuring its integrity, confidentiality and availability. It involves tools, technologies, and best practices to protect networks, devices and data from attacks or unauthorized access. A data breach can have a range of devastating consequences for any business. It can unravel a company's reputation through the loss of consumer and/or partner trust. The loss of critical data, such as source files or intellectual property, can cost a company its competitive advantage. Unfortunately, cyber attacks are increasingly damaging to organizations [2]. In 2018, billions of people were affected by data breaches and cyber attacks, and consumer confidence in organization's ability to protect their privacy and personal information continued to erode. Nearly 70 percent of consumers believe organizations are vulnerable to hacking and cyber attacks, and say they are less likely to continue or start doing business with organizations that have been compromised [3].

Discovering and predicting this type of behavior is one of the main reasons why many organizations implement a Security Operations Center (SOC). Sans defined a SOC as: "*A combination of people, processes, and technology protecting the information systems of an organization through proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimizing damage from unwanted effects, typically on a 24/7/365 basis*" [4]. SOCs offer assurance that threats will be detected and prevented in real-time. It's main goals are to provide faster response to security events, the protection of the consumer's trust and data which will consequently minimize costs. A SOC uses a range of tools that collect data from across the network and various devices, monitors for anomalies and alerts of potential threats. This thesis aims to explore and study these tools in order to analyze, understand and correct the vulnerabilities found.

1.1 Motivation

Oeiras Municipality has an infrastructure of nearly 3000 computers, 100 printers, 500 mobile devices not counting with the personal ones, all connected to the network infrastructure which has around 150 assets, including switches, routers, and access points. This infrastructure is controlled by two data centers, one in the IT Department location and the other at the Palácio do Egipto, located in the center of Oeiras. These two places work in high availability, which means that in case of failure in one of them, network traffic and management of critical services becomes the responsibility of the other. In normal functioning, it is the first one to work by default. This infrastructure serves all of the Oeiras's municipality, providing the internal applications that allow the services to function normally, as well as all the connectivity between them and internet access. Services like Loja do Cidadão, schools, libraries and all of the others inherent in a municipality at the disposal of its population. These services would not be possible without the IT department. We can say that the service provided by this department is the most crucial for the municipality to function properly.

In an institution with this dimension and attempting to become one of the most innovative and technological municipalities in the country, security is a main concern. Attacks have evolved to an unprecedented level of complexity and sophistication. Therefore, an organization's approach to these attacks has to include the investment or development of an effective and capable monitoring and prevention system capable of handling this type of incident as the implementation of preventive measures and good practices in the workplace.

The context currently experienced by society motivated by the outbreak of the pandemic has forced companies, especially in the technological area, to change their paradigm and way of functioning. Employees were forced to do their work remotely, which significantly increased the number of accesses from outside to the infrastructure. Obviously, this reality also applies to the Municipality of Oeiras, which had to provide its employees with the necessary tools to continue performing their function in the most normal possible way while trying to reconcile with the best cybersecurity practices.

1.2 Objectives

To this end, this work aims to study the Oeiras Municipality IT infrastructure in its entirety, and understand the various vulnerabilities and risks that may be present, both digital and behavioral. Further on, it is intended to present several solutions to mitigate and control these risks in the future.

In particular, the goals of this work are to explore and correct vulnerabilities found in the infrastructure both physically and logically. To achieve this objective, some intermediate steps were required, namely:

- Understand the use of a Security Information and Event Management (SIEM) and, after a study of risks and vulnerabilities has been carried out, make an assessment of the tools available. Those best suited to this case will then be implemented.
- Understand which are the most fragile points in the entire infrastructure; this will happen at various levels of the system, both computational as human interaction. The human aspect also represents

a crucial point of security or lack thereof. To this end, research will be carried out on social engineering vulnerabilities in terms of security behaviors and then a pedagogical plan will be put in place in order to improve them.

1.3 Contributions

The work developed within this thesis delivered the following main contributions around the matter of cybersecurity applied to this public entity infrastructure:

- Deployment and analysis of the applicability of the SIEM software deployed in-house, to improve the visibility of events occurring in the infrastructure i.e., Splunk;
- Manual vulnerability assessment of the IT infrastructure using standard penetration testing tools;
- Field study involving the employees of the Oeiras Municipality in order to characterize the level of social awareness in this public entity;
- Recommendations on how to improve the security of the IT infrastructure and social awareness of the employees.

1.4 Thesis Outline

The rest of this document is organized as follows: Chapter 2 presents some background and related work, respectively, where the infrastructure is presented and some definitions related to cibersecurity are introduced as well as the current top vulnerabilities and possible tools are analyzed. Chapter 3 describes the architecture of the implemented SIEM, its main characteristics and test cases that served to analyze its applicability to the objective of the study. Chapter 4 presents a manual evaluation using tools for assessing vulnerabilities, applying them to the network resources of the Municipality and presenting the recommendations most appropriate to the vulnerabilities found. In the last chapter of contributions, Chapter 5, aims to evaluate the knowledge and sensibility of the employees of the Municipality to the subject of cybersecurity, with the presentation of a survey, tests of social engineering and recommendations to improve the situations found.

Finally, Chapter 6 concludes this work, by summarizing the main findings obtained in this work and describing possible future work implementations to continue to improve the information security of the Municipality concerned.

Chapter 2

Background and Related Work

With so many governments, entities and private websites being attacked on a daily basis, and as they increasingly embrace digitalization, security has become a crucial factor in almost all organizations globally. Some companies, however, remain hesitant to give due importance to this important aspect until something terrible happens. Establishing a secure infrastructure should be what an entity thinks from the start. Ensuring the integrity, availability and confidentiality of information incorporates many tasks, from configuration management to ensure a robust system, effective cybersecurity and security policies to workforce training. The importance of all these aspects has been growing as the digital world evolves, forcing those in charge of each organization to do the same, evolving.

In this Chapter we first present the IT infrastructure of the Oeiras Municipality, which is the subject of our study. Then provide an overview of the main security risks: vulnerabilities, lack of visibility and social engineering. To help that goal we cover the main technologies employed today by the companies: SOC, SIEM, vulnerability scanners. Then provide a survey of the most relevant scientific literature.

2.1 The Oeiras Municipality Computational Infrastructure

In this section, a description of the Oeiras Municipality infrastructure is presented starting with a presentation of the overall view of the system followed by a detailed description of each critical service.

Overview of the IT infrastructure Figure 2.1 represents the IT infrastructure of the Oeiras Municipality. Within it are represented the most significant locations of the functional network that is responsibility of the IT department. The cloud symbol represents the access to the Internet by the network provider, through fiber optics. This access is delivered both at the main datacenter located at Lagar do Vinho as well as at the secondary datacenter at Palácio do Egipto for redundancy reasons. These datacenters are symbolized by the color red. The remaining locations are differentiated by the network speed delivered and whether they are available with high availability or not, that is, from A to D the speed decreases, as does its availability. The list of places covered by this network is too long, so only the most important are represented. These make up the Municipal Campus and together with the type A1 places are the only functional sites in case of failure of the main datacenter and are served by dark fiber optic connections illuminated by the department itself. The other sites have internet access through operator's VPN.

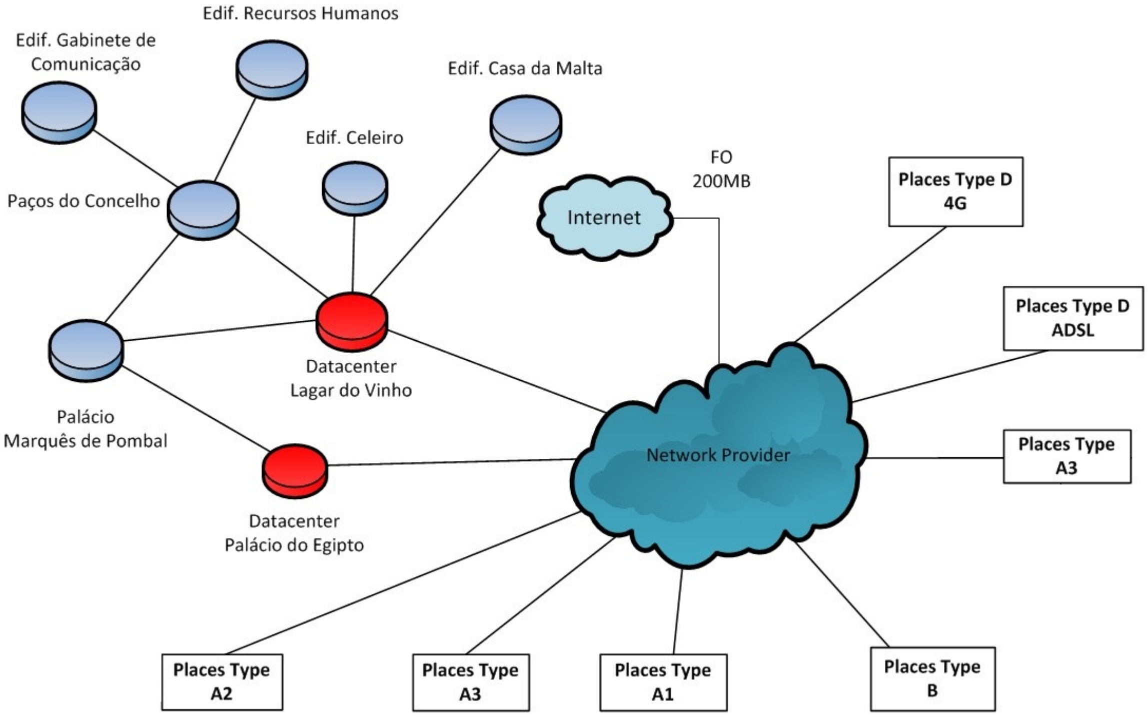


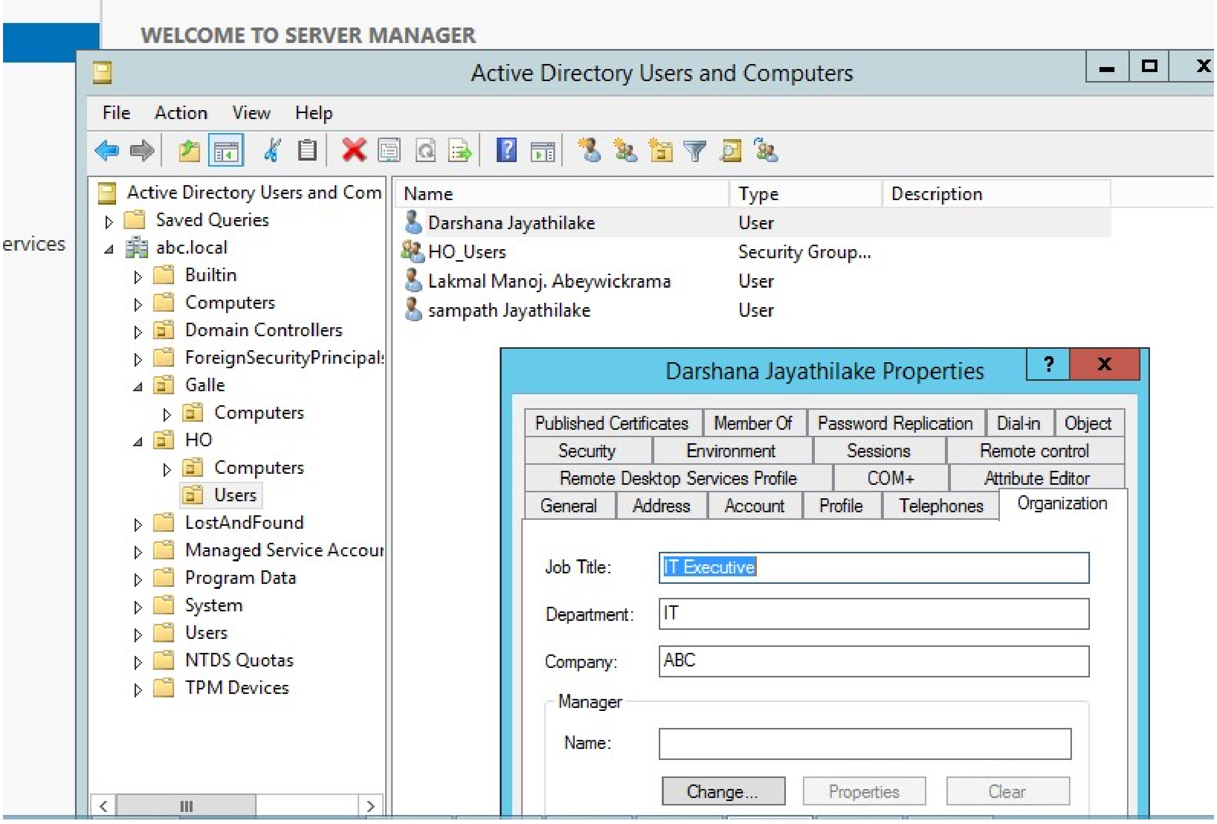
Figure 2.1: Oeiras Municipality network topology.

Critical services These services are defined as a set of IT infrastructure processes, technologies and organizational solutions that enable the normal functionality of the organization's activity. There are six critical services whose assets and networks, whether physical or virtual, are critical to the Oeiras Municipality. Their incapacitation or deactivation would have a debilitating effect in all the services that the municipality provides causing serious inconvenience at all levels of the institution. The following covers each of these services.

2.1.1 Technological Platform

Technological platform refers to the set of core services that serve as foundation layer with the necessary technology for the existence of all other services provided. This service is responsible for defining the entire architecture and operation of the network. It is able to control user access, control IP address allocation, allows easy network management and, above all, allows for scalability. The technology that supports this service includes:

- *Microsoft Active Directory:* One of the most important software tools to help in the organization of companies. The main service in Active Directory is Domain Services which stores directory information and deals with the interaction between the user and the domain, it checks the access when a user tries to enter a device or a server across the network (as illustrated in Figure 2.2). It is



Name	Type	Description
Darshana Jayathilake	User	
HO_Users	Security Group...	
Lakmal Manoj. Abeywickrama	User	
sampath Jayathilake	User	

Job Title: IT Executive

Department: IT

Company: ABC

Figure 2.2: Microsoft Active Directory example [5].

an LDAP/Kerberos-based directory services platform created to unify machines and users which allows administrators to have greater control over the security of the domain.

- *DNS (internal/external):* Domain Name Service works as a directory of names that matches IP addresses, as users take advantage of these names when referring to web pages and email addresses without the worry of knowing how the machine will locate them. These services are divided between an external and internal DNS. The external DNS is used to manage the organization's public IPs, allowing external users to reach desired services. For internal users, the infrastructure features a different DNS server that contains different information than the external DNS contains, as well as additional information about hosts and internal services. It also provides users with additional features such as recursion and caching.

- *DHCP:* Dynamic Host Configuration Protocol (DHCP) is a TCP/IP service protocol that automatically distributes network settings to the terminals that connect to the network. It was defined as a standard in October 1993, succeeding BOOTP. When a user connects to a network provided by the IT Department, he does not need to configure additional parameters (e.g. IP, mask, gateways, etc.) on his machine because they are automatically retrieved from the DHCP server or the router itself that works with a DHCP server and provides this set of information.

- *RADIUS:* Remote Authentication Dial In User Service (RADIUS) is an AAA (Authentication, Authorization and Accounting) protocol for applications such as access and network control and IP mobility. The user or client machine sends a request to the network device to be able to access the resources through its access credentials. In exchange, the network access resource sends the RADIUS an access request message, requesting authorization. This request includes user access credentials, typically consisting of a user name and password, or a certificate provided by the user. Additionally, the request contains information that the NAS knows about you, such as your IP address.

- *NTP:* The Network Time Protocol (NTP) service is designed to synchronize the time between the various devices on the network. The purpose of NTP is to keep the clock of each individual node accurate. This is done with the node periodically synchronizing its clock with that of the reference server. In the case of the Municipio de Oeiras, the Domain Controller 1, which will be depicted below in the document, functions as a NTP server. This service is previously synchronized with the NTP server provided by the Lisbon Astronomical Observatory. Internally, the most relevant service with the greatest impact on users would be the time clock, which is considered critical because of the risk of desynchronization leading to errors in time stamping. As far as security is concerned, in the case of logs and access controls, this could allow unauthorized access at unauthorized hours.

2.1.2 Security Platform

The security platform allows the protection of access to communications networks in order to control incoming/outgoing traffic and associated protocols/ports. It allows the protection of the access to the communications networks in order to control incoming/outgoing traffic and associated protocols/ports. It is composed by the architecture, tools, and processes that ensure the security of all computational's platform hardware, software, network, storage and other components.

- *IEEE 802.1X:* It is an IEEE standard protocol for port-based network access control. In addition, it provides authentication mechanisms for devices that want to attach themselves to a network. Any computer that connects to the network must first provide authentication information before it can be allowed on the network. It works in conjunction with RADIUS allowing authentication of devices already in the domain.

- *Firewall:* The firewall controls the traffic between the internal and external networks and is the core of network security policy. Every network needs malware defense, and advanced malware defense involves many layers of safeguards, including continuous network scans. There are many types of malware that a firewall can protect against, including viruses, worms, Trojans, spyware, adware and ransomware. Its features are identity and computer awareness; internet access and filtering; application control and intrusion and threat prevention. It allows for the customization of access for each type of service of the municipality, to deliver each one, without compromising security.

- *Cisco Ironport:* This service is integrated by two components, Email Security Appliance (ESA) and Web Security Appliance (WSA). The first, as the name implies, is an email security gateway.

Its basic capabilities include antivirus, antimalware, antiphishing, and anti-spam. It has a spam detection rate above 99%, and because email is one of the preferred attack vectors today, this service is a necessity for the organization to protect its users, as well as to protect itself from the risk behaviors they may have. The WSA service automatically blocks risky websites and tests unknown websites before allowing access to them.

- *Port Security:* This technology is used to restrict access from unauthorized devices, who are not in the domain. Each switch port has a limited number of MAC addresses it can learn, for example, if one device which is unknown tries to connect to switch port then it will be discarded. The port will then be shutdown having to request manual permission to the network administrators to be enabled again.
- *Access-Control Lists:* Allows to provide and enforces a set of rules defined to filter and control traffic based on IP addresses. It is defined in the network assets and allows or denies access between VLANs (Virtual Local Area Network).

2.1.3 Virtualization Service

This is the most critical service in the entire infrastructure. About 10 years ago, it was decided to start using the virtualization service, changing the entire infrastructure to virtual machines, except for some applications, thus saving time compared to what would be needed to build a physical infrastructure each time it was necessary to install a server. The resources can be managed and optimized according to the needs of the services and above all is scalable, allowing it to be increased without disruption. It is managed by the two geographically separated data centers with redundancy between them. If this service becomes unavailable to both managers everything else fails.

2.1.4 Databases Service

The database service provided by the IT department is used by the applications that the municipality has to provide to the population. In other words, from the supplier-customer point of view, being this department the provider of this service to the municipality and its citizens. In case of failure of the databases all the services of the municipality would stop, depending on whether it would be a global failure or in specific databases and instances.

2.1.5 Internet Provider Service

This service is divided into two components: the Internet Service Provider component for the municipality's other services, which is ensured and distributed by the IT department, meeting the needs of each element of the organization chart. The municipality of Oeiras also provides residents with Wi-Fi access in some public places. This access is also restricted, i.e., it is properly controlled using the tools mentioned in the security platform, to avoid undue access to the rest of the institution's network.

2.1.6 Website Hosting Service

The various organisms that make up the institution often develop activities and projects that require publication of a website, whether developed by the IT department or not. To this end, the department provides a web development and hosting service, with the necessary technologies for the pages to be available online. Because they are pages with public access and connected to the Municipality's infrastructure, they become critical and often fragile points for general security. What often happens is that the various departments and divisions that comprise them contract services that use the brand of the Municipality and are extremely fragile from the security point of view.

2.2 Risks: Vulnerabilities and Social Engineering

2.2.1 Definitions

"Securing a computer system has traditionally been a battle of wits: the penetrator tries to find the holes, and the designer tries to close them." - M. Gosser[6]

The study of vulnerabilities and their mitigation is the main objective of this work. There is no universal definition of what a vulnerability is, but all have a tendency to describe the concept in the same way. In the next paragraphs we will describe how global organizations define a vulnerability, as well as the impact and why it is important to discover vulnerabilities at the perimeter of the network. This is how some world-wide agencies define a vulnerability:

Common Vulnerabilites and Exposures (CVE)
"A "vulnerability" is a weakness in the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that, when exploited, results in a negative impact to confidentiality, integrity, or availability."[7]

European Union Agency for Cybersecurity (ENISA)
"A security vulnerability is a weakness an adversary could take advantage of to compromise the confidentiality, availability, or integrity of a resource."[8]

Microsoft
"A vulnerability is any flaw that makes it infeasible, even when implemented or used properly, to prevent an attacker from; usurping privileges, regulating internal protected operations, compromising data, or assuming trust that was not explicitly granted."[9]

ISO 27001
"A vulnerability is a weakness of an asset or control that could potentially be exploited by one or more threats."[10]

Open Web Application Security Project (OWASP)
"A vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application. Stakeholders include the application owner, application users, and other entities that rely on the application."[11]

Impact: The impact of a vulnerability is defined by the consequences that a company suffers because of that vulnerability. It is composed of two factors, the technical impact, which includes the availability, confidentiality and integrity of information at the mercy of vulnerability, and the impact from the point of view of the business in which the financial, legal or privacy consequences resulting from the loss or exposure of information are analyzed. The combination of the two factors described above evaluates the severity of a vulnerability in an organization's system. Regardless of vulnerability, the reputation and trust of an organization is always damaged, and it is possible to limit these consequences and thus the severity of a security breach by applying correct procedures and security policies.

2.2.2 Types of Vulnerabilities

Normally, four types of vulnerabilities are defined:

- *Hardware vulnerability:* This type of vulnerability includes, above all, changes at the physical level of the system, such as the addition of devices or interruption of traffic.

- *Software vulnerability:* Includes modifications of the software present in the host or its elimination. The most illustrative examples are trojan horses, information leaks and viruses.

- *Data vulnerability:* Includes the security, confidentiality and evaluability of data. Improper access to insider information is the most recurrent case of such attacks, as well as loss of data or alteration of data for personal benefit.

- *Web-based vulnerability:* The most common way to present and share information over the Internet is to do so based on web applications, making it one of the most used attack vectors.[12]

2.2.3 Web-based Vulnerabilities

One of the most important projects dedicated to determining and combating the causes that make the software insecure is OWASP (Open Web Application Security Project). OWASP is an open forum, formed by companies, organizations education and individuals from all over the world interested in the topic of security application (not only for the web). Together they form a security community information that works to create articles, methodologies, documentation, tools and technologies that are made available to the community in general and can be used free by anyone. One of OWASP's flagship projects is OWASP Top Ten. This is a document that identifies the top ten most important security risks in the web applications, and whose goal is to create security awareness in those who design applications by identifying some of the most critical risks than the applications web (and the organizations that use them) face[13].

The first version of OWASP Top Ten was launched in 2003, having undergone minor updates in 2004 and 2010. The 2013 version was renewed to prioritize risk and provide additional information on how to assess the risk of web applications. The most recent version was released in 2017 and follows the same approach as the 2013 version. The risks described in the OWASP Top Ten[13] are the following:

1. **Injection:** Injection failures, such as those occurring in SQL, operating system (OS) and LDAP. These failures occur when unreliable data is sent to an interpreter as part of a command or query. Hostile data from the attacker can trick the interpreter into executing unintentional commands or accessing the data without proper authorization.

2. **Broken Authentication:** Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise session passwords, keys or tokens, or exploit other failures of implementation to assume the identity of other users.

3. **Sensitive Data Exposure:** Many web applications do not properly protect sensitive data such as cards of credit or authentication credentials. Attackers may steal or modify such data to perform credit card fraud, identity theft or other crimes. Sensitive data requires additional protection methods such as encryption of data, as well as special precautions when exchanging data in the browser.

4. **XML External Entities (XXE):** This is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. This attack may lead to the disclosure of confidential data, denial of service, server side request forgery, port scanning from the perspective of the machine where the parser is located, and other system impacts.

5. **Broken Access Control:** Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise session passwords, keys or tokens, or exploit other implementation failures to assume the identity of other users.

6. **Security Misconfiguration:** Good security requires having defined and implemented a secure configuration for the application, frameworks used in the development, application server, server web, database server, and operating platform. All configurations of security must be defined, implemented and maintained because they are generally not safe by default. In addition, the software must be kept up to date, including the external code libraries used by the application.

7. **Cross-site Scripting XSS:** This failure occurs when an application includes unsafe data without proper validation. It is an attack technique that involves code provided by an attacker in an instance of the user's browser. The browser instance can be a standard web browser client or an embedded object in the browser, such as an RSS reader or an email client.

8. **Insecure Deserialization:** Serialization refers to a process of converting an object into a format which can be persisted to disk. Deserialization is the opposite of it, transforming serialized data coming from a file socket into an object. This vulnerability occurs when untrusted data is used to abuse the logic of an application or even execute arbitrary code upon it being deserialized.

9. **Using Components with Known Vulnerabilities:** Some components, such as libraries, frameworks, and other software modules, almost always run with the same privileges as the application. If a vulnerable component is exploited through an attack, server intrusion and severe data loss can be facilitated. Applications that use components with known vulnerabilities weaken the application's defenses and allow to expand the range of possible attacks and their impacts.

10. **Insufficient Logging and Monitoring:** Even though it is not a clear vulnerability like the other risks, it is a best practice guide to protect the application. Due to this problem, compromises are sometimes not detected at all or detected too late. An attack could be detected much sooner without this.

Importance of vulnerability assessment: With the expansion of cyber attacks and online dangers, it is critical to have a consistent beware of the security escape clauses that could turn into a pathway for hackers. These assessments permit security teams to apply an understandable and clear way to deal with and resolve security breaches in the IT infrastructure. This exercise, which must be done regularly, helps in distinguishing dangers and points of failure at the most punctual time conceivable and work on mitigation to close any breaches present in the system. This assessment assumes a crucial job in guaranteeing that an association meets cybersecurity consistency and rules.

This process includes different strategies, instruments, and scanners to discover grey areas in an infrastructure. The criticality of the vulnerabilities found relies upon how much effort is needed to found it and how exposed the company's data is to external entities, the smaller the effort to discover vulnerability and the greater the exposure, the greater the severity of the vulnerability. Periodic scans of the systems should be made to prevent serious situations that impact the service and correct functionality of an institution, as well as minimize the possibilities of exploitation by a malicious user. An organization should have a preventative rather than reactive posture.

Types of vulnerabilities scanners: There are two types of vulnerability assessment scanners: *active* and *passive*. The active methodology envelops everything an association does to foil system breaches, while the passive one involves every one of the manners in which the organization oversees its security. When settling on purchasing choices for your association, it is an error to feel that you need to pick between the two sorts of security. An organization should not have to choose between one perspective but have both.

Passive scanners rely on information obtained *a priori* about the network topology, the applications used, the services installed in the hosts and information about them. These types of scanners can obtain information on parameters such as the machine's operating system, the version of certain services present, whether all network devices run the most recent version of security patches, or even whether the machines run potentially malicious software. This type of scanner has the great advantage that it does not interfere with the normal functioning of the computer or server, however, it cannot make changes to the host, serving only as a warning. It is recommended by best practices that are configured to periodically evaluate the organization's network[14].

As for active scanners, they do not need previously obtained information, since they themselves start the information gathering process, which allows knowing information such as the configuration present in a host, or the constant monitoring of the activity of a certain machine in the network. This type of scans can be used to initiate internally controlled attacks, to discover vulnerabilities in the network. They can take actions to solve security problems, such as blocking a potentially dangerous IP address, only if they are not configured to do so.

2.2.4 Social Engineering

Human actions, whether intentional or not, are a major threat to platform and information security across all organizations. Regardless how robust the technology, any individual with access to an organization's systems and data, it is a potential vulnerability – a response to a phishing message, a mistakenly downloaded file or an opened email attachment containing a virus are the most significant and common weak points. Social Engineering is defined by social-engineer.org as "Any act that influences a person to take an action that may or may not be in their best interest". The idea behind this approach is to take advantage of a potential victim's natural tendencies and emotions to obtain information [15]. These attacks can be performed in any process where human interaction is involved and come in many different aspects, and the most common are the following:

Baiting: This type of attack uses a false promise to pique a victim's curiosity. The attacker wants to entice the target into taking action, luring him into a trap to possibly steal personal information or inflicting its system with malware. The easiest example to describe is an attacker leaving a malware-infected flash drive in a conspicuous area so that it arouses the victim's curiosity to the point where they pick up the object and insert it into their personal or company computer so that it is infected with malware.

Phishing: It is the most widely known vector of attack and consists of the practice of sending emails that appear to be from reliable sources so that the victim feels comfortable, in order to influence or obtain personal information. This information can be obtained by filling in fields with sensitive data, clicking on links to malicious websites or even downloading malware-infected attachments to the computer itself. For example, an email that supposedly comes from a bank agency where the victim has an account and asks the victim to update their account or card details, alleging security flaws, and this data is then used for the attacker's benefit.

Vishing: It is defined as the "practice of eliciting information or attempting to influence action via the telephone". It is similar to phishing since the goal is the same: obtain information that could possibly compromise an individual or an entire organization exploiting people's impulse to help another. This can be done by forging or omitting their phone number to an authority's or a technician to obtain sensitive information. In another level of complexity, some attackers use voice changers to make the attack more coherent. Help desk staff are a portion of an organization's most vulnerable individuals since their main responsibility is to give ”assistance” in a friendly and well mannered way to customers. This is frequently abused by an aggressor to obtain delicate data.

Impersonation: It is defined as the act of impersonating another person to gain physical access to a person, company or system. We can, for example, take the case and someone posing as a technician who comes to perform some assistance or maintenance on a site and the intentions are actually malicious. Of course, the biggest difficulty here is to have a credible appearance for the attack and there are several websites on the Internet that sell clothing from various professions. In extreme cases, being confident when going to a certain place to which you are not supposed to have access allows it to be given without any constraint.

2.3 Security Operations Center

What is a SOC? The easiest way to define a SOC is to describe what it does: it monitors, detects and possibly responds to security-related events of IT assets, including the network, databases, servers, and perimeter defenses such as firewalls.

Many terms were used to define this activity, such as Computer Security Incident Response Team (CSIRT), Cybersecurity Operations Center (CSOC) or Computer Incident Response Center (CIRC). For consistency reasons the term used in this work will be Security Operations Center (SOC). It is possible to define SOCs in several ways, and [16] says *”A SOC is a primarily composed team of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents”*, referring to this concept as a group of people and not as a set of tools. However, we think that the most correct definition which applies best to this case is [17], which says *”A Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents”*, encompassing both the technologies used with the people that use it and how. A SOC of any entity should be able to:

- Provide a secure channel to receive reports on suspicious security activity;
- Assist its constituent members in dealing with those incidents;
- Distribute information related to the events to its constituents;

Only after meeting these three criteria does IETF considers an organization to possess a SOC [18]. A SOC has the purpose of centralizing an organization's management of security, for it to be able to detect threats before they become security incidents.

External vs internal SOC: A System Operations Center can be part of the organization it serves or be placed as an external service to it. If it is external, it is an outsourced service, considered an MSSP (Managed Security Service Provider), which is run by a corporation that provides services to clients. It is the most used alternative in the business world, mainly because the responsibility of implementing and configuring the service is of the contracted company. Its main advantage is that it starts working immediately, with a team of security specialists, which guarantees effectiveness [19]. The size and characteristics of this service depend on the needs of the client, with different plans for all types of organizations. The only disadvantage is that it is an external service, i.e. the members of the organization that benefits from this service do not know how it works, they only receive alerts from the outsourced service.

An in-house SOC belongs to the company, has its own infrastructure and physical location. This requires a major investment as it requires a team to be deployed only for this service, which is equipped with appropriate tools and technologies so that it can perform its duty in the best way. The great advantage is again related to the location, the responsible team is inside the company and knows the infrastructure itself.

2.4 Security Information and Event Management

In the early days, there were relatively few IT security tools, which included antivirus for host monitoring, firewalls for perimeter protection and IDSs for intrusion detection. There was no integration between the various technologies, each one presenting its own interface depending on who developed it and relating the various events throughout the infrastructure was a complicated task, given the lack of compatibility between the various tools. SIEM tools were developed to be able to, in real-time, collect, filter, store, select, correlate, and create alerts for security-relevant events. The main functionality of this type of system is the ability to correlate events from different sources and in large quantities and normalize them in a common representation to all, turning this information into knowledge that can trigger measures and actions of defense, so that companies are able to establish and maintain a situational picture.

Figure 2.3 illustrates the basic architecture of a SIEM system, which accepts inputs from various network and security assets, including perimeter defense systems, intruder detectors, authentication systems, and device sensors. Each of these assets is individually configured to deliver abnormal or strange behavior events, converting these same events into a readable form that allows the analyst to create custom rules that will eventually trigger alerts. The parameterization of these alerts is a continuous process, in an initial phase, the system will notify several false positive alerts whose rules need to be fine-tuned so that the amount of these events decreases and only alerts are created for really important situations. Ideally, the SOC would be hierarchically structured, and this tuning would be done at a lower level and as the complexity of the alert increases, it would rise proportionally to levels above the workforce structure. The primary source is log data, but it can also process other forms of data, such as network telemetry. This is done in an agile way that allows the system to be scalable. Another capability of these systems is that it allows saving these events in a database, for a given time window,

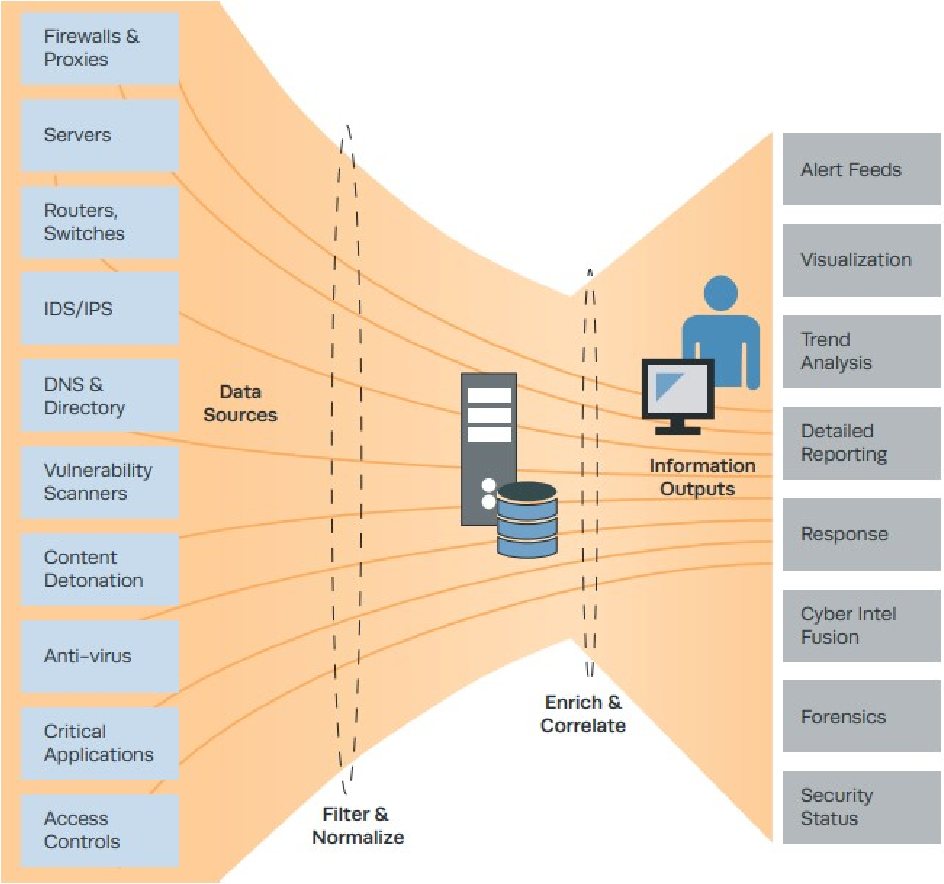


Figure 2.3: Architecture of a SIEM system [16].

thus allowing a temporal forensic analysis.

Recently there has been a marked increase in the offer of SIEM tools, with numerous proposals, each with different functionalities and compatibilities. For a comprehensive and detailed list of the options it is possible to consult the Gartner Magic Quadrant for SIEM [20], launched annually which analyzes all the SIEM systems currently available.

Collecting log data: A SIEM system is capable of collecting data from any device that produces security-related data, including servers, network assets, workstations and firewalls, turning it into actionable security insights. Log collectors can be hardware or software appliances, depending on the product and vendor. The most common way to do this is by using the syslog protocol which is a standard created by the IETF for transmitting log messages over IP networks [21]. Typically these can be installed centrally so that the organization does not need to install hundreds of collectors on the devices.

Standardization: When working with log data it is essential to have a normalization so that the SIEM is capable of reading an correlate events in an heterogeneous environment. Different products use different formats in their log messages, in an environment with thousands of sources, it becomes ingestible to read all the messages and each one has its own format. For all this process to be more agile and scalable it is necessary that SIEM has the ability to make all information homogeneous. Another perspective that intensifies the importance of normalization is the timestamp on log messages. Incident correlation and analysis becomes inefficient if it is dealing with time inconsistencies. To deal with these situations companies use NTP servers, so that all devices are synchronized, in case there are sources in different time zones this makes impossible situations where there are inconsistencies in date and time.

Event correlation: It is an essential function of any SIEM system which collects information that would normally go unnoticed. This feature allows to aggregate and analyze log data from all configured sources to discover security threats present across the network or strange behavior.

This technology combines information from all sources that become readable and comparable due to normalization and compares it to find patterns and relations making even the stealthiest attacks detectable. As Crawley says [22], a brute-force attack on an authentication server could be a scenario where five failed login attempts occur with different credentials by the same IP in a short period of time, followed by a successful attempt by the same IP with another credential on another machine, would be easily detected with a SIEM system with event correlation. These types of events could just be human errors and coincidences or could be cybersecurity incidents. It is then up to analysts to understand which situations are worrying or not.

SIEM system focuses on three main distinct strategies to correlate events: *similarity-based*, *knowledge-based*, and *statistical-based* engines. Knowledge-based correlation represents well-defined scenarios, which is continuously updated to stay relevant. For this knowledge to be well applied rules must be set for each known attack as, for example, brute-force attacks do not happen in the same circumstances as a malware. Similarity-based correlation tries to cluster and aggregate events while trying to find similarities in them. Since it only searches for similarities, this type of engine does not need precise information about the different types of attack. Finally, statistical correlation algorithms rely upon the knowledge of normal activities on the network. Developing correlation rules for a SIEM requires the highest skill level and familiarity with the network and expertise since too detailed rules may be too narrow to raise any alerts, and too general rules can cause false positives that reduce SOC's efficiency.

Rules and alerting: Developing rules to apply in the system requires the highest skill level and familiarity with the network and expertise since too detailed rules may be too stricted to raise any alerts, and too general rules can cause false positives that reduce SOC's efficiency and are time wasting. However, this process is time-consuming as well because the parameters should be verified, ensure that they are correctly configured.

In security matters, time is of the essence, and those responsible for taking action when they are supposed to know about incidents need to do so as soon as possible and as succinctly as possible, always with the necessary data to be able to do so correctly and without risk. That is why the possibility of creating alerts and sending notifications, whether by email or text message, is an eliminatory criterion when it comes to choosing a SIEM system. These alerts are personalized according to the severity of the event and, of course, the organization's wishes. It may even be possible to integrate this alert system with the ticket application and service management present in the infrastructure [19].

2.5 Vulnerability Scanners

There are different vulnerability scanners accessible in the market today. As [23] says, the vulnerability scanning process can be done at four main levels: application level testing for vulnerabilities, failures and bugs; host level diagnostics, which includes hardware, all software present in it and configurations; network level testing that looks for failures in access controls and packet operations; database identification in search of sensitive information that should be protected. The following tools are broadly used as they are open source and give the best results. Next, the most relevant tools are presented.

OpenVAS

”The Open Vulnerability Assessment System (OpenVAS) is a skeleton of several tools as a service offering a far reaching and infuential vulnerability scanning and vulnerability management solution.”[24] It is an Open Source Framework that provides a complete vulnerability management, composed by three modules, data, services and clients.

The data module has the Network Vulnerability Tests (NVT) which contain the tests that will be performed by the scanner. These tests are updated daily with NVT feed which is also a free service. It does not need to be installed on the target machine, it just needs to be installed and configured on a device with access to multiple hosts, so it works as a remote scanner. The clients module handles with the clients, via Web service or via command line prompt. The scanner and the manager are located in the Services module and is the manager that controls the scanner and interacts with the other two modules.

The OpenVAS scanner executes the Network Vulnerabilities Tests and stores them for future consultation in the Data module. This tool tests each port on a computer or server scanning for what services it is running and testing it for vulnerabilities that could be used for malicious attacks. Tests are done comparing with the Network Vulnerability Tests. OpenVAS has the advantages of being open source and constantly maintained however, its main benefit is allowing the configurations in a master-slave mode, with the first responsible for updating and managing the others[24].

NMAP

“NMAP (“Network Mapper”) is a free and open source utility for network discovery and security auditing.” [25]. It uses IP packets to find out which hosts are available on a network and related information, which services are running, which version of the operating system, which ports they listen on. It has been developed to scan large networks, but it also works on individual hosts. It listens for responses to determine if ports are open or closed or filtered in a firewall, for example. NMAP runs in the majority of the computer operating systems. Zenmap is the NMAP is the graphical user interface, it enables saving scans and comparing them, view display of ports running on a host and view network topology maps. This tool has unlimited ip scanning, it’s easy to setup and use and the scans are relatively fast.

OWASP ZAP

"OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free security tools which lets you automatically find security vulnerabilities in your applications."[11]. Its main focus is web applications testing for the major attacks these can suffer, like SQL injection, Cross-site-scripting (XSS), security misconfiguration, Cross-site request forgery (CSRF) or using components with known vulnerabilities. As shown in Figure 2.4, it works by creating a proxy server and forcing the website traffic to pass through that server, composed by auto scanners that intercept vulnerabilities in the website application.

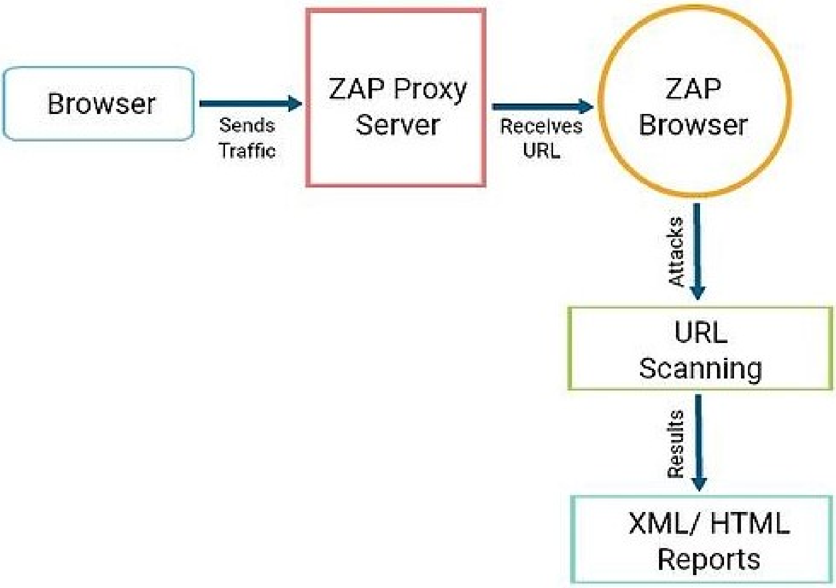


Figure 2.4: OWASP ZAP scanner architecture [11].

Nikto

Nikto [26] is an open source web server scanner implemented in Perl language which performs comprehensive tests against web servers. Nikto has the ability to crawl a website in the least amount of time. It uses a technique called mutation [11], which means it creates combinations of various HTTP and HTTPS tests together to form an attack, based on the Web server configuration and the hosted code. Thus, it checks for critical loopholes such as file upload misconfiguration, improper cookie handling, cross-scripting errors, insecure services, vulnerable scripts and outdated versions of programs installed on the target machine, which provides knowledge about potential problems and security vulnerabilities in computers or servers The fact that it is regularly updated provides reliable results, although, not every check is a security problem, some are just checks that give information about services or technologies present that maybe the security engineer did not know they are present in the server. It runs on every environment, supporting SSL, proxies, host authentication, IDS evasion and, the fact that is able to run on systems with low specifications makes it easier to deploy in any infrastructure [26].

During web scan, Nikto starts by inspecting and collecting as much information as possible about the webserver. Once this phase is over the software begins to recognize several vulnerabilities present on the victim machine. The more details found in the first phase, the more successful this will be. The Test Executor is the component of Nikto's architecture that is responsible for running the tests against the benchmark target. This is the Nikto plugin that takes one test at a time from the tool's database and runs it. These tests are done through HTTP requests to the URL defined in the command. After this, the Data Collector and Analyzer components are called to check if the test was successful or not. If a known vulnerability was found it is called the component that measures the risk of that failure based on the metrics of the tool. Some examples of Nikto's plugins include the Cookies plugin that checks IP addresses present in cookies returned by HTTP requests and the CGI plugin that lists when possible the presence of Common Gateway Interfaces, responsible for telling the webserver how to pass data to and from an application. The Data Collector and Analyzer is responsible for verifying if a known vulnerability really exists on the host. This verification is done by collecting the response from the web server that is being analyzed and it is saved in a variable and then compared with the expected value registered in the test database. This analysis of the response is done in two parts: the confirmation of the successful test and the calculation of the risk associated with the vulnerability. supports a wide variety of options that can be used in different situations encountered, which allow the user to have more control and customize the vulnerability assessment.

WPScan

Content Management Systems (CMS) is a web application that allows users with different knowledge levels of programming to build, manage, and maintain an online website. For this, they are becoming widely used being WordPress the most used one, with a market share of 39%. Since they are so easy to use, people do not always pay that much attention to security requirements when developing the content. With this in mind, it is of the most usefulness and importance to study and use a WordPress vulnerability scanning tool [27]. WPScan is a software developed in the Ruby programming language, being a tool for scanning vulnerabilities in WordPress sites which was first created in 2011. With the use of WPScan, it is possible to perform a series of analyses and tests [28]. The simplest way to use this application is to clone its official repository on the Github platform. However, in our case, it is already available in the Debian-based Kali Linux distribution.

With this software, it is possible to enumerate several configurations that the website presents. Being a black box scanner it does not have access to the application's source code but uses enumeration techniques like the ones an attacker in real life would do, but in a more automatic way and directed only to WordPress applications. Some of the options that can be done during a scan are:

- Detecting the versions of WordPress, plugins and themes;

- Search and listing of usernames;

- Verification of weak passwords in use;

- Brute force attack simulation;

When developing a WordPress website it is possible to choose several components to build it, such as themes, plugins, and even the content management system version itself. These themes and plugins are developed independently, without supervision and each one has its own weaknesses. This combined with the fact that they are available to anyone makes them a very attractive entry point from an attacker's point of view. With WPScan it is possible to list all the plugins and themes present in an application, as well as the vulnerabilities of each one. After that, it is possible to explore each one of them to get the most out of it. As well as the WordPress version as each one presents different features and options and of course it also presents flaws.This obtaining of maximum information about the website is made through content analysis and several requests in order to obtain a desired behavior of the website. The reading of the headers pattern when compared with the headers patterns already known and included in the tool is one of the controls that allows us to understand which plugin and version is present on a page.

The listing of a username is a process in which one tries to detect a part of the access credentials to the administration page of a WordPress site. This attack looks for subtle differences in how the web application reacts to specific requests. Depending on the type of response it is possible to realize whether a user exists or not. While this alone does not present itself as a serious vulnerability, from the point of view of the attacker it represents half of the information necessary to have full control of the application. This tool also has the functionality to try a brute force attack to the user's password. In other words, this vulnerability can have great relevance in a larger attack.

By default, WordPress is vulnerable to user enumeration, which means that the developer needs to pay attention to this fragility, which is not the case most of the time. The option to run this enumeration in the WPScan tool is the ”***–enumerate u***” after establishing the URL. Three main approaches are used in this search. The first one is a consequence of a feature called permalinks that is established by default in WordPress. Permalinks are permanently defined URLs for individual publications and pages - *https://exampleurl.com/?p=123*, for example. In the same way, it is possible to list all the authors of the website using their ID, for example, *https://exampleurl.com/?author=1*. With this same URL, it is also possible to list all publications of the same user. It is possible to abuse this feature to find out which usernames are valid for a given WordPress website. Another way of detecting a valid username in this type of platforms is the message that is returned by it when a correct and incorrect user is entered and depending on the WordPress version present on the page. It is visible in the source code of the WPScan tool, available in ”**login_error_messages.rb**”, responsible for analyzing this vulnerability. Even in the first lines of the code of this one, it is possible to see comments that mention this detail. This option to find out the user names explores the relationship between the version of the CMS and the answer returned, in which for example, if the version is lower than *3.1*, extremely outdated, say, in case a valid username is entered and an incorrect password is returned the message ”Incorrect password”. This way it is possible for a malicious user to try with several parameters until the valid one is found.

The third approach mentioned in this work explores the relationship between WordPress and the possible plugins installed on the website. Several plugins use an XML sitemap that allows search engines to better understand the structure of the website so they can return pages faster. This sitemap works as an index that is automatically updated as content is added or deleted. With the proper path, it is possible to reach this map that also provides users unless the administrator disables this option. So by default WordPress websites with these plugins are also vulnerable to user enumeration using this technique.

Running these scans with the WordPress Vulnerability Database API set makes it possible to check detailed data on WordPress version vulnerabilities, plugin vulnerabilities, and theme vulnerabilities. This database is updated daily as new fragilities are discovered.

2.5.1 Information Systems

As studied before, a Security Information and Event Management is the core part of identifying and addressing cyber attacks. It works as a platform to manage infrastructure data in real-time, such as event monitoring, log management, and incident response. There has been a growing commitment on the part of security companies to develop this type of solutions, each with its own characteristics and features, suitable for different types of systems. Some of the solutions available in the market are described below.

ArcSight ESM

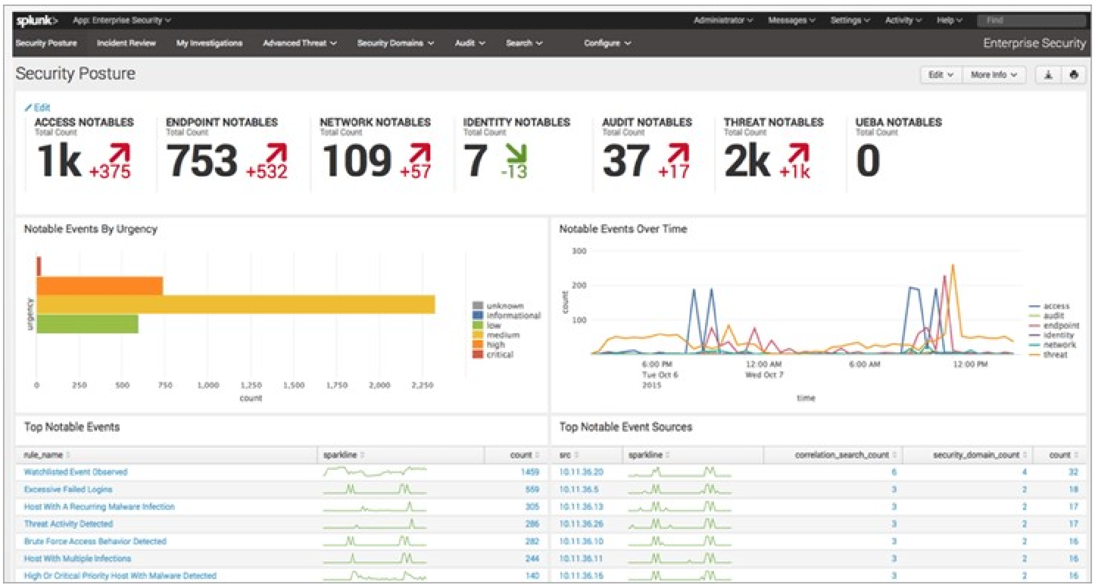
ArcSight Enterprise Security Manager [29] has features of distributed correlation and cluster view. It is good in sources ingestion as it supports more than 500 device types for analyzing the data. It is available through the appliance, software, AWS, and Microsoft Azure. Provides a distributed correlation by combining SIEM correlation engine with distributed cluster technology. For the data collection makes use of agents or connectors, supporting more than 300 of connectors. It is ideal for large IT environments because it enables the user to search through existing logs, making it a robust possibility with a built-in identity tracking program so that can it is possible to detect unwanted users on a network. It is one of the most popular SIEM tools available with its ability to compile log data and conduct extensive data analytics with real-time analysis of the system.

Alienvault ESM

Alienvault ESM [30] is the only platform with multiple security features, such as asset discovery and inventory, vulnerability assessment, intrusion detection, event correlation, log collection and management and compliance reports. As most of these solutions makes use of sensors and endpoint agents. One of the more unique aspects of Alienvault's solution is the Open Threat Exchange (OTX) which is a web page where users upload “indicators of compromise” (IOC) to help other users detect threats and suspicious activity, this works as a community to spread knowledge assess if there are any other users in the same situation. Another of its advantages is that it is one of the more competitively priced SIEM solutions with an intuitive and relatively easy to interact interface.

IBM QRadar

IBM has established itself one of the best companies in organiza-tion-driven security solutions and its SIEM software contains the core capabilities of these kind of systems and also already includes an user behavior analytics feature which permits to address insider threats [31]. All log management goes through one tool: QRadar Log Manager and it offers a suite of log management, analytics, data collection and intrusion detection to help security administrators maintain the network infrastructure secure. One of the main advantages of this solution is that it includes a risk modeling analytics, allowing to simulate potential attacks and monitor physical and virtual environments.



Top Notable Events

rule_name	sparkline	count
Watchlisted Event Observed		1459
Excessive Failed Logins		559
Host With A Recurring Malware Infection		305
Threat Activity Detected		286
Brute Force Access Behavior Detected		282
Host With Multiple Infections		244
High Or Critical Priority Host With Malware Detected		140

Top Notable Event Sources

src	sparkline	correlation_search_count	security_domain_count	count
10.11.36.20		6	4	32
10.11.36.5		3	2	18
10.11.36.13		3	2	17
10.11.36.26		3	2	17
10.11.36.10		3	2	16
10.11.36.11		3	2	16
10.11.36.16		3	2	16

Figure 2.5: Splunk dashboard view[32].

Splunk

Splunk[32] presents itself as one of the most popular SIEM solutions in the market. It has incorporated analytics and network and machine data can be monitored on a real-time basis as the system scans for potential vulnerabilities. It triggers alerts that can be defined by the user and tuned to match the organization needs. As interaction it counts with a very simple interface which first presents a basic overview of an incident before displaying in-depth observations on the event. The Asset Investigator feature flags for malicious actions using correlation rules, and allows the user to track and classify a security event. It works with any machine data, on cloud or on-premises and its automated actions and workflows enable a quick and assertive response to incidents.

The customization of dashboards and visualizations was one of the requirements and Splunk presents itself as the solution that best fills this gap in the available solutions. As far as the rest of the functionalities are concerned, all the tools presented work in a similar way, varying in the simplicity of their interface and a possible exclusive functionality. All of them have variable prices, which was also a selection criteria. After the gathering of all functionalities described above and the selection criteria, as well as the fact that it is available as soon as possible so that it can be implemented, tested and put into production, the solution chosen was Splunk.

2.6 Related Work on IT Security Monitoring

Several publications have been made over time on vulnerability and security monitoring in IT infrastructures. On [33][34][35][36] different methods used for intrusion detection and cybersecurity are discussed along with the most common breaches detected on infrastructures. When it comes to vulnerability analysis using penetration testing tools, used to discover breaches in systems, it is studied in [37][38][39] how it is possible to provide active cyber defence using Vulnerability Assessment and proactive actions taken to solve vulnerabilities and stop possible attack. In [40][41][42] some premium/open source VAPT tools have already been approached.

Related work to analysis of log events and how it can enable the detection of anomalous events relevant to cybersecurity have been studied previously in [43][44][45]. As the applicability of SIEM to analyze security events in previous publications [46][47][48]

In [49][50] the compliance of employees with the information security policy (ISP) of an organization and how it can improve end user's behavior is identified[51]. Social engineering attacks have already been discussed too in several publications helping to the conclusion that the human interaction is the weakest link in a cybersecurity environment [52][53][54][55].

2.7 Summary

In this chapter some fundamental concepts of Information Security were presented, such as its definition and properties. We also introduced the main vulnerabilities with greater impact on the infrastructure of most organizations, as well as the tools most commonly used for their analysis. Finally, a market study of the Security Information and Event Management solutions was made and the respective characteristics were presented.

In the next chapter the implementation of the chosen solution will be described and discussed, as well as evaluated using real scenarios.

Chapter 3

Deployment and Assessment of In-House SIEM

This chapter presents the first contribution of this thesis which consists of the deployment and evaluation of a SIEM in the IT infrastructure of the Municipality of Oeiras. Our objective is to develop a practical implementation of a SIEM tool to assess whether it is an added value to improve visibility in the infrastructure of the Municipality of Oeiras, giving its employees a better understanding of relevant events and incidents and at the same time make it safer. Next, we start by described the methodology for choosing an appropriate SIEM. We then present the entire deployment process of our selected SIEM: Splunk. We include a brief presentation of Splunk's architecture and highlight the steps that were necessary to implement it in our deployment scenario. Lastly, we describe some case studies put into practice, whose results will then serve to justify the conclusions and evaluations of this chapter.

3.1 Methodology

Choosing the SIEM technology to be deployed for monitoring the IT infrastructure of the Municipality of Oeiras required us to survey the existing SIEM tools in the seek of a tool that can maximize the level of scrutiny about the state of the network, computers, and services. At the present time, a purely manual or unassisted approach for examining this IT infrastructure has become impractical due to the complexity of these systems. Moreover, taking into account the Covid-19 pandemic, the Municipality had to adapt and send practically everyone to remote work. This further increased the difficulty of delineating a network perimeter and allowing IT Department personnel to have good visibility of the infrastructure.

For this it was necessary to perform a market study of which SIEM tool to choose. Every year Gartner Inc., a research company, publishes a report called “The Magic Quadrant for Security Information and Event Management”, where it examines the various advantages and disadvantages of each of the SIEM vendors with the most market share, according to the components “Ability to Execute” and “Completeness of Vision”. Figure 3.1 illustrates this analysis.

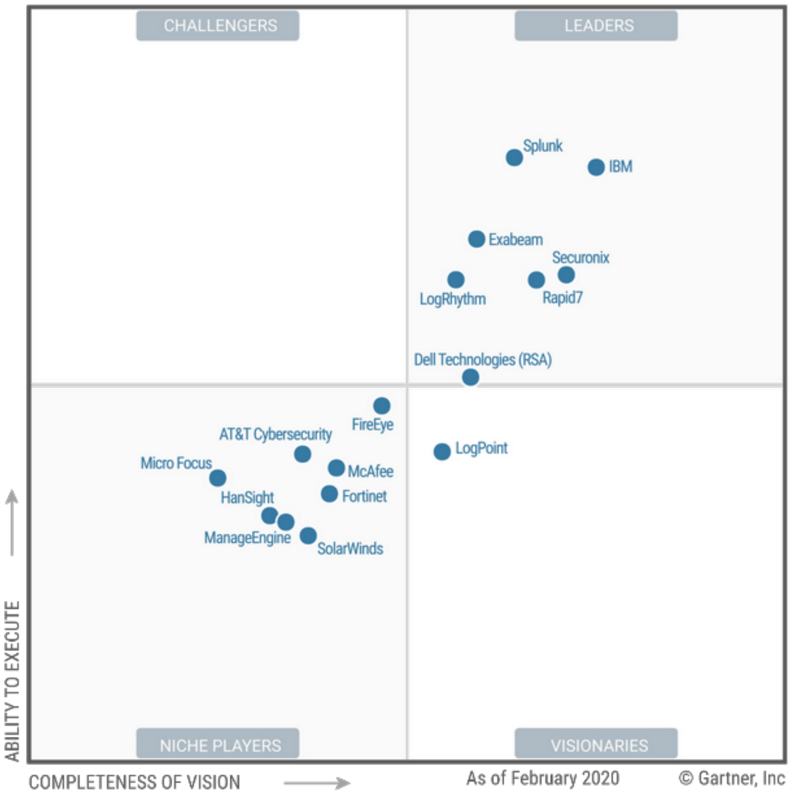


Figure 3.1: Gartner's SIEM Magic Quadrant [20]

According to the document [20], the "Ability to Execute" component evaluates criteria such as the tool's ability to provide features such as real-time monitoring, incident management, the ease with which deployment is done, price, vendor reliability in continuously maintaining the product, and the reported experience of other customers. Regarding the "Completeness of Vision" component, the study is done regarding the following criteria: the vendor's ability to respond by understanding the market needs and applying them to the product, as well as the marketing strategy carried out. This graph is divided into four market segments:

- **Niche Players:** vendors who provide SIEM platforms that are a good option for a specific use case, however, they are quite limited when it comes to investment and consequently functionality;
- **Visionaries:** this quadrant is composed of vendors that have a good ability to read and predict how the technology and their needs will evolve, although they are not as good in execution as the following segments;
- **Challengers:** composed of vendors that have several options of products or versions, that is, they have a lot of market presence and execution capacity, yet they are not outstanding in any specific ability;
- **Leaders:** this quadrant, as the name suggests, presents the market leaders, execution capacity, and investment possibility. These present the largest customer base, functionalities, and market vision, as well as constant capacity for innovation and vision. As a result, they are also able to offer the best customer experience.

Capabilities	Alienvault	IBM	Arcsight	Splunk
Architecture/Deployment	3.0	4.1	2.9	4.5
Cloud Readiness	3.1	4.1	2.9	4.0
Operations and Support	3.2	4.7	3.3	4.2
Data Management	2.9	4.0	2.9	4.0
Analytics	2.4	4.1	3.3	4.0
Response and Incident Management	2.7	3.8	3.0	3.7
Content Packaging and Management	2.7	4.0	2.9	4.2
Forensincs	2.8	3.7	2.9	3.6
User Experience and Interface	2.6	3.9	2.9	4.7
Total	**25.6**	**36.4**	**27.0**	**36.9**

Table 3.1: SIEM Rating on Critical Capabilites [56]

Another study, by the same company, which is also crucial for a better perception and comparison of the various functionalities of the SIEM tools is the “Critical Capabilities for Security Information and Event Management”, published annually. In this document, nine capabilities across SIEM technologies were evaluated. The result of this evaluation is presented in the table 3.1, having a metric scale between 1 and 5, being 5 the best score for each criterion.

After these two studies and without any further analysis, Splunk was the tool with the best qualities and possibilities to deliver the desired results. Additional factors favorable to the companies that joined the public bidding launched by the Oeiras Municipality for the acquisition of the license of this type of platform, the one that guaranteed to do it in the shortest time possible and with the lowest price, also presented the solution of Splunk. Although the possibility of technical support was common to all. The license acquired was from the Splunk Enterprise version which is the core product that allows the future addition of paid add-ons such as User Behavior Analytics which is a solution that helps companies to find internal threats and users with anomalous behavior. This version has all the features listed as necessary and allows you to collect, search, analyze, and view data from various types of sources and devices.

3.2 Deployment of Splunk

The following describe the steps taken to set up Splunk for the purpose of monitoring the IT infrastructure of the Municipality of Oeiras. First, we briefly present how we customized the architecture of Splunk for our targeted scenario. Then we describe the installation and configuration details of this system.

3.2.1 Customized Splunk Architecture

Splunk consists of three main components: Universal Forwarders, Indexer, and Search Head. The first one is present in the source and is responsible for collecting the information and then forwarding it to the Indexer, which is the component in charge of receiving, transforming, and organizing the information into an index. Upon request from the swearch head component it also looks for specific data. Finally, Search Head is responsible for interacting with the user and presenting the results back, after forwarding the requests to Indexer [57]. These results can be presented as tables, charts or even raw data. For searching, filtering and presentation of results, Splunk uses Search Processing Language (SPL), its own language developed for use in the tool, which is based on SQL and Unix syntax, with more than 140 commands [58]. Our implemented architecture is mirrored in the diagram depicted in Figure 3.2, composed of two indexers, a search head and a syslog server.

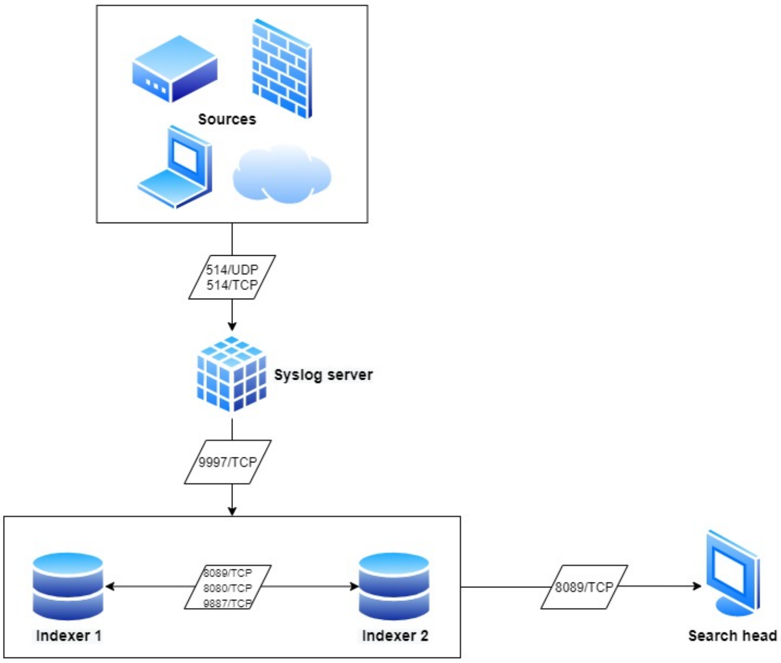


Figure 3.2: Splunk architecture.

For our implementation we chose to distribute the indexing task by two instances, thus creating two Indexers. Having this availability in the infrastructure allows a better distribution of resources in order to obtain greater speed in receiving information from sources since it is a large infrastructure where data is generated by several machines and more than one user may be making requests to the system.

One component that is not mandatory but which we have used in our deployment is a machine that will work as a Syslog server. Syslog is a client/server protocol for the transmission of messages whose destination is usually called Syslog daemon/server. The addition of this node allows receiving data from network and security equipment without agents installed, so-called *forwarders* when its configuration is not as simple and intuitive for example on a Windows Server. Moreover, it allows continuing to receive data from sources even when the Splunk service is down, for reasons of updates or new configurations. That is, the data is sent from the devices to the Syslog server which it then sent to the SIEM indexers.

The specifications of the components were sized taking into account the recommendations of the technical documentation of Splunk and for a comfortable use of infrastructure resources, without compromising the performance of the system [57]. Table 3.2 lists the CPU, memory, and storage resources available on the machines dedicated to each of Splunk's components.

Server	CPU	Memory	Storage
Syslog Server	2 cores	4GB	80GB
Indexer x 2	6 cores	16GB	1TB
Search Head	6 cores	16GB	30GB

Table 3.2: SIEM structure specification.

3.2.2 Splunk Installation and Configuration

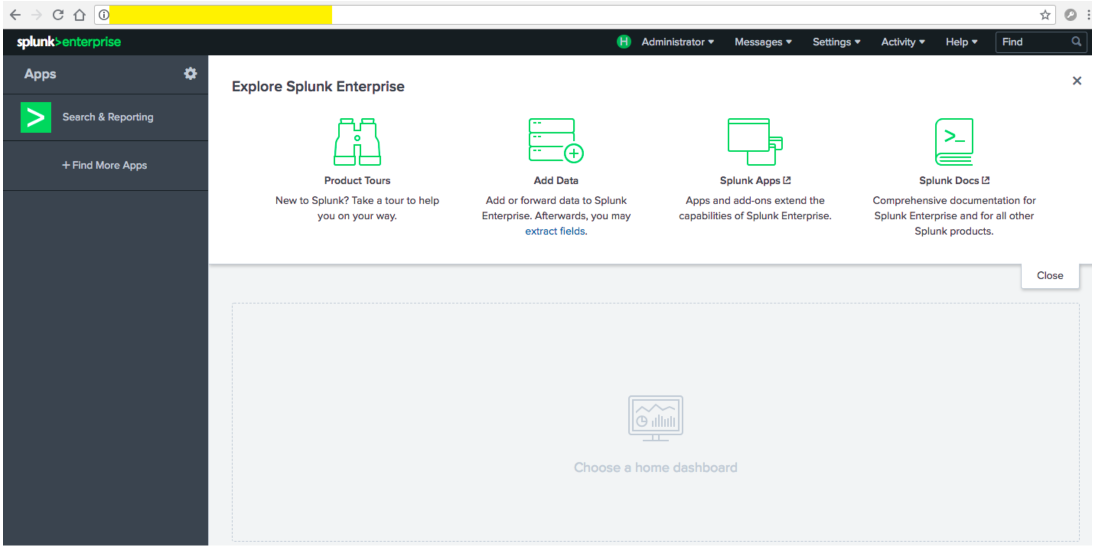
This section discusses all necessary changes and adjustments to Splunk's system components and software. To start the data collection process it was necessary to decide which nodes of the IT infrastructure of the Municipality of Oeiras would be in the scope of the SIEM build. Note that the ultimate goal of this part of the project is to create a SIEM that can correlate and link events that occur horizontally across multiple machines and vertically across multiple levels of infrastructure.

Once the critical services reported in Section 2.1 were listed, the identification of those that would be part of the system was done by conversation with the IT Department Network and Systems Administration teams. From this came the following prioritized data sources: i) the two Windows Domain Controllers,DC01 and DC02, ii) the Firewall, iii) the VPN. These form the foundation for a better visibility of internal events in the domain, with the two Domain Controllers, capable of recording all changes made at the level of user management and permissions of the various objects of the domain, the Firewall for a view of network interactions with the outside and vice versa and finally the VPN, a tool that employees placed in remote work use to connect to the infrastructure of the institution or even external companies that need to make an intervention.

After this analysis phase, it was possible to finally start the implementation of the project. To configure the Syslog server it was necessary to make sure that ***rsyslog*** service, native to the Linux operating system was running and then indicate in the configuration file located in the path ***../etc/rsyslog/conf.d*** the various IP addresses of the sources. However, to prevent the memory of this server from eventually filling up, the utility was configured ***logrotate*** allowing better management of log files [59]. This was configured to populate seven log files with information from Checkpoint Firewall and VPN, where each one of the files would represent one of the last seven hours of data. This information was rotated to a different file every hour, guaranteeing that in the one called **chkp.log** would always be the most recent information and in the **chkp.log.6** the oldest information.

At the Search Head the software downloaded from the vendor's website needed to be installed. After the initial setup, Splunk presents a UI accessible by browser at the address: ***http://serverip:8000***.

To forward events to the indexers it is necessary to execute the installation of the Universal Forwarder package also available on the vendor's website. This is the only configuration needed on the client side when using the forwarder, as was the case with Domain Controllers. On the server side, the input.conf file is necessary to choose which types of events you want to receive, and how to index it. Here, only security related events have been selected, such as permission changes of a user or Group Policies enforcement. In the case of the VPN and Firewall, which have the management console on the same



New to Splunk? Take a tour to help you on your way.

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk Enterprise.

Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

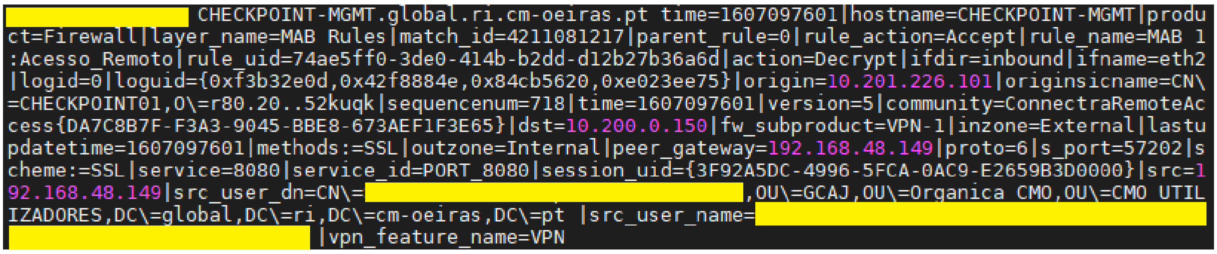
Figure 3.3: Splunk home screen.

machine, it was necessary to create a syslog exporter and on the Splunk side, install Checkpoint's native application for the platform in Search Head and Indexers.

The executed command on the management blade of the VPN and Firewall is the following:

cp_log_export add name exporter-syslog targetserver serverip target-port 514 protocol tcp format splunk readmode semi-unified

The event used to demonstrate the configuration and treatment of data focuses on account logon activities in the Municipality. The following listing, depicted in Figure 3.4, was extracted from the log file is an example of a VPN login. Note that the anonymized data is personal data of a user that has not been authorized for public processing within this work.



```
[redacted] CHECKPOINT-MGMT.global.ri.cm-oeiras.pt time=1607097601|hostname=CHECKPOINT-MGMT|produ
ct=Firewall|layer_name=MAB Rules|match_id=4211081217|parent_rule=0|rule_action=Accept|rule_name=MAB 1
:Acesso_Remoto|rule_uid=74ae5ff0-3de0-414b-b2dd-d12b27b36a6d|action=Decrypt|ifdir=inbound|ifname=eth2
|logid=0|loguid={0xf3b32e0d,0x42f8884e,0x84cb5620,0xe023ee75}|origin=10.201.226.101|originsicname=CN\
=CHECKPOINT01,O\=r80.20..52kuqk|sequencenum=718|time=1607097601|version=5|community=ConnectraRemoteAc
cess{DA7C8B7F-F3A3-9045-BBE8-673AEF1F3E65}|dst=10.200.0.150|fw_subproduct=VPN-1|inzone=External|lastu
pdatetime=1607097601|methods:=SSL|outzone=Internal|peer_gateway=192.168.48.149|proto=6|s_port=57202|s
cheme:=SSL|service=8080|service_id=PORT_8080|session_uid={3F92A5DC-4996-5FCA-0AC9-E2659B3D0000}|src=1
92.168.48.149|src_user_dn=CN\=[redacted],OU\=GCAJ,OU\=Organica CMO,OU\=CMO UTIL
IZADORES,DC\=global,DC\=ri,DC\=cm-oeiras,DC\=pt |src_user_name=[redacted]
 |vpn_feature_name=VPN
```

Figure 3.4: Example of VPN session login log.

The first step in dealing with this type of event is to determine which elements are relevant to be processed by the SIEM. The amount of information that arrives per second in the system required that only the necessary information is collected and kept in processing. The relevant fields for future analysis are present in the following table:

This data is evaluated in the content of the fields and the evaluation of the results can only be done through validation and use of the fields. The main fields that were identified were the name of the sensor

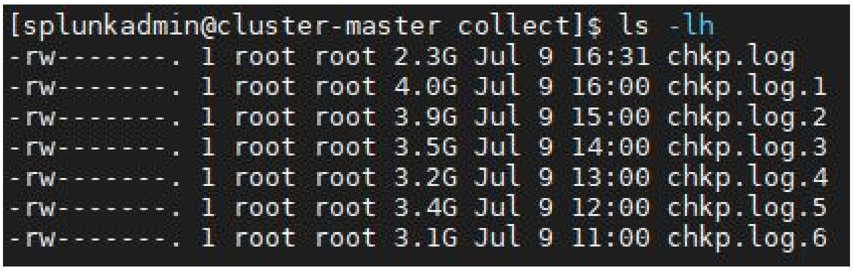
Field	**Type**	**Value**
Time	Timestamp	1607097601
The time the event was received by the VPN manager		
HostName	String	CHECKPOINT-MGMT
The name of the source host that received the event		
Product	String	Firewall
The device that generated the event		
Rule_Name	String	MAB 1:Acesso_Remoto
The rule of the firewall that allowed the event to occur		
Src	Integer	10.201.226.101
The IP address of the source host		
Dst	Integer	10.200.0.150
The IP address of the destination host		
Fw_Subproduct	String	VPN-1
The name of the sensor that originated the event		
S_Port	Integer	57202
Port on the origin of the event from the source machine		
Src_User_Dn	String	GJAC
Domain information about the user (example shown is pseudonymised)		
Src_User_Name	String	Ana Paula Silva
The username associated with the event (example shown is pseudonymised)		

Table 3.3: VPN login data fields.

that generated the event, the IP addresses and the user information like name and domain data.

At this point in the project, we were faced with a problem that we were not aware of. The team responsible for hiring the Security Information and Event Management license improperly forecast the size of the information that need to be uploaded into the platform. This translated into the number of sources and amount of data that could be redirected to the system as the contracted license proved to be quite short in order to cover all the needs of the Municipality, whose ultimate goal was to be able to correlate events that take place in the infrastructure at all levels. The license purchased consisted of a limit of 15GB of data per day allowed for treatment in Splunk. This limit was exceeded everyday in about 5 hours, solely with the data from the VPN and Firewall, given that most of the Municipality's collaborators were remote working.

This made it impossible to configure all the previously discussed sources in the SIEM. A new hiring process was started with a daily data value of 100GB. However, it was finalized it was necessary to



```
[splunkadmin@cluster-master collect]$ ls -lh
-rw-------. 1 root root 2.3G Jul 9 16:31 chkp.log
-rw-------. 1 root root 4.0G Jul 9 16:00 chkp.log.1
-rw-------. 1 root root 3.9G Jul 9 15:00 chkp.log.2
-rw-------. 1 root root 3.5G Jul 9 14:00 chkp.log.3
-rw-------. 1 root root 3.2G Jul 9 13:00 chkp.log.4
-rw-------. 1 root root 3.4G Jul 9 12:00 chkp.log.5
-rw-------. 1 root root 3.1G Jul 9 11:00 chkp.log.6
```

Figure 3.5: VPN and firewall log files size.

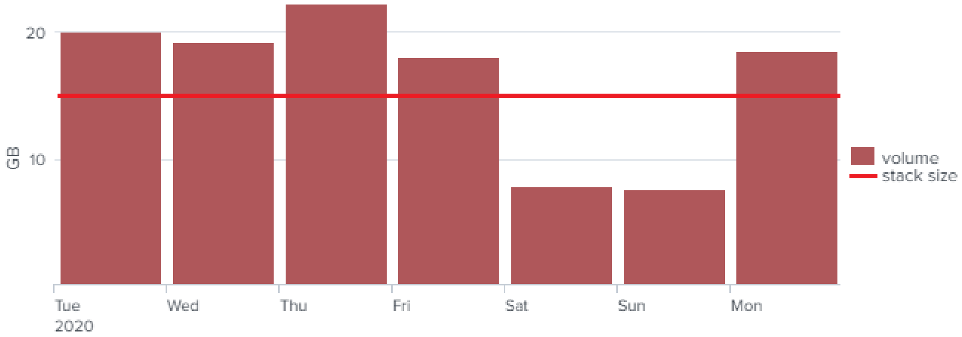


Figure 3.6: Average daily license usage per week.

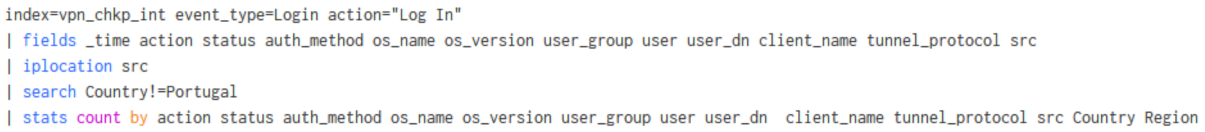
decide which sources to load the system with. Once again, the context in which most employees found themselves derived the decision to upload information from the VPN instead of other sources of input. Given this, all the implementation and evaluation of Splunk technology, presented here, was affected by the constraint of only using one data source.

3.3 Security Event Analysis

The ability to create alerts served as criteria of choice of the best software to use. For the demonstration and analysis of this functionality, taking into account the fact that most of the municipality's employees were teleworking, some rules were developed to test a few scenarios. These events extracted from the platform were collected from the VPN. In particular, we configured Splunk with rules to trigger alerts for three specific events: successful logins from foreign countries, VPN brute-force login attempts, and webmail brute-force login attempts. Next, we provide an account on how these rules were set up and present our main findings while running Splunk for the time period between June and September.

3.3.1 Success Login from Foreign Country

The first developed alert exploits the information of an access login after being handled by the platform which was created in order to understand where this same access had been made from. It arose from the need to try to minimize the risks of having the network security perimeter completely open, with some employees having to work with personal computers whose content and state is unknown. This rule aims to understand or at least help define whether a given access is made from a given country by



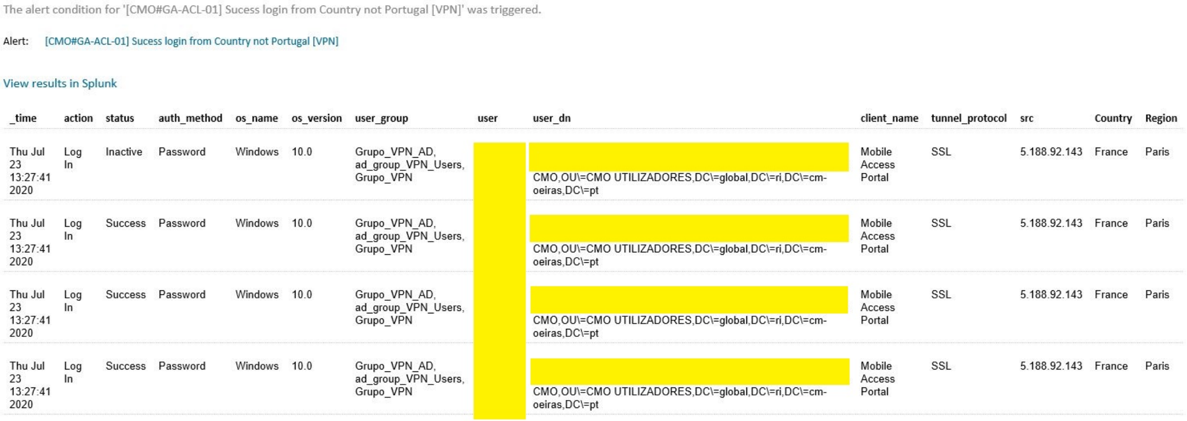
```
index=vpn_chkp_int event_type=Login action="Log In"
| fields _time action status auth_method os_name os_version user_group user user_dn client_name tunnel_protocol src
| iplocation src
| search Country!=Portugal
| stats count by action status auth_method os_name os_version user_group user user_dn  client_name tunnel_protocol src Country Region
```

Figure 3.7: Search rule that alerts for undue access.

someone who is or is not in that geographical point, is undue or not, confirmed later contacting the user.

The search rule that should trigger the alert is written in the previously mentioned SPL language and takes advantage of Checkpoint's add-on capability to transform the information sent to it into a standard form after the relevant fields are given. Events related to VPN index and Login event type are filtered and data fields like time, status, auth_method, os_name, user_group and user_dn are extracted. Then the location of the source host is calculated taking into account the IP address with the src field, to which we just asked to be returned access information outside Portugal. Finally, the data is grouped by the same fields from which information was extracted.

After some time an alert was received in the email box configured for this purpose. The alert included a login made by a user's account with an IP address located in France, more specifically in Paris. The following image shows a screenshot of the alert email:



The alert condition for '[CMO#GA-ACL-01] Sucess login from Country not Portugal [VPN]' was triggered.

Alert: [CMO#GA-ACL-01] Sucess login from Country not Portugal [VPN]

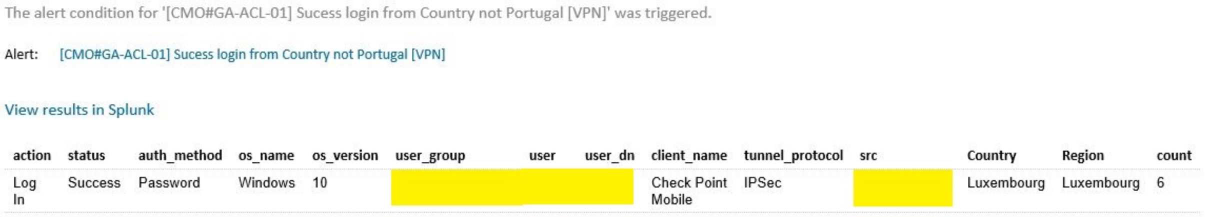
View results in Splunk

_time	action	status	auth_method	os_name	os_version	user_group	user	user_dn	client_name	tunnel_protocol	src	Country	Region
Thu Jul 23 13:27:41 2020	Log In	Inactive	Password	Windows	10.0	Grupo_VPN_AD, ad_group_VPN_Users, Grupo_VPN	[redacted]	[redacted] CMO,OU\=CMO UTILIZADORES,DC\=global,DC\=ri,DC\=cm-oeiras,DC\=pt	Mobile Access Portal	SSL	5.188.92.143	France	Paris
Thu Jul 23 13:27:41 2020	Log In	Success	Password	Windows	10.0	Grupo_VPN_AD, ad_group_VPN_Users, Grupo_VPN	[redacted]	[redacted] CMO,OU\=CMO UTILIZADORES,DC\=global,DC\=ri,DC\=cm-oeiras,DC\=pt	Mobile Access Portal	SSL	5.188.92.143	France	Paris
Thu Jul 23 13:27:41 2020	Log In	Success	Password	Windows	10.0	Grupo_VPN_AD, ad_group_VPN_Users, Grupo_VPN	[redacted]	[redacted] CMO,OU\=CMO UTILIZADORES,DC\=global,DC\=ri,DC\=cm-oeiras,DC\=pt	Mobile Access Portal	SSL	5.188.92.143	France	Paris
Thu Jul 23 13:27:41 2020	Log In	Success	Password	Windows	10.0	Grupo_VPN_AD, ad_group_VPN_Users, Grupo_VPN	[redacted]	[redacted] CMO,OU\=CMO UTILIZADORES,DC\=global,DC\=ri,DC\=cm-oeiras,DC\=pt	Mobile Access Portal	SSL	5.188.92.143	France	Paris

Figure 3.8: Alert email triggered by the defined rule.

At this point, it was necessary to contact the worker to try to find out whether access was legitimate or not. After a brief phone call it was possible to conclude that he was in Portugal and did not have any other Virtual Private Network or software that would allow him to mask the geographic location of the computer present on it. Given this, the first step put in place was to block the account in question and not activate it again before being forced to change the password. In case of a complete configuration of the SIEM platform, with a license capable of hosting all the critical services listed above, it will be possible to correlate the activity with to the account in question. The remaining steps taken in this situation have not been authorized to be made public in this thesis.

This type of rule can also trigger alerts to situations of legitimate accesses, such as employees who are in remote work outside Portugal or even companies hired to provide services in the Municipality



The alert condition for '[CMO#GA-ACL-01] Sucess login from Country not Portugal [VPN]' was triggered.

Alert: [CMO#GA-ACL-01] Sucess login from Country not Portugal [VPN]

View results in Splunk

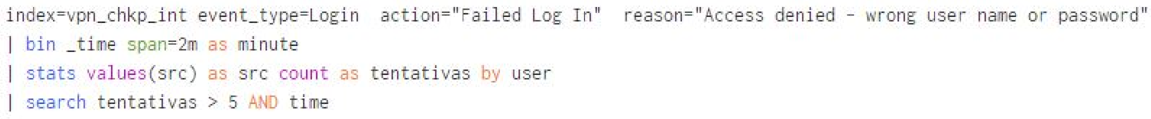
action	status	auth_method	os_name	os_version	user_group	user	user_dn	client_name	tunnel_protocol	src	Country	Region	count
Log In	Success	Password	Windows	10	[redacted]	[redacted]	[redacted]	Check Point Mobile	IPSec	[redacted]	Luxembourg	Luxembourg	6

Figure 3.9: Email alert that proved to be a false positive.

who present employees in this situation as well. This situation occurred sometimes with a company that provided software development services in the IT Department and had an employee who was in Luxembourg. For this specific situation, the rule above was adapted to exclude events from the alerts with that user located in Luxembourg. The ***"AND"*** condition also includes in the results the accesses of that account in which both restrictions were not verified simultaneously.

3.3.2 VPN Brute-force Login Attempt

This alert was developed to detect cases where the same user account had several failed VPN login attempts in a short time. This kind of situations can be translated in the so-called brute force attack [60]. For this the following rule was implemented and put into production:

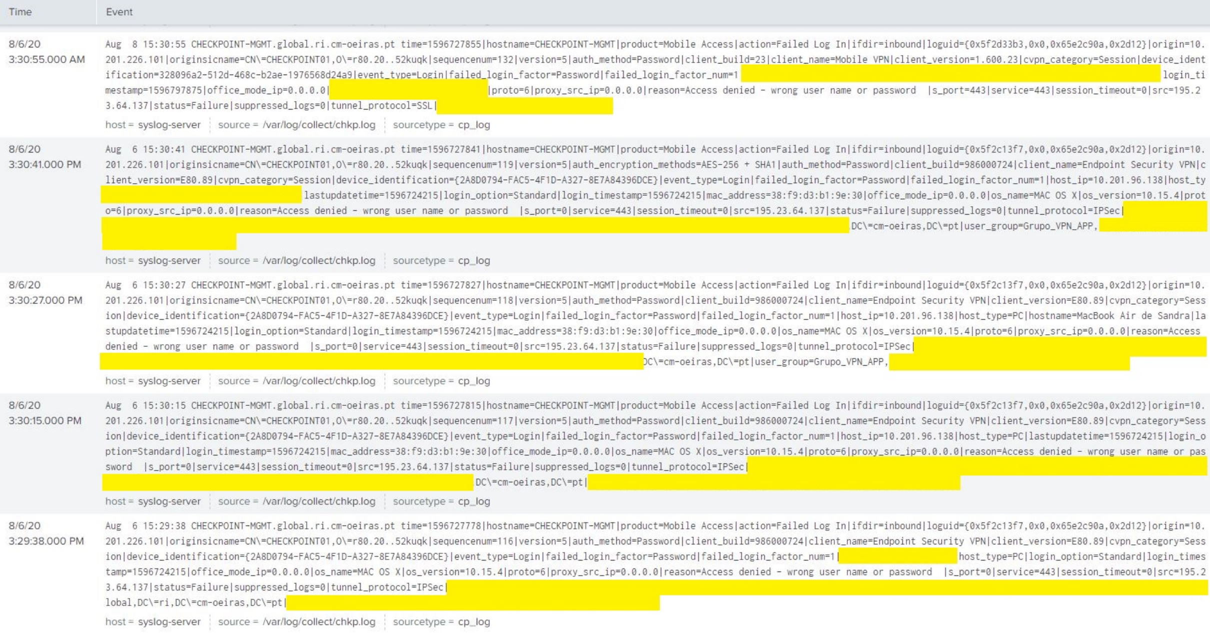


```
index=vpn_chkp_int event_type=Login  action="Failed Log In"  reason="Access denied - wrong user name or password"
| bin _time span=2m as minute
| stats values(src) as src count as tentativas by user
| search tentativas > 5 AND time
```

Figure 3.10: Search rule that alerts for several attempts of login.

Events related to VPN index and Login event type were filtered and data fields like action, and the reason for that was extracted as well. The time range for this alert to be triggered was set to 2 minutes. The number of attempts was calculated taking into account the same user account to which we just asked to be returned those cases where there were more than five failed attempts. Next, the data was grouped and returned by the same fields from which information was extracted. This alert was also triggered some time after being put into production. It stated that a user account had 6 failed attempts of login in the VPN.

Figure 3.11 depicts the logs that made such a situation detectable in the Splunk software. It is possible to see that the first attempt has the time of 15:29:38 and the fifth attempt with the time of 15:30:55. These events meet the criteria defined in the rule for a possible brute force attack. As in the previous case, we contacted the user in question to understand whether this situation was known to him or not. And as before, this situation also corresponded to an illegitimate case of attempted access. With this in mind, the first measures taken were also similar, with the account being blocked and the respective password replaced. Following this event, the Network Administration team, which is in charge of managing the VPN, was advised to configure the maximum number of five failed access attempts for



```
Time                Event
8/6/20              Aug  8 15:30:55 CHECKPOINT-MGMT.global.ri.cm-oeiras.pt time=1596727855|hostname=CHECKPOINT-MGMT|product=Mobile Access|action=Failed Log In|ifdir=inbound|loguid={0x5f2d33b3,0x0,0x65e2c90a,0x2d12}|origin=10.
3:30:55.000 AM      201.226.101|originsicname=CN\=CHECKPOINT01,O\=r80.20..52kuqk|sequencenum=132|version=5|auth_method=Password|client_build=23|client_name=Mobile VPN|client_version=1.600.23|cvpn_category=Session|device_ident
                    ification=328096a2-512d-468c-b2ae-1976568d24a9|event_type=Login|failed_login_factor=Password|failed_login_factor_num=1 [redacted] login_ti
                    mestamp=1596797875|office_mode_ip=0.0.0.0|[redacted]|proto=6|proxy_src_ip=0.0.0.0|reason=Access denied - wrong user name or password  |s_port=443|service=443|session_timeout=0|src=195.2
                    3.64.137|status=Failure|suppressed_logs=0|tunnel_protocol=SSL|[redacted]
                    host = syslog-server  source = /var/log/collect/chkp.log  sourcetype = cp_log
8/6/20              Aug  6 15:30:41 CHECKPOINT-MGMT.global.ri.cm-oeiras.pt time=1596727841|hostname=CHECKPOINT-MGMT|product=Mobile Access|action=Failed Log In|ifdir=inbound|loguid={0x5f2c13f7,0x0,0x65e2c90a,0x2d12}|origin=10.
3:30:41.000 PM      201.226.101|originsicname=CN\=CHECKPOINT01,O\=r80.20..52kuqk|sequencenum=119|version=5|auth_encryption_methods=AES-256 + SHA1|auth_method=Password|client_build=986000724|client_name=Endpoint Security VPN|c
                    lient_version=E80.89|cvpn_category=Session|device_identification={2A8D0794-FAC5-4F1D-A327-8E7A84396DCE}|event_type=Login|failed_login_factor=Password|failed_login_factor_num=1|host_ip=10.201.96.138|host_ty
                    [redacted] lastupdatetime=1596724215|login_option=Standard|login_timestamp=1596724215|mac_address=38:f9:d3:b1:9e:30|office_mode_ip=0.0.0.0|os_name=MAC OS X|os_version=10.15.4|prot
                    o=6|proxy_src_ip=0.0.0.0|reason=Access denied - wrong user name or password  |s_port=0|service=443|session_timeout=0|src=195.23.64.137|status=Failure|suppressed_logs=0|tunnel_protocol=IPSec|[redacted]
                    DC\=cm-oeiras,DC\=pt|user_group=Grupo_VPN_APP,[redacted]
                    host = syslog-server  source = /var/log/collect/chkp.log  sourcetype = cp_log
8/6/20              Aug  6 15:30:27 CHECKPOINT-MGMT.global.ri.cm-oeiras.pt time=1596727827|hostname=CHECKPOINT-MGMT|product=Mobile Access|action=Failed Log In|ifdir=inbound|loguid={0x5f2c13f7,0x0,0x65e2c90a,0x2d12}|origin=10.
3:30:27.000 PM      201.226.101|originsicname=CN\=CHECKPOINT01,O\=r80.20..52kuqk|sequencenum=118|version=5|auth_method=Password|client_build=986000724|client_name=Endpoint Security VPN|client_version=E80.89|cvpn_category=Sess
                    ion|device_identification={2A8D0794-FAC5-4F1D-A327-8E7A84396DCE}|event_type=Login|failed_login_factor=Password|failed_login_factor_num=1|host_ip=10.201.96.138|host_type=PC|hostname=MacBook Air de Sandra|la
                    stupdatetime=1596724215|login_option=Standard|login_timestamp=1596724215|mac_address=38:f9:d3:b1:9e:30|office_mode_ip=0.0.0.0|os_name=MAC OS X|os_version=10.15.4|proto=6|proxy_src_ip=0.0.0.0|reason=Access
                    denied - wrong user name or password  |s_port=0|service=443|session_timeout=0|src=195.23.64.137|status=Failure|suppressed_logs=0|tunnel_protocol=IPSec|[redacted]
                    DC\=cm-oeiras,DC\=pt|user_group=Grupo_VPN_APP,[redacted]
                    host = syslog-server  source = /var/log/collect/chkp.log  sourcetype = cp_log
8/6/20              Aug  6 15:30:15 CHECKPOINT-MGMT.global.ri.cm-oeiras.pt time=1596727815|hostname=CHECKPOINT-MGMT|product=Mobile Access|action=Failed Log In|ifdir=inbound|loguid={0x5f2c13f7,0x0,0x65e2c90a,0x2d12}|origin=10.
3:30:15.000 PM      201.226.101|originsicname=CN\=CHECKPOINT01,O\=r80.20..52kuqk|sequencenum=117|version=5|auth_method=Password|client_build=986000724|client_name=Endpoint Security VPN|client_version=E80.89|cvpn_category=Sess
                    ion|device_identification={2A8D0794-FAC5-4F1D-A327-8E7A84396DCE}|event_type=Login|failed_login_factor=Password|failed_login_factor_num=1|host_ip=10.201.96.138|host_type=PC|lastupdatetime=1596724215|login_o
                    ption=Standard|login_timestamp=1596724215|mac_address=38:f9:d3:b1:9e:30|office_mode_ip=0.0.0.0|os_name=MAC OS X|os_version=10.15.4|proto=6|proxy_src_ip=0.0.0.0|reason=Access denied - wrong user name or pas
                    sword  |s_port=0|service=443|session_timeout=0|src=195.23.64.137|status=Failure|suppressed_logs=0|tunnel_protocol=IPSec|[redacted]
                    DC\=cm-oeiras,DC\=pt|[redacted]
                    host = syslog-server  source = /var/log/collect/chkp.log  sourcetype = cp_log
8/6/20              Aug  6 15:29:38 CHECKPOINT-MGMT.global.ri.cm-oeiras.pt time=1596727778|hostname=CHECKPOINT-MGMT|product=Mobile Access|action=Failed Log In|ifdir=inbound|loguid={0x5f2c13f7,0x0,0x65e2c90a,0x2d12}|origin=10.
3:29:38.000 PM      201.226.101|originsicname=CN\=CHECKPOINT01,O\=r80.20..52kuqk|sequencenum=116|version=5|auth_method=Password|client_build=986000724|client_name=Endpoint Security VPN|client_version=E80.89|cvpn_category=Sess
                    ion|device_identification={2A8D0794-FAC5-4F1D-A327-8E7A84396DCE}|event_type=Login|failed_login_factor=Password|failed_login_factor_num=1|[redacted] host_type=PC|login_option=Standard|login_times
                    tamp=1596724215|office_mode_ip=0.0.0.0|os_name=MAC OS X|os_version=10.15.4|proto=6|proxy_src_ip=0.0.0.0|reason=Access denied - wrong user name or password  |s_port=0|service=443|session_timeout=0|src=195.2
                    3.64.137|status=Failure|suppressed_logs=0|tunnel_protocol=IPSec|[redacted]
                    lobal,DC\=ri,DC\=cm-oeiras,DC\=pt|[redacted]
                    host = syslog-server  source = /var/log/collect/chkp.log  sourcetype = cp_log
```

Figure 3.11: Logs of failed attempts of login.

a given account. Although the Splunk alert allowed to gain knowledge of this type of situations, a block in the management console allows to prevent an eventual brute force attack to succeed.

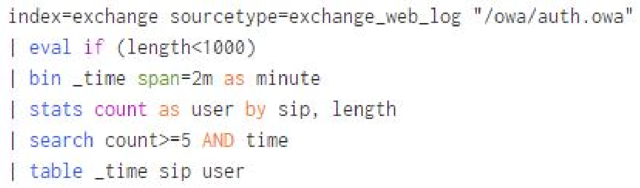
3.3.3 Webmail Brute-force Login Attempt

This case study was one that was planned to be developed and implemented, but due to the previously detailed issue of license limitations it was not actually possible to do so. However, it will be detailed as if this had been done, to the possible extent.

One of the tools available to the municipality's employees in a public way, i.e, without having to be connected to its private network, is webmail. This service has the same functionalities as the e-mail service installed in each one's computers and is available with a URL access using the user's credentials. This public availability of the service also presents disadvantages, namely the fact that it is public and can represent an entry point to the rest of the Municipality's network infrastructure. This, combined again with the situation caused by the pandemic context and the circumstances in which some of the employees had to work, proved to be a concern from the security assessment point of view. For this and with Splunk working at its fullest, it would be a best practice to have in production a rule that would trigger an alert for an attempted brute force attack on a user's email account, through the webmail portal. To configure this rule it is necessary to analyze a log of a login access to Outlook Webmail, a Microsoft Exchange service. The following log represents a real case of an access, although pseudonomized for security reasons:

1.1.1.1, Jose, 08/26/2020, 13:45:05, ExchangeServer, 10.10.10.10, 613, 302, POST, /owa/auth.owa

The first field is the source IP address, the second is the username, the time of the login, the hostname of the destination server, the response time length, the status code and the last field is the access link. This way, we could create the following rule to analyze the events of authentication attempt:



```
index=exchange sourcetype=exchange_web_log "/owa/auth.owa"
| eval if (length<1000)
| bin _time span=2m as minute
| stats count as user by sip, length
| search count>=5 AND time
| table _time sip user
```

Figure 3.12: Rule to alert to webmail brute force attacks.

The events would be filtered by length of response time, that is smaller when an authentication attempt is unsuccessful, allowing five attempts in a two minute time span per user. This rule would alert to possible dictionary attacks or so-called brute force attacks on the Municipality's webmail service.

3.4 Summary

This chapter aimed to discuss the implementation of a SIEM system, detail its architecture and finally test its capabilities and functionality in the Municipality of Oeiras. The limitation described in Section 3.3.2 ended up influencing the possibility of testing to which the technology could have been subjected, making it impossible to correlate events. However, together with the fact that the Municipality's VPN was being used by most of the workforce, this would always be one of the services to be tested regarding integration with the platform. As well as the use of webmail which increased substantially due to its public availability. In the first case, two alerts were developed to test VPN access by a country other than Portugal and also that of several failed authentication attempts within two minutes. Both situations were put into production and promptly alerted by Splunk, however it was not possible to correlate any further data in other services related to the user accounts in question, because of the restriction documented earlier. In the case of webmail, a hypothetical rule was developed that would also allow alerting to a brute force attack, analyzing access logs and the SPL language.

The tool provided visualization, alarm generation, and event management which facilitated the tracking of security-related incidents. Although it was not possible to evaluate it at its maximum extent, the platform is able to integrate with any kind of security event source, including the presence of some native add-ons for sources such as Checkpoint Firewall and Microsoft Active Directory, with some additional knowledge of the associated syntax and environment. However, it takes a significant time to implement and develop the rules, it can also create a high amount of false positive alerts and most of its performance depends on the quality of the data, that is, the logs.

In summary, the results presented in this chapter suggest that a SIEM is a technology that when well deployed and maintained can be helpful to increase the knowledge of the events that occurred in the infrastructure, but it is not a tool designed to improve the security of a certain network.

Chapter 4

Vulnerability Assessment

This chapter presents the second contribution of this work, i.e., an analysis of vulnerabilities present in the IT infrastructure of the Municipality of Oeiras. To this end, we intend to make use of some of the most widely used vulnerability scanning tools available in the market. We aim to make an analysis of it, study their possible impacts on the infrastructure, and define measures for them. This need comes from the peculiarities that present themselves in this institution. First, the network architecture has scaled in a rather unstructured and heterogeneous way. In addition, the installed software does not follow a development cycle considering security policies. Often, this development is also contracted to external companies, whose priority is functionality and not so much on security. In the following, we clarify our methodology, and then present our results by the types of vulnerabilities we found.

4.1 Methodology

Pentesting tools are used to discover vulnerabilities on networked computer systems. These tools were used through a virtual machine deployed in the main infrastructure network of the Municipality of Oeiras. Some of these tools are already in the installed Kali Linux distribution. Our objective is to cover various types of vulnerabilities, using these tools and analyze their possible impact on the institution. The tools used have already been described in Section 2.5.

Vulnerability testing was carried out on Municipality-owned web sites and also on websites hosted externally too. The testing was held for a period of 7 months from February to August 2020. For privacy reasons, the website url, name of the website and IP address will be anonymized in this document. The process was conducted as follows: we started by using a selected tool to discover vulnerabilities in the desired component. Then we made a study of the vulnerability found, its severity, and possible impact on the infrastructure. Finally, we outlined a plan of measures to resolve this same flaw.

4.2 SSL/TLS Certificates

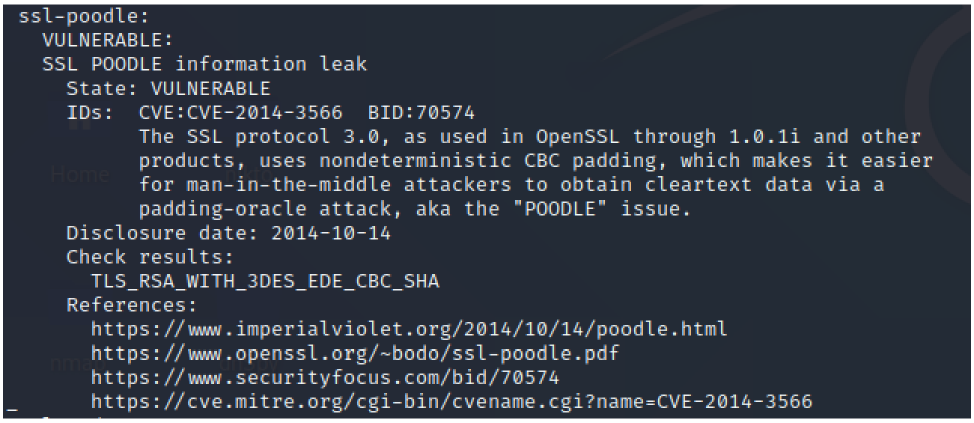
The first type of vulnerabilities that we found is related to SSL/TLS certificates. These were found by manual inspection and without the use of any of the tools indicated above. Only then, for confirmation, a testing software tool was used, which is available online and completely free, SSL Server Test from Qualys [61]. During the recognition phase of the resources that would be targeted by the analysis of vulnerabilities, it was possible to detect that some the resources of the Municipality had insecure configurations from the point of view of SSL/TLS certificates.

Secure Socket Layer (SSL) and its successor Transport Socket Layer (TLS) intend to deliver secure end-to-end communication over the Internet [62]. Based on the model of public keys infrastructures and certificates, it was developed to ensure confidentiality, authenticity and integrity of communications. When a browser connects to a website using TLS, it asks the server to authenticate itself, or confirm its identity. This authentication process uses cryptography to verify that a trusted independent third party, or certificate authority, has registered and identified the server. This mechanism is also used to protect the data that is sent, keeping it confidential and verify its integrity. When analyzing SSL/TLS it is necessary to consider which versions are considered secure and which ones are not. SSL versions 1.0, 2.0 and 3.0 have all been considered insecure[63]. The TLS protocol is considered an evolution of SSL. Although TLS's first two versions are already considered deprecated, versions 1.2 and 1.3 are considered secure. Thus, so for this work, we consider all previous versions insecure.

In the IT infrastructure of the Municipality of Oeiras it was possible to check that some websites did not present certificates, thus maintaining insecure communications. Some others presented certificates with outdated protocol versions, or even self-signed certificates and wildcards, concepts that will be explained later. We were able to confirm this through an online testing tool to SSL configuration of servers.

Vulnerability to DROWN and POODLE attacks: One of the websites (among several others) presented a certificate that makes use not only of the SSL version 3.0 and TLS 1.0 and 1.1, (all insecure) but also TLS 1.2 which is a recommended version. Since this test was made a few days before version 1.1 became officialy deprecated, the software only gives it a warning state. Two of the vulnerabilities to which this type of certificate is subjected to are the *DROWN* and *POODLE* attacks [64]. The first was discovered in 2016 and its name comes from Decrypting RSQ with Obsolete and Weakened Encryption (DROWN). The attack allows the attacker to break the encryption and obtain passwords or sensitive information that is being exchanged in communication [65].

Regarding the POODLE attack, it makes use of the fact that some TLS clients, to interact with legacy servers, offer older protocol versions, such as SSL 3.0, at the time of the initial handshake. This version presents a weakness that can be exploited by a ”man-in-the-middle” attacker to decrypt secure HTTP cookies. To achieve this it is necessary to run a JavaScript agent on the website concerned, so that the victim's browser starts HTTPS requests, and thus intercept and modify SSL records sent by the browser. If this record is accepted, the attacker can decrypt a byte of the cookies [64]. With the Nmap tool we can also check that this webserver is vulnerable to this attack. Using the command **nmap -sV –script=vuln**

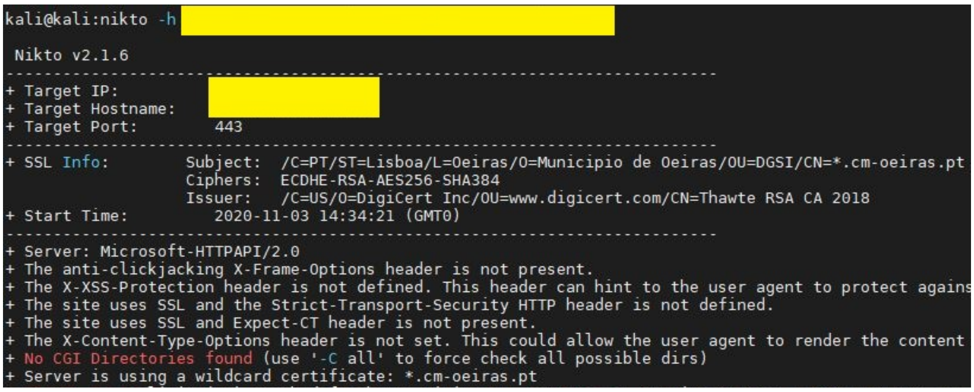


```
ssl-poodle:
  VULNERABLE:
  SSL POODLE information leak
    State: VULNERABLE
    IDs:  CVE:CVE-2014-3566  BID:70574
          The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
          products, uses nondeterministic CBC padding, which makes it easier
          for man-in-the-middle attackers to obtain cleartext data via a
          padding-oracle attack, aka the "POODLE" issue.
    Disclosure date: 2014-10-14
    Check results:
      TLS_RSA_WITH_3DES_EDE_CBC_SHA
    References:
      https://www.imperialviolet.org/2014/10/14/poodle.html
      https://www.openssl.org/~bodo/ssl-poodle.pdf
      https://www.securityfocus.com/bid/70574
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
```

Figure 4.1: Presence of the vulnerability POODLE confirmed.

webserverip, which makes use of the ”vuln” script available for the tool. This script enhances Nmap’s ability to produce relevant Common Vulnerabilities and Exposures [66] information about the services discovered in the host target.

For these vulnerabilities the only recommendation and that was made to the Infrastructure team, is to update the certificate to one that uses the versions considered safe.



```
kali@kali:nikto -h [redacted]

 Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          [redacted]
+ Target Hostname:
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=PT/ST=Lisboa/L=Oeiras/O=Municipio de Oeiras/OU=DGSI/CN=*.cm-oeiras.pt
                   Ciphers:  ECDHE-RSA-AES256-SHA384
                   Issuer:   /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=Thawte RSA CA 2018
+ Start Time:         2020-11-03 14:34:21 (GMT0)
---------------------------------------------------------------------------
+ Server: Microsoft-HTTPAPI/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect agains
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server is using a wildcard certificate: *.cm-oeiras.pt
```

Figure 4.2: Wildcard certificate configured in a website.

Vulnerability to wildcard reuse attacks: Figure 4.2 ilustrates the presence of another insecure practice regarding the configuration and implementation of SSL/TLS certificates in the infrastructure which allowed to assume the reuse of a ”wildcard” certificate in several subdomains hosted on multiple servers. This fact presents itself as a possible vulnerability for the infrastructure because if one of the servers is compromised the same happens to the certificate. From that moment on, the integrity and confidentiality of all traffic involving the web servers in question would also be compromised. For the attacker, it would be possible to decrypt, modify, and re-encrypt the same. One way to mitigate this risk would be to present a certificate that is valid for each subdomain.

Vulnerability caused by self-signed certificates: When the VPN was implemented to cope with the Covid-19 pandemic, we found that it was using a “self-signed” certificate. This means that a certificate was not issued and verified by a trusted Certificate Authority [67], but by one created in-house. These have the advantage of being free of charge however, once committed and in case the attacker already has access to the system, it can spoof the victim's identity to make communications abroad.

One disadvantage of self-signed certificates is that they cannot provide explicit authentication for the public key. Any malicious actor can reproduce a good looking certificate that makes it practically impossible to be distinguished from the legitimate one before some successful communication with the owner takes place. If the public key signature verification fails the owner cannot tell if the key is not authentic or if the digital signature is wrong so that the owner can refuse the transaction. A previously successful legitimate communication may be proof of the authenticity of the public key, however, this can cause data privacy conflicts. Thus in a distributed environment like the Internet, it becomes impractical and unsafe to use self-signed certificates [68].

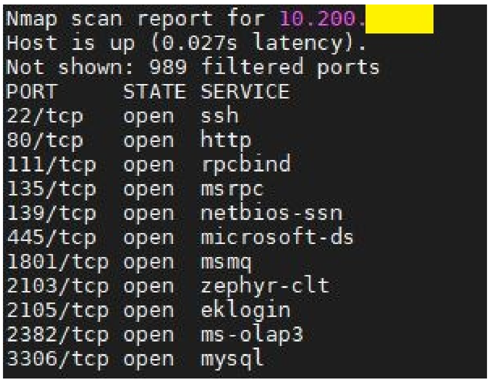
4.3 Open Ports

The fact that systems are exposed to external network probing makes the number of vulnerabilities to which systems are subjected even greater. Most of these attacks start in the so-called "recognition phase" [69], which consists of a systematic attempt to locate, collect, and identify the largest type of information about the target. The steps that may be present in this phase are information gathering, identifying active machines, network mapping, and finally, open ports. The fact that a port is open to connections can facilitate the establishment of communications but can present itself as a vulnerability.

To study this topic, and as mentioned earlier, the Nmap network mapping tool is used, which can be used to find open ports for connections. Nmap scan is based on TCP/IP protocols, it queries target hosts and the responses are translated into readable security data. While some port scanners only scan the most common or most commonly vulnerable port numbers on a given host, the result of a scan on a port in Nmap is generalized into one of three categories:

- **Open:** The host sent a reply indicating that a service is listening on the port;
- **Closed:** The host sent a reply indicating that connections will be denied to the port;
- **Filtered:** There was no reply from the host.

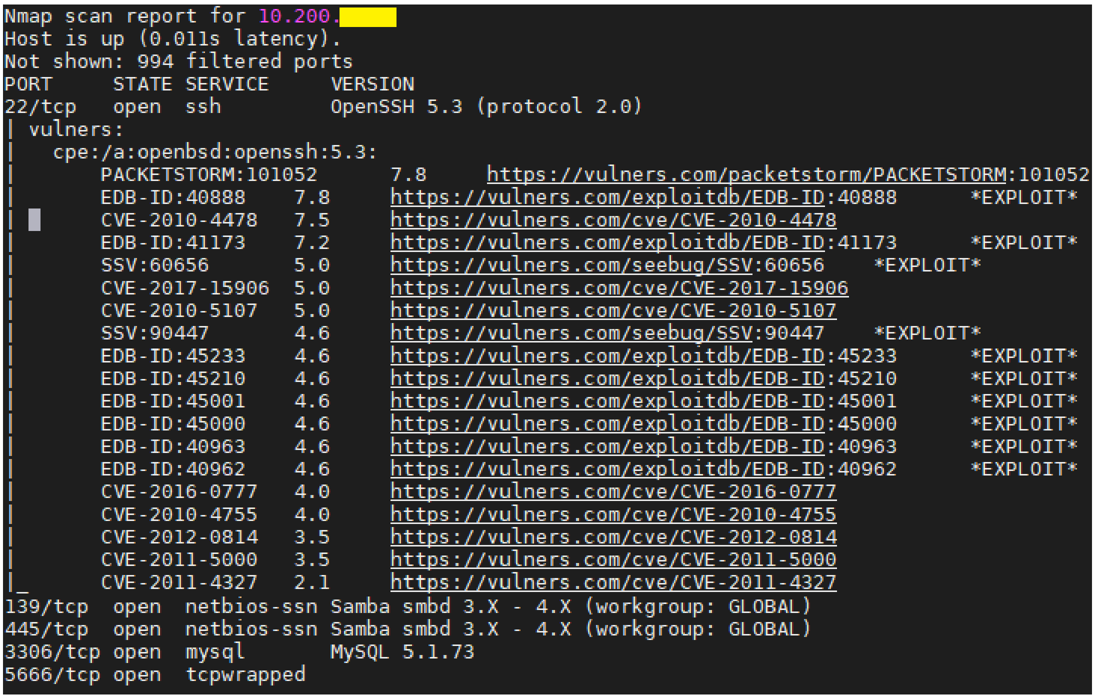
Each port has its own designated service and this same service may have vulnerabilities associated with it that can, of course, be used to benefit malicious intent. These ports are associated with a type of transport protocol and are identified by a number from 0 to 65535 and, up to port 1023, they are referred to as the well-known port numbers, referenced for being used by widely used processes and services. The first scan makes it possible to find out whether the hosts of the network being evaluated are connected, whether they accept connections or whether the machine is turned off. The tool pings each target using UDP, TCP and ICMP probes, after this scan, the ports that responded are listed while the others are given as filtered or closed. In Figure 4.4 it is possible to analyze the open ports at the target of the scan using **nmap -h 10.200.xxx.xxx**. It is also possible to scan which operating system is present on the host, as well as its version, using **nmap -O -v 10.200.xxx.xxx**.



```
Nmap scan report for 10.200.[redacted]
Host is up (0.027s latency).
Not shown: 989 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2382/tcp open  ms-olap3
3306/tcp open  mysql
```

Figure 4.3: Port scan result.

Again, if we use the Nmap Script Engine (NSE) with the ”vuln” script, we can find out what kind of vulnerabilities this host presents, given the corresponding ports and services that were discovered. With the command **nmap -Pn -sV –script=vuln 10.200.xxx.xxx** we get the following output:



```
Nmap scan report for 10.200.[redacted]
Host is up (0.011s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:5.3:
|       PACKETSTORM:101052      7.8     https://vulners.com/packetstorm/PACKETSTORM:101052
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
| █     CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|       EDB-ID:41173    7.2     https://vulners.com/exploitdb/EDB-ID:41173      *EXPLOIT*
|       SSV:60656       5.0     https://vulners.com/seebug/SSV:60656    *EXPLOIT*
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2010-5107
|       SSV:90447       4.6     https://vulners.com/seebug/SSV:90447    *EXPLOIT*
|       EDB-ID:45233    4.6     https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
|       EDB-ID:45210    4.6     https://vulners.com/exploitdb/EDB-ID:45210      *EXPLOIT*
|       EDB-ID:45001    4.6     https://vulners.com/exploitdb/EDB-ID:45001      *EXPLOIT*
|       EDB-ID:45000    4.6     https://vulners.com/exploitdb/EDB-ID:45000      *EXPLOIT*
|       EDB-ID:40963    4.6     https://vulners.com/exploitdb/EDB-ID:40963      *EXPLOIT*
|       EDB-ID:40962    4.6     https://vulners.com/exploitdb/EDB-ID:40962      *EXPLOIT*
|       CVE-2016-0777   4.0     https://vulners.com/cve/CVE-2016-0777
|       CVE-2010-4755   4.0     https://vulners.com/cve/CVE-2010-4755
|       CVE-2012-0814   3.5     https://vulners.com/cve/CVE-2012-0814
|       CVE-2011-5000   3.5     https://vulners.com/cve/CVE-2011-5000
|_      CVE-2011-4327   2.1     https://vulners.com/cve/CVE-2011-4327
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: GLOBAL)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: GLOBAL)
3306/tcp open  mysql       MySQL 5.1.73
5666/tcp open  tcpwrapped
```

Figure 4.4: Vulnerabilities scan with NSE.

If we analyze the output obtained, we notice that version 5.3 of the OpenSSH software present on the webserver presents several vulnerabilities that can be exploited by a malicious individual. These vulnerabilities will not be described in depth for not being the scope of this work. However, it is relatively easy for someone to exploit these flaws, for example, with the Metasploit framework [70], which allows the exploitation of these vulnerabilities in a very intuitive and simple way. Notice also in the last lines, not only the version of the database management service “MySQL”, which is also outdated and whose present version has vulnerabilities [71], as well as the name of the domain of the municipality, GLOBAL.

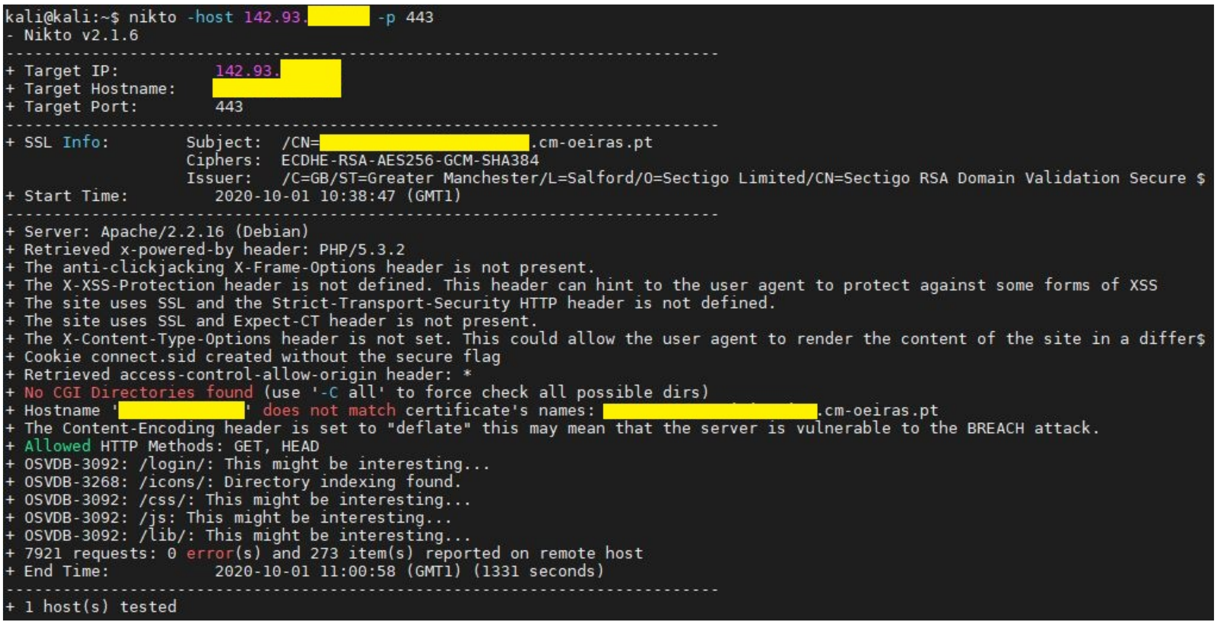
This analysis delivers information that can be valuable to a malicious individual. An open port presents itself as a possible attack surface, i.e., it should be reduced to the minimum possible. For this, the organization must be able to analyze all the ports that are open and evaluate which are really needed to be in that position or which can and should be closed to connections from outside and even for internal connections, in case a compromised internal server tries a lateral jump.

With these findings, although they represent only a small sample of an infrastructure that is composed of several publicly exposed virtual machines and web servers, we were able to notice a number of possible open ports that could possibly be closed or with a filtered state, that present several vulnerabilities about to be explored. Although it has not been possible to report all these instances in detail, they should be checked as closely as possible by the teams responsible for the service, so that they can assess what the real need for these conditions is. Not being possible to close all the ports, because that would turn off the services for which the machine was created, one should make an analysis and then assume the risk of the ports that need to be open.

4.4 Web Applications

Given a large number of public websites present in the infrastructure of the Municipality, taking into account the scope of this work, we decided to analyze the security of the web pages, as they present themselves as a typical target to attacks [72]. We used Nikto and OWASP Zap tools to test some websites and servers in the Municipality regarding misconfigurations and security vulnerabilities.

More specifically, we executed the command **nikto -host 142.93.xxx.xxx -p 443** to perform the evaluation of vulnerabilities present in the page under study. Figure 4.5 shows the output.



```
kali@kali:~$ nikto -host 142.93.[redacted] -p 443
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          142.93.[redacted]
+ Target Hostname:
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=[redacted].cm-oeiras.pt
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure $
+ Start Time:         2020-10-01 10:38:47 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.2.16 (Debian)
+ Retrieved x-powered-by header: PHP/5.3.2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a differ$
+ Cookie connect.sid created without the secure flag
+ Retrieved access-control-allow-origin header: *
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Hostname '[redacted]' does not match certificate's names: [redacted].cm-oeiras.pt
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Allowed HTTP Methods: GET, HEAD
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3092: /js: This might be interesting...
+ OSVDB-3092: /lib/: This might be interesting...
+ 7921 requests: 0 error(s) and 273 item(s) reported on remote host
+ End Time:           2020-10-01 11:00:58 (GMT1) (1331 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 4.5: Nikto scan output.

In this analysis we can identify several failures:

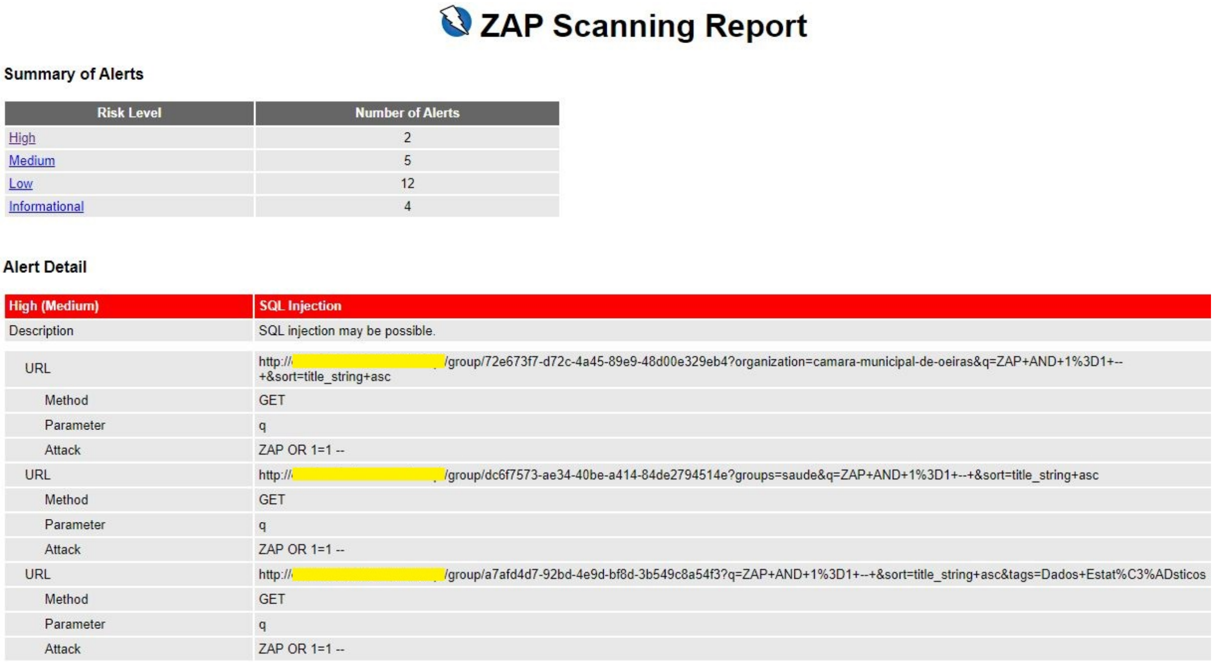
- Webserver returns the technology configured in it;

- X-Frame-Options header is not set;
- XSS protection header is not defined;
- The X-Content-Type-Options header is not set;
- The hostname does not match the certificate name;
- It is possible to list indexed directories;
- Possibly vulnerable to BREACH attack [73].

From this analysis we can draw several conclusions: the possibility of being able to perform webserver fingerprinting [74] is not in itself a vulnerability, but it is information that can end up making the task of someone malicious easier, so measures must be taken, such as, in the case of an Apache web server, configure the **mod_headers** module to hide information from the host. If we want to go further in the measure, a reverse proxy can be used which creates an additional layer of security. The **X-Frame-Options** header prevents *clickjacking* attacks [75], in which a user is led to believe that he is clicking on a button or link on a page, while in reality he is doing so on a transparent layer at the top of that page, controlled by a malicious entity. This way, the header should be configured which instructs the browser to not allow framing from other domains. The X-XSS header stops loading pages when refleted cross-site scripting is detected[76]. This type of attack uses code injections when a user's input is immediately returned by the web application in the form of an error or result message, without the information sent by the user being stored securely on the server. This information can be used illegitimately if it is, for example, confidential information. For this reason it is recommended that it be configured in all webservers, not being a header that may cause constraints with the content of the page. In the case of the point where it is stated that the hostname does not match the name on the certificate that is configured, this goes against the fault mentioned in Section 4.2 where we addressed the problem of using wildcard certificates. The listing of indexed files may allow access to information that should not be public. In this case, we are not aware of the folders in question presenting themselves as ”important” from a security point of view, however, this situation should be evaluated and even if this is not the case, then there is no need to be able to list these same files.

Another tool used to return possible vulnerabilities in web servers is OWASP Zap. Since this tool has been presented in Chapter 2, we will only explain its use and its output. This tool was only used in its standard functionalities, where we only need to provide the URL of the website in question; it then performs a battery of tests on the page. With this it was possible to obtain the following output in HTML format, as show in Figure 4.6.

If we look at this excerpt of the report we can see that this page is susceptible to SQL Injection attack [77], in the URLs indicated and with the parameters represented. The vulnerability was detected by successfully retrieving more data than originally returned by manipulating the parameter. This vulnerability was described in Chapter 2, exactly because it is in the top 10 of vulnerabilities found in web applications present on the Internet today. As for main recommendations to mitigate these situations,



ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	5
Low	12
Informational	4

Alert Detail

High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	http://[redacted]/group/72e673f7-d72c-4a45-89e9-48d00e329eb4?organization=camara-municipal-de-oeiras&q=ZAP+AND+1%3D1+--+&sort=title_string+asc
Method	GET
Parameter	q
Attack	ZAP OR 1=1 --
URL	http://[redacted]/group/dc6f7573-ae34-40be-a414-84de2794514e?groups=saude&q=ZAP+AND+1%3D1+--+&sort=title_string+asc
Method	GET
Parameter	q
Attack	ZAP OR 1=1 --
URL	http://[redacted]/group/a7afd4d7-92bd-4e9d-bf8d-3b549c8a54f3?q=ZAP+AND+1%3D1+--+&sort=title_string+asc&tags=Dados+Estat%C3%ADsticos
Method	GET
Parameter	q
Attack	ZAP OR 1=1 --

Figure 4.6: SQL Injection attack report.

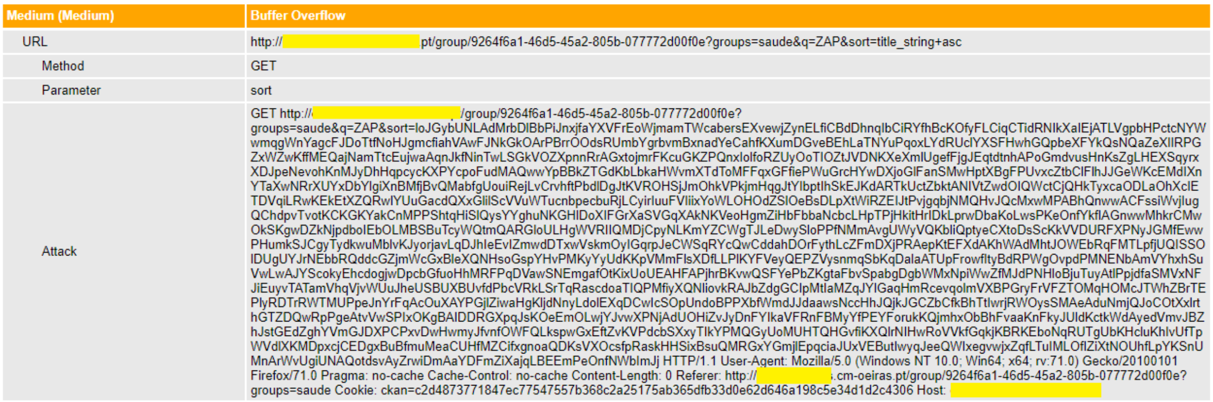
the input given by the client-side should never be trusted. When it is possible to check these inputs, then they should be made and a whitelist of allowed characters should be applied.

In the same report, we can also identify that a buffer overflow [78] exploit can be performed in this page (see Figure 4.7). This attack is characterized by overwriting the memory spaces allocated to a certain process, which should not be modified. This type of action can lead to the creation of exceptions, segmentation faults, and processing errors that can result in abnormal behavior of the application or even allow an adversary to inject code for local execution. To combat the possibility of this procedure, the web application code should be rewritten to present proper return length checking mechanisms so that it is not possible for an individual to exceed the limits of the memory allocated to the process.

4.5 Wordpress

Wordpress is arguably the most widely used Content Management System (CMS) on websites available. Its ease of configuration and low demand for programming knowledge make it increasingly adopted by those who need to develop a web page. This is also true in the Municipality of Oeiras, where the various organic units choose to use this platform to develop websites in order to present their projects in a more dynamic, current and accessible way to the population. However, this development is not always done with the knowledge of the software team, much less being guided by a development and implementation procedure aimed at the best cybersecurity practices.

The Wordpress tool enriches the content of their websites by making available to those who develop several content management plugins that are developed by individuals and are not verified. This type of themes and plugins are available in a kind of market to which each one can add to their page. It



Medium (Medium)	Buffer Overflow
URL	http://[redacted]pt/group/9264f6a1-46d5-45a2-805b-077772d00f0e?groups=saude&q=ZAP&sort=title_string+asc
Method	GET
Parameter	sort
Attack	GET http://[redacted]/group/9264f6a1-46d5-45a2-805b-077772d00f0e?groups=saude&q=ZAP&sort=loJGybUNLAdMrbDlBbPiJnxjfaYXVFrEoWjmamTWcabersEXvewjZynELfiCBdDhnqlbCiRYfhBcKOfyFLCiqCTidRNIkXaIEjATLVgpbHPctcNYWwmqgWnYagcFJDoTtfNoHJgmcfiahVAwFJNkGkOArPBrrOOdsRUmbYgrbvmBxnadYeCahfKXumDGveBEhLaTNYuPqoxLYdRUclYXSFHwhGQpbeXFYkQsNQaZeXIlRPGZxWZwKffMEQajNamTtcEujwaAqnJkfNinTwLSGkVOZXpnnRrAGxtojmrFKcuGKZPQnxlolfoRZUyOoTIOZtJVDNKXeXmlUgefFjgJEqtdtnhAPoGmdvusHnKsZgLHEXSqyrxXDJpeNevohKnMJyDhHqpcycKXPYcpoFudMAQwwYpBBkZTGdKbLbkaHWvmXTdToMFFqxGFfiePWuGrcHYwDXjoGlFanSMwHptXBgFPUvxcZtbClFlhJJGeWKcEMdlXnYTaXwNRrXUYxDbYlgiXnBMfjBvQMabfgUouiRejLvCrvhftPbdlDgJtKVROHSjJmOhkVPkjmHqgJtYlbptlhSkEJKdARTkUctZbktANIVtZwdOIQWctCjQHkTyxcaODLaOhXclETDVqiLRwKEkEtXZQRwlYUuGacdQXxGlilScVVuWTucnbpecbuRjLCyirluuFVliixYoWLOHOdZSlOeBsDLpXtWiRZEIJtPvjgqbjNMQHvJQcMxwMPABhQnwwACFssiWvjlugQChdpvTvotKCKGKYakCnMPPShtqHiSlQysYYghuNKGHIDoXIFGrXaSVGqXAkNKVeoHgmZiHbFbbaNcbcLHpTPjHkitHrlDkLprwDbaKoLwsPKeOnfYkflAGnwwMhkrCMwOkSKgwDZkNjpdbolEbOLMBSBuTcyWQtmQARGloULHgWVRIIQMDjCpyNLKmYZCWgTJLeDwySloPPfNMmAvgUWyVQKbliQptyeCXtoDsScKkVVDURFXPNyJGMfEwwPHumkSJCgyTydkwuMblvKJyorjavLqDJhleEvlZmwdDTxwVskmOylGqrpJeCWSqRYcQwCddahDOrFythLcZFmDXjPRAepKtEFXdAKhWAdMhtJOWEbRqFMTLpfjUQISSOlDUgUYJrNEbbRQddcGZjmWcGxBleXQNHsoGspYHvPMKyYyUdKKpVMmFlsXDfLLPlKYFVeyQEPZVysnmqSbKqDalaATUpFrowfltyBdRPWgOvpdPMNENbAmVYhxhSuVwLwAJYScokyEhcdogjwDpcbGfuoHhMRFPqDVawSNEmgafOtKixUoUEAHFAPjhrBKvwQSFYePbZKgtaFbvSpabgDgbWMxNpiWwZfMJdPNHloBjuTuyAtlPpjdfaSMVxNFJiEuyvTATamVhqVjvWUuJheUSBUXBUvfdPbcVRkLSrTqRascdoaTIQPMfiyXQNliovkRAJbZdgGClpMtlaMZqJYlGaqHmRcevqolmVXBPGryFrVFZTOMqHOMcJTWhZBrTEPlyRDTrRWTMUPpeJnYrFqAcOuXAYPGjlZiwaHgKljdNnyLdolEXqDCwlcSOpUndoBPPXbfWmdJJdaawsNccHhJQjkJGCZbCfkBhTtlwrjRWOysSMAeAduNmjQJoCOtXxlrthGTZDQwRpPgeAtvVwSPlxOKgBAIDDRGXpqJsKOeEmOLwjYJvwXPNjAdUOHiZvJyDnFYlkaVFRnFBMyYfPEYForukKQjmhxObBhFvaaKnFkyJUldKctkWdAyedVmvJBZhJstGEdZghYVmGJDXPCPxvDwHwmyJfvnfOWFQLkspwGxEftZvKVPdcbSXxyTlkYPMQGyUoMUHTQHGvfiKXQlrNIHwRoVVkfGqkjKBRKEboNqRUTgUbKHcluKhlvUfTpWVdlXKMDpxcjCEDgxBuBfmuMeaCUHfMZCifxgnoaQDKsVXOcsfpRaskHHSixBsuQMRGxYGmjlEpqciaJUxVEButlwyqJeeQWlxegvwjxZqfLTulMLOflZiXtNOUhfLpYKSnUMnArWvUgiUNAQotdsvAyZrwiDmAaYDFmZiXajqLBEEmPeOnfNWblmJj HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0 Pragma: no-cache Cache-Control: no-cache Content-Length: 0 Referer: http://[redacted].cm-oeiras.pt/group/9264f6a1-46d5-45a2-805b-077772d00f0e?groups=saude Cookie: ckan=c2d4873771847ec77547557b368c2a25175ab365dfb33d0e62d646a198c5e34d1d2c4306 Host: [redacted]

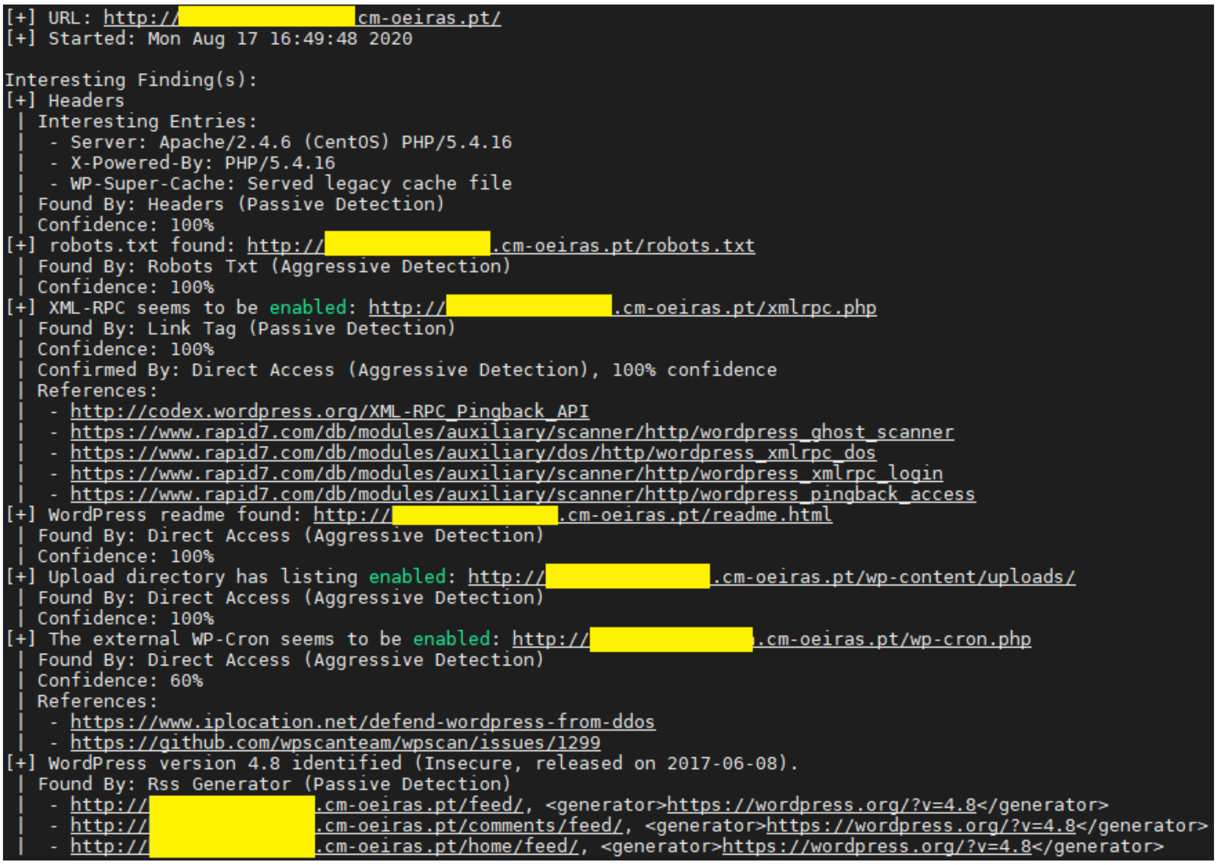
Figure 4.7: Buffer overflow scan report.

becomes obvious that this is a convenient way for individuals with malicious intentions to distribute malware or obtain information from others [27].

Considering this fact, given the number of websites developed in this CMS, we conclude that it would be in the best interest to dedicate a part of this work to the security assessment of web pages developed in Wordpress. To this end, we used a tool dedicated to security analysis of themes, plugins and platform configurations, called WPScan, which has already been introduced in Chapter 2. To demonstrate this analysis we used a website developed in the technology whose URL is anonymized throughout the work for safety reasons, as in previous situations. This analysis was done with the configuration of the vulnerability scanner API that is made available to developers and security analysts with a limited volume of daily scans. This API makes available the platform vulnerability database that includes WordPress vulnerabilities, plugin vulnerabilities, and theme vulnerabilities.

The first analysis of the tool evaluates the answers given by the website and information that can be taken from the headers presented (see Figure 4.8). With this output it is possible to report several security problems present on this page. Again, it is possible to make web server fingerprinting to discover the technologies present in it. The file robots.txt [79] which is supposed to be used to indicate to search engines which directories not to index, may contain confidential information. The feature XML-RPC which is a feature activated by default that enables information to be transmitted by HTTP as the transport mechanism and XML as the encoding mechanism. However, over the years, this has become a greater security concern than a beneficial functionality, because it allows attackers to use xmlrpc.php to access the website through a dictionary attack or launch a Distributed Denial-of-Service attack using the pingback feature [80]. In the same report it is possible to see that the version of Wordpress of this website is outdated, also has vulnerabilities that are registered and therefore is unsafe.

By using WPScan in the chosen URL and the **–enumerate vp** flag, we can get the plugins identified in the page that have vulnerabilities as well as configuration flaws. In Figures 4.9 and 4.10, we can see that the same page also has outdated and vulnerable plugins, with detailed flaws and that can be explored with relative ease. These plugins become a gateway to the server, for example, and consequently to the

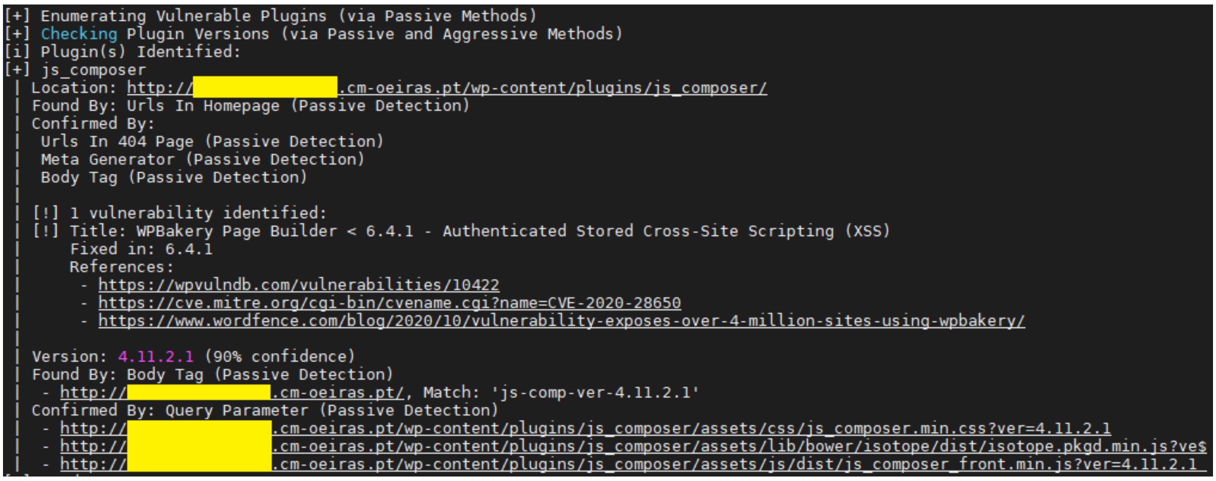


```
[+] URL: http://[redacted]cm-oeiras.pt/
[+] Started: Mon Aug 17 16:49:48 2020

Interesting Finding(s):
[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.6 (CentOS) PHP/5.4.16
 |  - X-Powered-By: PHP/5.4.16
 |  - WP-Super-Cache: Served legacy cache file
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
[+] robots.txt found: http://[redacted].cm-oeiras.pt/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%
[+] XML-RPC seems to be enabled: http://[redacted].cm-oeiras.pt/xmlrpc.php
 | Found By: Link Tag (Passive Detection)
 | Confidence: 100%
 | Confirmed By: Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
[+] WordPress readme found: http://[redacted].cm-oeiras.pt/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
[+] Upload directory has listing enabled: http://[redacted].cm-oeiras.pt/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://[redacted].cm-oeiras.pt/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 4.8 identified (Insecure, released on 2017-06-08).
 | Found By: Rss Generator (Passive Detection)
 |  - http://[redacted].cm-oeiras.pt/feed/, <generator>https://wordpress.org/?v=4.8</generator>
 |  - http://[redacted].cm-oeiras.pt/comments/feed/, <generator>https://wordpress.org/?v=4.8</generator>
 |  - http://[redacted].cm-oeiras.pt/home/feed/, <generator>https://wordpress.org/?v=4.8</generator>
```

Figure 4.8: Website information and vulnerabilites.

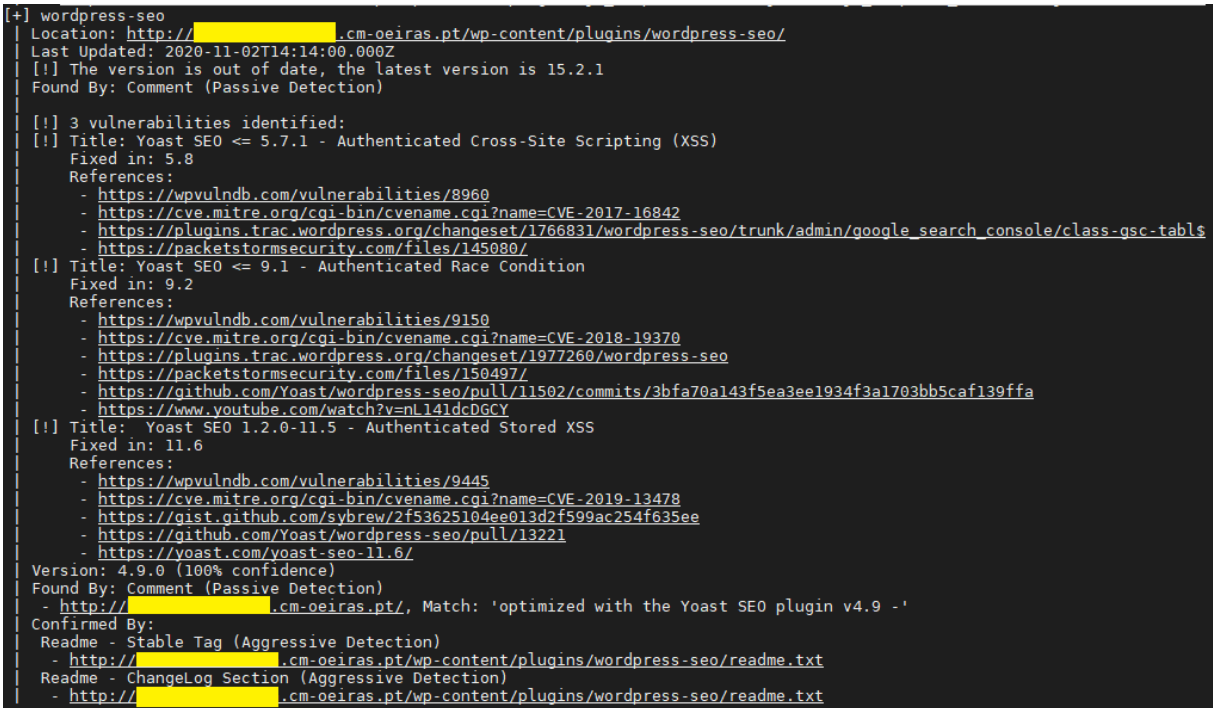
infrastructure of the entire Municipality.



```
[+] Enumerating Vulnerable Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
[i] Plugin(s) Identified:
[+] js_composer
 | Location: http://[redacted].cm-oeiras.pt/wp-content/plugins/js_composer/
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By:
 |  Urls In 404 Page (Passive Detection)
 |  Meta Generator (Passive Detection)
 |  Body Tag (Passive Detection)
 |
 | [!] 1 vulnerability identified:
 | [!] Title: WPBakery Page Builder < 6.4.1 - Authenticated Stored Cross-Site Scripting (XSS)
 |     Fixed in: 6.4.1
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/10422
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28650
 |      - https://www.wordfence.com/blog/2020/10/vulnerability-exposes-over-4-million-sites-using-wpbakery/
 |
 | Version: 4.11.2.1 (90% confidence)
 | Found By: Body Tag (Passive Detection)
 |  - http://[redacted].cm-oeiras.pt/, Match: 'js-comp-ver-4.11.2.1'
 | Confirmed By: Query Parameter (Passive Detection)
 |  - http://[redacted].cm-oeiras.pt/wp-content/plugins/js_composer/assets/css/js_composer.min.css?ver=4.11.2.1
 |  - http://[redacted].cm-oeiras.pt/wp-content/plugins/js_composer/assets/lib/bower/isotope/dist/isotope.pkgd.min.js?ve$
 |  - http://[redacted].cm-oeiras.pt/wp-content/plugins/js_composer/assets/js/dist/js_composer_front.min.js?ver=4.11.2.1
```

Figure 4.9: Wordpress plugins vulnerabilities - part 1.

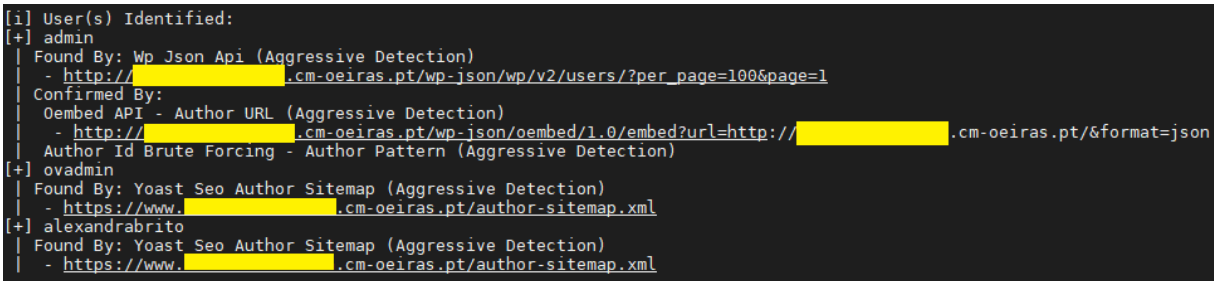
However, there is more information one can find out about this website and its settings. The **–enumerate u** flag allows the use of brute force techniques of the WordPress management platform user ID and plugins that can make use of registering authors of publications. In this scan (see Figure 4.11) we can see that it is possible to enumerate users who use the platform. The first one was discovered using



```
[+] wordpress-seo
 | Location: http://[redacted].cm-oeiras.pt/wp-content/plugins/wordpress-seo/
 | Last Updated: 2020-11-02T14:14:00.000Z
 | [!] The version is out of date, the latest version is 15.2.1
 | Found By: Comment (Passive Detection)
 |
 | [!] 3 vulnerabilities identified:
 | [!] Title: Yoast SEO <= 5.7.1 - Authenticated Cross-Site Scripting (XSS)
 |     Fixed in: 5.8
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/8960
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-16842
 |      - https://plugins.trac.wordpress.org/changeset/1766831/wordpress-seo/trunk/admin/google_search_console/class-gsc-tabl$
 |      - https://packetstormsecurity.com/files/145080/
 | [!] Title: Yoast SEO <= 9.1 - Authenticated Race Condition
 |     Fixed in: 9.2
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9150
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19370
 |      - https://plugins.trac.wordpress.org/changeset/1977260/wordpress-seo
 |      - https://packetstormsecurity.com/files/150497/
 |      - https://github.com/Yoast/wordpress-seo/pull/11502/commits/3bfa70a143f5ea3ee1934f3a1703bb5caf139ffa
 |      - https://www.youtube.com/watch?v=nL141dcDGCY
 | [!] Title:  Yoast SEO 1.2.0-11.5 - Authenticated Stored XSS
 |     Fixed in: 11.6
 |     References:
 |      - https://wpvulndb.com/vulnerabilities/9445
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13478
 |      - https://gist.github.com/sybrew/2f53625104ee013d2f599ac254f635ee
 |      - https://github.com/Yoast/wordpress-seo/pull/13221
 |      - https://yoast.com/yoast-seo-11.6/
 | Version: 4.9.0 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://[redacted].cm-oeiras.pt/, Match: 'optimized with the Yoast SEO plugin v4.9 -'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://[redacted].cm-oeiras.pt/wp-content/plugins/wordpress-seo/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://[redacted].cm-oeiras.pt/wp-content/plugins/wordpress-seo/readme.txt
```

Figure 4.10: Wordpress plugins vulnerabilities - part 2.

the REST API used by WordPress that lists information of registered users who have already authored a post on the page. The last two users were discovered because the website contains a plugin called “Yoast SE” that works like an XML sitemap [81], used to let search engines know which posts to index. This plugin provides the authors sitemap in /**authors-sitemap.xml** which is defined by default. We recommended to disable this feature, even if there is a need to use the rest of the plugin’s functionalities.



```
[i] User(s) Identified:
[+] admin
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://[redacted].cm-oeiras.pt/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Oembed API - Author URL (Aggressive Detection)
 |   - http://[redacted].cm-oeiras.pt/wp-json/oembed/1.0/embed?url=http://[redacted].cm-oeiras.pt/&format=json
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
[+] ovadmin
 | Found By: Yoast Seo Author Sitemap (Aggressive Detection)
 |  - https://www.[redacted].cm-oeiras.pt/author-sitemap.xml
[+] alexandrabrito
 | Found By: Yoast Seo Author Sitemap (Aggressive Detection)
 |  - https://www.[redacted].cm-oeiras.pt/author-sitemap.xml
```

Figure 4.11: Users enumeration.

In summary, this analysis of WordPress pages using the WPScan tool has allowed us to uncover that although it is an intuitive platform that allows to create functional and pleasant looking pages, it has several flaws and vulnerabilities. Its implementation must be done following a security analysis process and must be monitored and updated regularly.

With the results obtained we can conclude that the development of web pages should be done centrally and not in a heterogenous way, without this being communicated or even supervised. This reveals a problem of communication and lack of procedures regarding the development of the software present in the infrastructure of the Municipality, which consequently translates into possible security vulnerabilities.

4.6 Summary

In this part of the assessment, it was possible to discover vulnerabilities related to web applications and that are more relevant attacks from the point of view of notoriety and general knowledge. However and as we can see, this still does not translates into a process of their development with the proper settings that allow the applications the possibility to defend themselves from attacks like those portrayed. This type of applications should follow a software development process that, although it would not compromise its functionality, if guarantees were created from a security point of view. This balance between functionality and security should become a common practice in the Municipality, reinforced by procedures and norms that should be respected in order to try to prevent unpleasant situations that, as we could see, are not difficult to happen. This kind of analysis reinforces that not only in the public with not much literacy there is some lack of sensitivity and notions of cybersecurity. Next, we present our third major contribution of this thesis which focuses on studying the cybersecurity awareness of the Oeiras Municipality's IT staff.

Chapter 5

Cybersecurity Awareness

In this chapter, we present the third major contribution of this thesis. This contribution consists of a field study aimed at assessing the cybersecurity awareness of the employees that work for the Oeiras Municipality and have access to its IT infrastructure. We begin with a more detailed motivation of this study and an explanation of its main goals. Then we present our methodology which consists of a survey addressed to the employees of the IT Department. This survey is used to gather information for this work, and analyze some instances of social engineering attacks that have been mounted. Lastly, we discuss the results of this enquiry and outline some measures and good practices of cybersecurity.

5.1 Study Motivation and Goals

The constant development of new threats with predominance in cyberspace, the abundance of attacks on the Internet, such as data theft, like photographs, bank information, identity theft or the crime of extortion, require a user to be increasingly aware of the importance of protecting his information and to have the appropriate behaviors in its use. Attackers have increasingly turned their attention to people as their targets of the organization's vulnerabilities. Implementing the latest security technologies may not help much if users are not aware or properly trained (Singer & Friedman, 2014) [82].

Ignorance or lack of awareness of good cybersecurity practices present themselves as the greatest threats to the security of information systems. Nowadays, it is known that the best way to improve a company's situation regarding the security of its assets is not only through technical solutions but also by increasing the awareness and education of employees who use these same systems. However, these common practices of digital security continue to be ignored in daily use by most individuals, which puts at risk the integrity and confidentiality of a company's data.

In the topic of cybersecurity, users are often referred to as the "weakest link" [83]. The report by IBM Security & Ponemon Institute (IBM Security & Ponemon Institute, 2018) estimates that the cost of incidents related to security breaches in organizations in the United States has increased and that in the sum of these incidents, 31% were caused by employee negligence. On the other hand, some types of risk behavior, although not a specific cybersecurity failure, may result in one. For example, not logging out of the user account or applications, using unsafe passwords and using them repeatedly on different platforms, filling out forms with personal data without being sure if it is reliable, interacting with phishing emails, or not being able to distinguish whether or not you may be the target of a social engineering attack. Of course, these events are more likely to focus on less informed and less aware individuals. Accidental misuse is listed as one of the main reasons for security breaches[84]. Many well-meaning employees may bypass the company's security policy to meet business needs or simply to speed up some type of procedure, an action that can lead to a security breach even if accidental. For example, some users may click "Reply All" instead of "Reply" when sending confidential documents by email. Others may expose sensitive personal information using email, websites, blogs or social networks.

Kaushalya and Randeniya [85] share the reasons for misusing technology as: *accidental*, where they include inadequate knowledge of the system, stress and lack of knowledge in interacting with the technology; *ignorance* which includes lack of awareness and lack of training; *intentional* consisting of data theft, personal difference and deliberate ignorance of rules. That being said, the human factor is inseparable from the concept of cyber security. A visual way to demonstrate this interconnection between people, processes and technology is the McCumber cube (as depicted in Figure 5.1). It consists of a security model that defines the relationship between information states, critical information characteristics and security measures and intends to convey the idea that to develop an appropriate information systems security, all its dimensions and attributes and its interconnections must be questioned [86], which also applies to education, training and awareness.

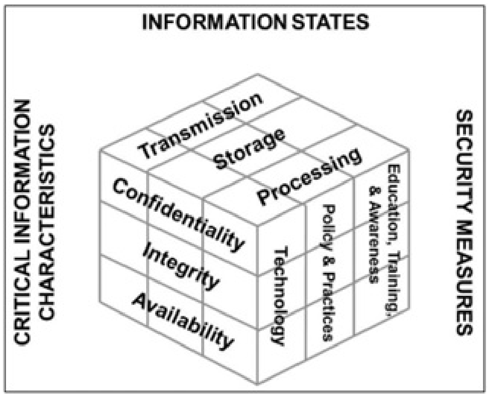


Figure 5.1: The McCumber Cube [86].

Our study aims at assessing the cybersecurity awareness of the IT department staff at the Oeiras Municipality. We focus only on the first two reasons stated above, i.e., accidental misuse and misuse by ignorance, because they are the ones that can later cause a potential attack via social engineering.

5.2 Methodology

In this study, we evaluate the state of affairs at the Oeiras Municipality in terms of awareness and notions of security in the workplace. We concentrate on a relatively small set of users representing the total universe of employees as we were not authorized to distribute our survey to a larger number of workers. The data was initially gathered through a survey that was outlined to cover the most relevant cybersecurity issues nowadays. We conducted the whole process as follows. First, three situations of possible attacks involving social engineering techniques were outlined and its outcomes were analyzed together with the survey results. Next, we drew our conclusions about the knowledge that the collaborators of the municipality have on the subject. Finally, we laid out several measures and resolutions that intend to help make the interaction between human subjects and the technology more secure.

The methods of qualitative, quantitative and mixed research were considered for the analysis of the results. The most important distinction between these methods is the way they represent data and research results [87]. However, we think that the best way to analyze the data resulting from the survey developed and the social engineering situations targeted to municipality employees would be a mixed approach that would include both numerical and non-numerical analysis, as the object of study is the human being and its behaviors and therefore quite abstract and subjective [88].

5.3 Survey

The survey was conducted via a questionnaire that aimed at gathering information about the knowledge, behaviors and thoughts related to the topic of cybersecurity on the part of the municipality's employees. It was designed with Google Forms and consisted of a brief presentation of its scope and purpose, a reminder that all data would be treated anonymously, followed by 19 questions, the first 3 of which served to characterize the individual from the point of view of age, gender and function within the department. Then, the questionnaire was divided in three parts:

- Initially the respondent was asked if he or she had ever participated in an awareness-raising or training session on the topic of cyber-security, if he or she finds the topic relevant and if, in a form of self-reflection, he thinks he knows how to act in a hypothetical case of a cyber-security incident, so that it was possible to understand the level of literacy of the target audience.
- The following questions included some what-if scenarios of use cases and several options of approaches to the same scenario to be chosen. Some questions about notions of digital security were developed and, taking into account the context of a pandemic experienced, questions were also asked about habits and circumstances experienced while users were placed in remote work.
- Finally, the participants were asked to try to classify their workplace from the point of view of physical and computational security, in the most honest way possible.

The inquiry was sent to 27 participants by email, using the corporate email and duly identified the purpose of this study. The form was available to be filled out during the entire month of September 2020.

5.4 Social Engineering Attack Scenarios

For a further analysis and evaluation of the behavior of the Municipality's employees in possible attack situations using social engineering techniques, it was necessary to prepare three case studies using

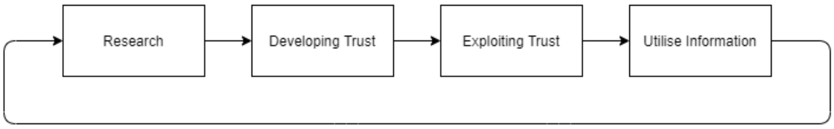


Figure 5.2: Social engineering cycle[89].

different techniques. In order to choose the cases put into practice, their practicality and speed of execution were evaluated, without the need to resort to external resources. The scenarios apply the techniques described in more detail in Section 2.2.4 of this document.

The case studies use the best known attack model, created by Kevin Mitnick, the *social engineering attack cycle* [89]. As illustrated in Figure 5.2, this model encompasses four phases of a social engineering attack: *research*, *developing rapport and trust*, *exploiting trust*, and *utilizing information*, that is, all attacks start by gathering the greatest amount of information about the object of study, developing a sense of trust, exploiting that trust and using the information gathered to execute the attack. Using the framework described in [89], we also analyzed the variables present in each scenario. All participants were anonymized. Responsibility issues have been dealt with internally.

5.4.1 Use Case 1: Vishing Attack

The first example of an attack of social engineering carried out in the scope of this work made use of the *vishing technique*. The plan of attack would have the following description:

> A telephone call would be made to the general and public number of the Municipality of Oeiras, by someone posing as an employee of a technical assistance company of air conditioning systems to try to discover the existence and the respective physical location of the data centers of the infrastructure of the institution. The premise given would be that an intervention would be scheduled. However, no specific information was given about the date and time of the intervention, within the employees of the supposed company. This information would then be part of a larger plan to inflict some physical damage to these data centers.

Given the tremendous importance of these interventions to the IT infrastructure, which houses the core components of the network and virtualization system, this would be highly harmful to the organization. These critical services and their implication were detailed earlier in the document. Mapping this scenario using *Social Engineering Attack Framework* [89] (see Figure 5.2), we describe the features of the attack as follows:

- **Social Engineer:** the social engineer is an individual;
- **Target:** The target is an organization. In this scenario the target is the Oeiras Municipality;
- **Medium:** The medium is a phone call;
- **Goal:** The goal of this action is to find out as much information as possible about the organization's data center, including the number of existing ones, location, access modes and much more;

- **Compliance Principles:** The compliance principles used are commitment or consistency;
- **Technique:** The technique used is vishing;

Attack execution: The phone call was made by a member of the IT Department staff who had recently started working so that there was no risk of his voice being recognized and so that it would be as similar as possible to someone without information from the institution obtained internally. With the call directed to the general number of the Municipality, which is completely public and accessible, the individual identified himself as an employee of a technical assistance company of refrigeration systems that would be hired to perform a maintenance service in the data centers of the organization. The employee who answered the call had no information about the data centers and forwarded it to a second employee of one of the departments of the Municipality. The second employee promptly assisted the supposed employee and provided several pieces of information: (1) the location of both data centers, (2) with whom he would have to talk to have access to them, (3) what was the location of the refrigeration systems and even managed to find out (4) the name of the employee who regularly performed the maintenance. This information was given under the excuse that the responsible for the infrastructure was on vacation, was not contactable and had not left him all the necessary information. With the gathered intel, the scenario was given as finished and the attack as successful. The results will be discussed later in this document.

5.4.2 Use Case 2: Baiting Attack

The following scenario intended to make use of the *baiting technique* which, although it seems quite banal, also proves to be one that presents many cases of success. This is because it is a technique that intends to attract the individual and lure him into performing a given action by sharpening his curiosity. The plot of this action was quite simple:

> To leave a pen drive apparently abandoned on a meeting table that is in the center of the building where the IT Department facilities are. In this case the flash drive contained only a plain text file that showed the message: “If you found this flash drive, please return it to the Security and Monitoring Unit of the Oeiras Municipality”.

In case it was a real attack, the pen drive could contain malicious files that eventually would perform some hazardous action on the computer where it had been inserted or even spread malware throughout the network. In this attack we can describe the following variables:

- **Social Engineer:** the social engineer is an individual;
- **Target:** The target is an individual, although the ultimate target is the Oeiras Municipality;
- **Medium:** The medium is a flash drive;
- **Goal:** The goal of this action is to inject a malicious file in an individual’s computer;
- **Compliance Principles:** The compliance principles used are commitment or consistency;

- **Technique:** The technique used is baiting.

Attack execution: Given the location of the meeting table and the fact that there are surveillance cameras in that location, it would always be easy to see if someone would pick up the object and even the identity of the person. It would not be possible to know whether they inserted the flash drive into their computer or what they would do with it. After a few hours of placing the flash drive, an employee of the IT Department had the "kindness" to return it to the Unit, after realizing who it belonged to and so it was easy to understand who picked up the flash drive and what he did with it. As in the previous case, this action was given as completed and successful.

5.4.3 Use Case 3: Impersonation Attack

The third and last scenario intended to make use of the social engineering technique called *impersonation*, in which one individual poses itself as another person to try to gain access to a resource he originally would not have. The plan of this scenario would be that:

> An individual would impersonate an employee of the Department of Informatics to gain access to the video surveillance circuit recorder of Parque dos Poetas, a green space widely frequented in the council, in order to later extract information from it.

In this case, a very recent employee of the Municipality was recruited, who does not perform services in the field and is not known by the other departments, so that the scenario would be as realistic as possible. The features present in this example are:

- **Social Engineer:** the social engineer is an individual;
- **Target:** The target is the video surveillance circuit recorder;
- **Medium:** The medium is face to face;
- **Goal:** The goal of this action is to gain access to the video surveillance circuit recorder to extract or eliminate data from it;
- **Compliance Principles:** The compliance principles used are commitment or consistency and authority;
- **Technique:** The technique used is impersonating.

Attack execution: The individual in question pretended to be a recent employee for the Municipality who was not yet aware of the location of the rack where the resource was located. He approached the employee (victim) of a private security company that is present on the site, to whom he was very cordial and ready to indicate its location. At no time was it necessary for the "employee" to show any kind of higher-ranked identification or authorization. During the minutes the attacker was inside the room where the recorder was placed, he was always alone and without any supervision. After a few minutes he left the place quite naturally, stating that the task that had brought him there was finished. Once again and following the previous examples, the attack was given as successful.

5.5 Survey Results

From the survey (see Appendix A) we were able to get 29 responses out of a possible 33. Besides the readiness with which the employees responded to it, it was possible to receive some comments from some employees for the importance of the matter of cybersecurity to be finally treated, especially directed to those who deal with the technology, such as not only the personnel of the IT Department but all the rest of the Municipality.

Current training in cybersecurity: When we analyze the survey answers we started to realize that there is a clear lack of training on the subject of cyber security. As shown in Figure 5.3, over 62% of the participants said they had never participated in a training action on the subject. This data reveals that the organization has overlooked the importance of investing in the training of its employees in cybersecurity.

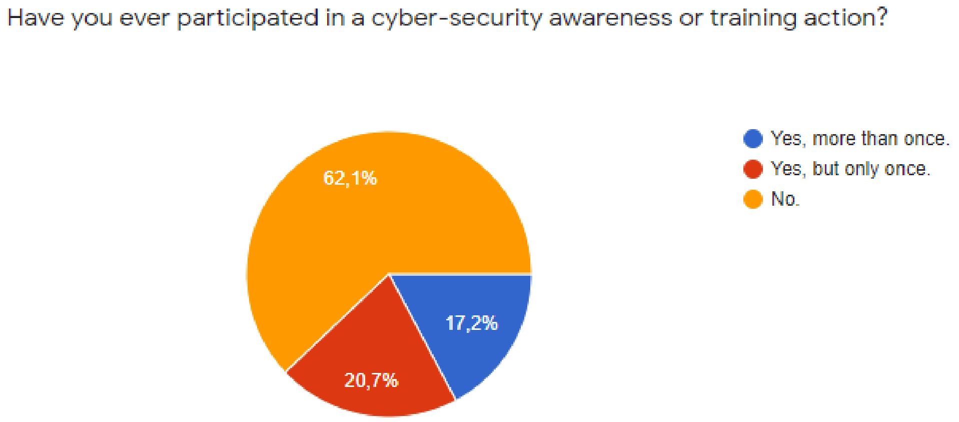


Figure 5.3: Presence of employees with training in cybersecurity.

Need for further training in cybersecurity: Although more than half of the participants answered that they had never received training on cybersecurity, most of them, even in a smaller percentage (i.e., about 55%), state that they have sufficient knowledge on the subject for a good performance of their functions (see Figure 5.4).

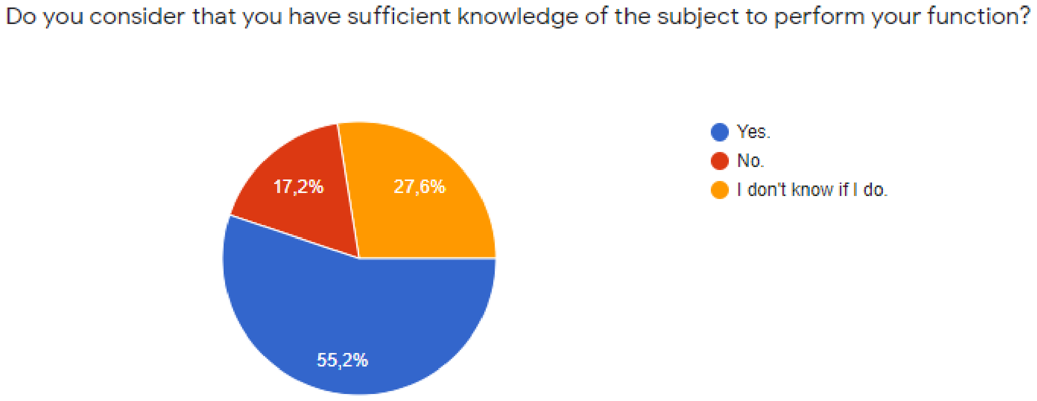
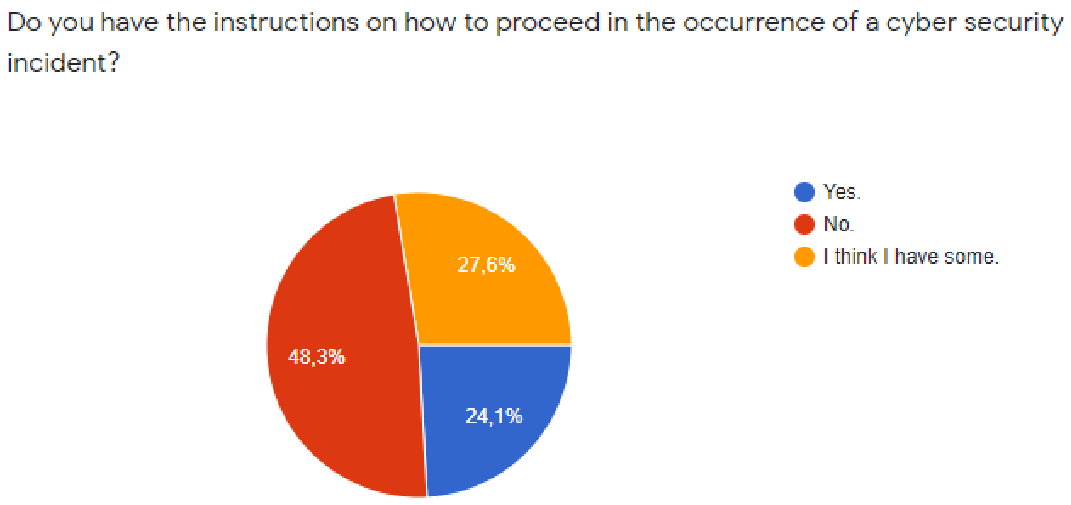


Figure 5.4: Evaluation of personal need for more training.

These results show that the participants have acknowledged that they have no need to evolve and acquire more knowledge on the subject. What, in a theme such as cybersecurity that is constantly developing, can be recognized as completely incorrect and even negligent. One reason for this result may be that they have not found the topic so important and that there is no need to waste time knowing more about it. However, when asked if the issue is important and if the Municipality's employees should be trained in this sense, only one participant did not answer yes. The combination of answers to these three questions shows that, although most of the employees in the Informatics Department think they already have enough knowledge for their job, the subject is important and the employees should be trained. Given this data, we conjecture that if more than half of the employees who regularly deal with technology have no training in cybersecurity, non-tech savvy employees would be even more so.

Lack of guidelines and procedures: As we are dealing with such a transversal theme at all levels, both physical and technical, it would be of the utmost importance that all employees receive training on the subject, especially those who are responsible for planning, configuring and developing the technology that the rest will use, contrary to what we can draw from these responses. Once again it was possible to verify the contradiction in their answers when asked if they thought they had in their possession the instructions on how to proceed in case of a cyber security incident. This question, to which about half answered no, was intended to understand whether the management transmits the necessary guidelines to the remaining employees. In most cases this has not happened, which in the event of a cybersecurity incident, an employee does not know what to do, whether intentionally or not, any action may end up making the situation worse.



Do you have the instructions on how to proceed in the occurrence of a cyber security incident?

Figure 5.5: Lack of guidelines from workforce.

In the same survey some questions related to the theme of remote work were inserted, once again given the lived context. These questions included access to work resources from devices whose status is unknown by the security platforms of the Municipality, or even the sharing of the work computer by someone unknown to it. From this it was possible to realize that the best cyber security practices were not always present when employees were in a position to work in their homes.

Finally, the issue of the authentication method in resources of the Municipality, the password, was also addressed. In this topic, more than half of the employees admitted using the same password for more than one device or platform, and the most present method of managing passwords was memorization, which allows us to conclude that we are really facing a situation where a good part of the participants have weak passwords from the point of view of security, because only then they would be able to manage them by memorization.

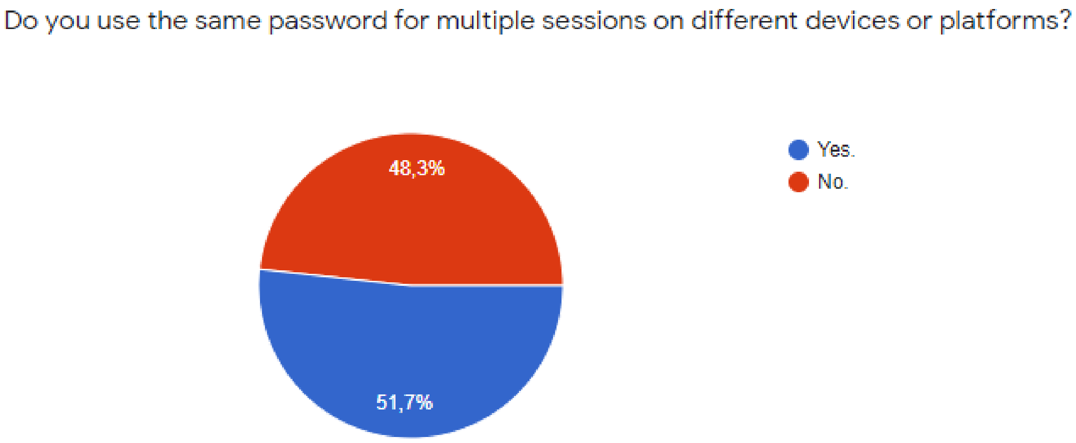


Figure 5.6: Password usage from the workers.

5.6 Security Recommendations

After all data collected from the illegitimate accesses to the Municipality's VPN, the illiteracy verified by some users, as well as the presence of some bad practices regarding cyber-security, the work project intended to give some lectures or training to the employees not only of the IT Department, but to all employees of the Municipality. Unfortunately, this initiative was not yet authorized by higher instances. Nevertheless, we continued to work on technical solutions that could be proposed to try to minimize security risks in the interaction between users and technologies. From this, the following list of recommendations is proposed to be implemented at the Oeiras Municipality.

5.6.1 Two-factor Authentication

One of the technical measures analyzed and proposed for implementation was the deployment of a dual-factor authentication solution for access to the organization's systems [90]. Given the situations analyzed in Section 5.5, we verified the urgent need to do so, especially in the resources most accessed by employees in telework, such as VPN and webmail. This method follows the premise of using two of the three following factors: *something you know* (for example, passwords), *something you have* (for example, tokens) and *something you are* (for example, fingerprints) [91].

All the analyzed systems in the Oeiras Municipality were based on a single authentication method with only the need for a user and password, which in the event of an account being compromised, it would be possible to access the institution's network from there. We studied several solutions and alternatives for this method, such as the use of physical tokens[92]. However this was discarded for its ease of being lost, stolen or simply forgotten by the user. The most viable solution was to use the cell phone as a means to use the second method, in this case it would be the receipt of a code per text message, which would later be inserted in the authentication window of the platform in question. It would also be possible to use it with the receipt of a notification, which only required a ”touch” on the user's cell phone screen to confirm that the access attempt was legitimate. The disadvantage of this solution was the acquisition of a two-factor authentication tool.

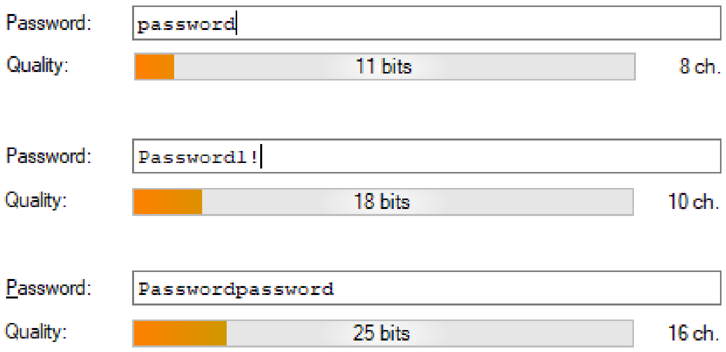
The technical specifications of the implementation of the solution were not considered relevant for the scope of this work, however only to point out that at the time of writing of this document, the solution was only deployed on the VPN access. As far as webmail access is concerned, this approach is at the moment not possible due to infrastructure architecture issues.

5.6.2 Password Management

Another of the conclusions that could be drawn from the answers to the questionnaire was that the management of employees' passwords is quite negligent, and there are even those who admit to using a document that they keep with them to manage their passwords. The policy in the Municipality establishes that the access passwords to the systems must contain at least 8 characters, including at least one capital letter, one small letter, a special character and a number.

However, in this work, we argue that these recommendations are outdated, not excluding that they were considered the most correct for several years. According to the National Institute of Standards and Technology (NIST), the guidelines for creating secure passwords no longer include the obligation to use this character mixture, since an analysis of leaked passwords databases found that they are not as secure as thought. This is mainly due to the fact that users were encouraged to only slightly change an insecure password by, for example, adding only a capital and a special character. As they were obliged by the security policy to change it, they repeated the process of a slight modification, always following variations of the previous key. For example, the password “password” would become “Password1!” If we analyze the complexity of this password in comparison with e.g. “Passwordpassword” which seems to be much simpler and easier to memorize, we realize that from the point of view of ease of attack, the latter is stronger (see Figure 5.7).

It stands to reason then that NIST's recommendations present today a greater relevance in the length of a password and not so much in its complexity when it comes to the mixture of characters [93]. Naturally, the adaptation of this measure does not alter the behavior of the users and does not force them to stop managing their passwords using a piece of paper that they keep with them. However it helps at least to strengthen this component when it comes to attempts to decipher the password, by an external agent. Independently of all measures, training and education of users is fundamental to raise their awareness to existing security risks.



Password: password

Quality: 11 bits 8 ch.

Password: Password1!

Quality: 18 bits 10 ch.

Password: Passwordpassword

Quality: 25 bits 16 ch.

Figure 5.7: Comparison of passwords strength.

5.6.3 Data Encryption

Once again, to overcome the limitations of the human factor in this matter and the fact that most users of the network and files of the Municipality have their computers at home, it became necessary to think about a measure to safeguard the information contained in them in the event of loss or misplacement.

In this sense, it was possible to use disk encryption software. Such a tool would verify the integrity of the hardware and the operating system at computer start-up. If this verification was successful then an encryption key was released which allowed the boot to continue. If the volume is removed from the machine it is practically impossible to read the information within the same [94]. This measure would protect the information contained in the machines that are outside the premises of the Municipality. However, due to data data recovery issues or troubleshooting by the Help Desk unit, it was not considered a measure to be applied, by the coordination of the Department. Nevertheless, it is an approach treated in this work.

5.6.4 Zero-trust Model

As seen in the sections above, the human being remains the weakest link in the security infrastructure of an organization. To minimize the dependency on user actions, it was advised that the Municipality adopts a zero-trust strategy. The current situation provides network users and resources with a static trust-based management that does not make periodic evaluations of access controls or makes use of a policy of "blacklisting" instead of "whitelisting". This type of model aims to improve security in a model that better adapts to the complexity of the network, the hypothesis of roaming workers and at the same time manages to protect users, devices and data, regardless of location.

This model assumes that security breaches can effectively occur and does not take as secure all the events that occur within the infrastructure. Before any access is given, it must be authenticated, authorized and encrypted. Also included is the "least access principle" [95], where only the necessary minimum rights must be granted to a user for access to a resource and for the shortest period of time possible. For example, employees of the Oeiras Municipality should not have administrator permissions on the machine they work on. It has also been advised to measure *microsegmentation* to minimize lateral movement on the network, i.e. not to allow someone with access to one server, for example, to move to another on the same network. Zero trust model is all about eliminating trust from a system rather than deeming a system as trusted [96]. This measure was handed over for further consideration by the management.

5.6.5 Procedures and Policies

When the answers to the inquiry were analyzed, we noticed that almost half of the participants answered that they did not know how to proceed in the occurrence of a cyber security incident. But when we asked the person responsible for this information, we reported that there was practically no documentation available to the IT Department employees and the one that existed was completely outdated. As part of this work, and in an attempt to provide some procedures to employees in situations related to information security, an Information Security Policy and an Incident Management Policy were developed. The first one intends to give the basis for the way information is managed, to provide specific standards considered correct by the various organic entities of the Municipality. The second aims to define the rules for a correct management of information security incidents, taking into account the appropriate reaction to such events and limitation of potential damage.

We argue that these documents have an important relevance because, as stated in [49], employees who are several times considered the weakest link in information security management, can also reveal themselves as valuable assets in risk reduction action. Employees who comply with these documents present themselves as a crucial factor in a good evaluation of information security.

5.7 Summary

This chapter intended to study the relationship of the Municipality's collaborators with the cyber-security theme. For this purpose, an inquiry was initially developed that intended to test the opinion and knowledge of the same collaborators, which allowed the conclusion that although most of them consider the subject important, they think that they no longer need more training on it. However, in the same survey it was possible to verify that they do not have enough knowledge or the best behaviors in the workplace. Scenarios that used social engineering techniques were put into practice, in which it became clear that this is the component of the topic in which the infrastructure is most vulnerable, given that all of them were given as successful. As a way to try to minimize some of these risks and strengthen the organization's resources, technical measures were outlined for specific risks.

In summary, the results of this study revealed that there is a clear flaw in the cybersecurity education of employees that can be solved with specific training. It was also possible to conclude that there are several technical measures that can be implemented to improve security in employee interaction with the technology.

Chapter 6

Conclusions and Future Work

Every day new vulnerabilities are found and various infrastructures are affected by them. In this work we had the objective of studying the vulnerabilities present in all the infrastructure that includes the IT Department of the Municipality of Oeiras. For this we divided the work in three parts, the implementation of a SIEM tool to increase the visibility of incidents that occur in the network, the use of tools for pentesting and analysis of vulnerabilities to discover and discuss the existence and resolution of these same vulnerabilities and, to finish, a study of notions and knowledge of cyber security with the employees of the Department that included an inquiry and drills of social engineering attacks.

It should be noted that these results were verified in an analysis directed only to the IT Deparment, as far as the other employees of the Municipality are concerned, we can expect an increase in illiteracy and lack of sensitivity on the subject. With these results, we can conclude that awareness has not been cared of and should be improved in all stakeholders. This is where training is recommended, to minimize risks and increase employees' knowledge. In such dispersed organizations, with such a complex and heterogeneous network, the risk of being connected to a malicious device or a malicious individual entering the facility increases considerably. It is therefore crucial to invest in the training of employees so that they can adopt more responsible behaviors in their daily lives. Although this investment may seem large and difficult to justify if there is no risk situation, if such and attack occurs the damage and costs to the municipality may be incalculable.

6.1 Achievements

The various contributions of this work that have as final objective the evaluation of security vulnerabilities of the infrastructure of the IT Department of the Municipality of Oeiras are:

The evaluation of the functionalities of a Security Information and Event Management tool allowed the conclusion that this type of platform greatly increases the visibility of incidents that occur in the infrastructure. The testbed employed used information regarding VPN access, which made the study somewhat limited, but sufficient to understand the added value of this type of tool. As a disadvantage, this platform has its license cost per data size processed, which was one of the causes for the analysis to be so limited. The creation of rules and alerts is also not very intuitive, since it always depends on whether for the selected source there is a native application or you need to create the indexing fields manually.

The manual vulnerability assessment using the open-source pentesting tools returned several interesting findings about the resources present in the infrastructure. It was possible to notice vulnerabilities in the configuration of certificates, servers, web applications, and content management platforms. These flaws, although not all described in the document, reveal that functionality is a priority above security, with some negligence in terms of configuration and maintenance of security services. All the vulnerabilities that have been discovered have a measure of resolution, some of them quite simple and do not clash with the commitment to functionality. Moreover, it was possible to notice with this chapter of the study, the heterogeneous way in which the present software is developed, without following secure implementation guidelines.

Regarding the study field of cybersecurity knowledge by the Municipality's employees, the performed inquiry allowed to conclude that there is a clear lack of knowledge and sensitivity on the subject, although in the answers most of the respondents affirm that they have enough knowledge on the subject to perform their function. This answer was contradicted by observing, daily, several unsafe behaviors on the workplace that do not follow the considered good practices of cybersecurity. As for the field scenarios that tested social engineering in the infrastructure, all of them were successful from the point of view of the attack, which means that from the point of view of security they revealed immense flaws and problems. From this, it is possible to conclude that an urgent need to training the Municipality's workforce, both in theoretical and practical knowledge of good practice in workplace safety.

In summary, this work allows to conclude that the Municipality should not assume itself as safe and with the best cybersecurity practices. It also revealed that several behaviors must be improved, and several resolution measures that allow improvising the posture of the infrastructure regarding the matter, must be put into practice.

6.2 Future Work

The SIEM tool could be much more productive for the provided purpose, with more sources so it can make better use of its event correlation functionality.

The use of vulnerability analysis tools should also be done regularly and to all the resources of the Municipality, with a properly documented process to treat the resulting vulnerabilities. In parallel, guidelines and an operation manual should be established on how to perform software updates on the organization's machines.

Finally a future step should also include, training on cyber-security would be taught to employees of the Municipality of Oeiras, involving issues such as social engineering and good practices to have in the workplace.

Bibliography

[1] Symantec, Inc. A new zero-day vulnerability discovered each week. https://www.symantec.com/security-center/threat-report, , , visited 2019-12-29.

[2] Ponemon Institute LLC. 2018 cost of data breach study: Impact of business continuity management, October 2018. https://www.ibm.com/downloads/cas/AEJYBPWA, visited 2019-10-21.

[3] N. A. Joseph Muniz, Gary McIntyre. *Security Operations Center: Building, Operating, and Maintaining Your SOC*. Cisco Press, Indianapolis, 46240 USA, 2 edition, 2016.

[4] C. Crowley and J. Pescatore. The definition of soc-cess, August 2018. https://www.sans.org/reading-room/whitepapers/analyst/definition-soc-cess-2018, visited 2019-11-15.

[5] Microsoft Active Directory,. https://social.technet.microsoft.com/wiki/contents/articles/28644.active-directory-snapshot.aspx., visited 2019-12-01.

[6] M. Gosser. Uc davis. https://seclab.cs.ucdavis.edu, visited 2019-12-02.

[7] Common Vulnerabilities and Exposures. vulnerability terminology. https://cve.mitre.org/about/terminology.html, , visited 2019-12-03.

[8] European Union Agency for Cybersecurity. Vulnerability definition,. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary, visited 2019-12-03.

[9] Microsoft. Security update severity rating system,. https://www.microsoft.com/en-us/msrc/security-update-severity-rating-system, visited 2019-12-03.

[10] ISO 27000. Infosec definitions,. https://https://www.praxiom.com/iso-27000-definitions.htm#Vulnerability, visited 2019-12-03.

[11] OWASP ZAP ,. https://www.zaproxy.org/docs/, visited 2019-12-09.

[12] D. M. U. K. Kavita S. Kumavat, Ranjana P. Dahake. Overview of vulnerability analysis. *International Journal of Emerging Technology and Advanced Engineering*, 3(10), October 2013. ISSN 2250-2459.

[13] OWASP Project,, . https://owasp.org/www-project-top-ten/, visited 2020-06-09.

[14] Difference between active passive vulnerability scanners. https://smallbusiness.chron.com/difference-between-active-passive-vulnerability-scanners-34805.html, visited 2019-11-28.

[15] Security through Education. Social engineering defined,. https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/, visited 2019-12-06.

[16] Carson Zimmerman. Mitre - ten strategies of a world-class cybersecurity operations center, 2014. https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf, visited 2019-10-15.

[17] McAfee. What is a soc?,. https://www.mcafee.com/enterprise/en-ca/security-awareness/operations/what-is-soc.html, visited 2019-11-06.

[18] R. Shirey,. Internet security glossary,, August 2007. https://tools.ietf.org/html/rfc4949, visited 2019-11-20.

[19] Gartner, Inc. Information technology gartner glossary,. https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider, visited 2019-11-29.

[20] T. B. Kelly Kavanagh, Gorka Sadowski. *Magic Quadrant for Security Information and Event Management*. Gartner, Inc., Stamford, 06902 USA, 2018. https://www.gartner.com/doc/3894573/magic-quadrant-security-information-event.

[21] R. Shirey,. Internet security glossary,, August 2007. https://tools.ietf.org/html/rfc5424, visited 2019-11-29.

[22] Kim Crawley, ATT Cybersecurity. How siem correlation rules work,. https://cybersecurity.att.com/blogs/security-essentials/how-siem-correlation-rules-work, visited 2019-11-29.

[23] N. Karangle, A. K. Mishra, and D. A. Khan. Comparison of nikto and uniscan for measuring url vulnerability. pages 1–6, 2019. doi: 10.1109/ICCCNT45670.2019.8944463.

[24] OpenVAS Overview,. http://www.openvas.org/about.html, visited 2019-12-09.

[25] G. F. Lyon. *Nmap Network Scanning : Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com LLC, Sunnyvale, 94086 USA, 2008. http://www.nmap.org/book.

[26] Nikto,. https://resources.infosecinstitute.com/introduction-nikto/, visited 2019-12-09.

[27] A. K. B. R. Vibhandik. Vulnerability assessment of web applications - a testing approach. *Forth International Conference on e-Technologies and Networks for Development (ICeND)*, pages 1–6, September 2015. doi: 10.1109/ICeND.2015.7328531.

[28] OWASP Project,, . https://owasp.org/www-project-top-ten/, visited 2020-06-09.

[29] M. Focus. *ArcSight Enterprise Security Manager: Data Sheet*. 2018. https://www.microfocus.com/media/flyer/arcsight_enterprise_security_manager_ds.pdf.

[30] ATT Cybersecurity,. https://cybersecurity.att.com/documentation/usm-appliance/intro/security-concepts-terminology.htm, visited 2019-12-18.

[31] IBM,. https://https://mindmajix.com/ibm-qradar-tutorial, visited 2019-12-18.

[32] Splunk Documentation,. https://docs.splunk.com/Documentation/Splunk/8.0.1/Updating/Deploymentserverarchitecture, visited 2019-12-18.

[33] D. H. Lakshminarayana, J. Philips, and N. Tabrizi. A survey of intrusion detection techniques. pages 1122–1129, 2019. doi: 10.1109/ICMLA.2019.00187.

[34] U. Bashir and M. Chachoo. Intrusion detection and prevention system: Challenges opportunities. pages 806–809, 2014. doi: 10.1109/IndiaCom.2014.6828073.

[35] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi. A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1):41–50, 2018. doi: 10.1109/TETCI.2017.2772792.

[36] A. Warzyński and G. Kołaczek. Intrusion detection systems vulnerability on adversarial examples. pages 1–4, 2018. doi: 10.1109/INISTA.2018.8466271.

[37] J. Goel and B. Mehtre. Vulnerability assessment penetration testing as a cyber defence technology. *Procedia Computer Science*, 57:710–715, 12 2015. doi: 10.1016/j.procs.2015.07.458.

[38] P. S. Shinde and S. Ardhapurkar. Cyber security analysis using vulnerability assessment and penetration testing. *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, pages 1–5, 2016.

[39] M. Shah, A. Sajid, M. Kamran, Q. Javaid, and S. Zhang. An analysis on host vulnerability evaluation of modern operating systems. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 7:245–254, 05 2016. doi: 10.14569/IJACSA.2016.070430.

[40] S. Umrao, M. Kaur, and G. GUPTA. Vulnerabilty assessment and penetration testing. *International Journal of Computer Communication Technology (IJCCT) ISSN (ONLINE): 2231 - 0371*, 3:71–74, 01 2012. doi: 10.47893/IJCCT.2016.1367.

[41] P. Xiong and L. Peyton. A model-driven penetration test framework for web applications, 2010.

[42] A. Austin and L. Williams. One technique is not enough: A comparison of vulnerability discovery techniques. pages 97–106, 2011. doi: 10.1109/ESEM.2011.18.

[43] M. Landauer, F. Skopik, M. Wurzenberger, and A. Rauber. System log clustering approaches for cyber security applications: A survey. *Computers Security*, 92:101739, 05 2020. doi: 10.1016/j.cose.2020.101739.

[44] S. Messaoudi, A. Panichella, D. Bianculli, L. Briand, and R. Sasnauskas. A search-based approach for accurate identification of log message formats. pages 167–177, 05 2018. doi: 10.1145/3196321.3196340.

[45] Z. Li, M. Davidson, S. Fu, S. Blanchard, and M. Lang. Converting unstructured system logs into structured event list for anomaly detection. *ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security*, pages 1–10, 08 2018. doi: 10.1145/3230833.3230855.

[46] A. Haque, A. DeLucia, and E. Baseman. Markov chain modeling for anomaly detection in high performance computing system logs. 2017. doi: 10.1145/3152493.3152559. URL `https://doi.org/10.1145/3152493.3152559`.

[47] R. Montesino, S. Fenz, and W. Baluja García. Siem-based framework for security controls automation. *Information Management Computer Security*, 20, 10 2012. doi: 10.1108/09685221211267639.

[48] M. Landauer, F. Skopik, M. Wurzenberger, and A. Rauber. System log clustering approaches for cyber security applications: A survey. *Computers Security*, 92:101739, 05 2020. doi: 10.1016/j.cose.2020.101739.

[49] B. Bulgurcu, H. Cavusoglu, and I. Benbasat. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. 34(3), 2010. ISSN 0276-7783.

[50] L. Souza, M. Silva, and T. Ferreira. The acceptance of information technology by the accounting area. *Sistemas Gestão*, 12:516–524, 12 2017. doi: 10.20985/1980-5160.2017.v12n4.1239.

[51] H.-S. Rhee, C. Kim, and Y. Ryu. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers Security*, 28:816–826, 11 2009. doi: 10.1016/j.cose.2009.05.008.

[52] R. Heartfield and G. Loukas. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers Security*, 76, 02 2018. doi: 10.1016/j.cose.2018.02.020.

[53] R. Heartfield, G. Loukas, and D. Gan. An eye for deception: A case study in utilising the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks. 06 2017. doi: 10.1109/SERA.2017.7965754.

[54] K. Krol, J. Spring, S. Parkin, and A. Sasse. Towards robust experimental design for user studies in security and privacy. 05 2016.

[55] S. Rahman, R. Heartfield, W. Oliff, G. Loukas, and A. Filippoupolitis. Assessing the cyber-trustworthiness of human-as-a-sensor reports from mobile devices. 06 2017. doi: 10.1109/SERA.2017.7965756.

[56] K. M. Kavanagh, T. Bussa. Critical capabilities for security information and event management, 2020. https://http://www.softshell.ag/wpcontent/uploads/2020/02/magic_quadrant_for_security__315428.pdf,.

[57] Splunk Documentation, . https://docs.splunk.com/Documentation/Splunk/8.1.0/Overview/AboutSplunkEnterprisedeployments, visited 2020-08-07.

[58] Splunk Documentation, . https://www.splunk.com/en_us/resources/search-processing-language.html, visited 2020-08-07.

[59] Splunk Documentation, . https://docs.splunk.com/Documentation/Splunk/8.1.0/Capacity/Estimateyourstoragerequirements, visited 2020-06-07.

[60] N. R. Z. Z. H. Zhang, D. Yao. Causality reasoning about network events for detecting stealthy malware activities. *Computers Security*, 58:180–198, 2016. doi: 10.1016/j.cose.2016.01.002.

[61] Qualys, Inc. Ssl server test. https://www.ssllabs.com/ssltest/, visited 2020-10-29.

[62] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov. The most dangerous code in the world: validating ssl certificates in non-browser software. pages 38–49, 10 2012. doi: 10.1145/2382196.2382204.

[63] Y. Xiao, M. Li, S. Chen, and Y. Zhang. Stacco: Differentially analyzing side-channel traces for detecting ssl/tls vulnerabilities in secure enclaves. 2017. doi: 10.1145/3133956.3134016. URL https://doi.org/10.1145/3133956.3134016.

[64] B. Möller, T. Duong, and K. Kotowicz. This poodle bites: Exploiting the ssl 3.0 fallback. 2014.

[65] N. Aviram, S. Schinzel, J. Somorovsky, N. Heninger, M. Dankel, J. Steube, L. Valenta, D. Adrian, J. A. Halderman, V. Dukhovni, E. Käsper, S. Cohney, S. Engels, C. Paar, and Y. Shavitt. Drown: Breaking tls using sslv2. 2016.

[66] D. Baker, S. M. Christey, W. H. Hill, and D. Mann. The development of a common vulnerability enumeration. 1999.

[67] S. B. Roosa and S. Schultze. Trust darknet: Control and compromise in the internet's certificate authority model. *IEEE Internet Computing*, 17(3):18–25, 2013. doi: 10.1109/MIC.2013.27.

[68] B. Lee and K. Kim. Self-certificate: Pki using self-certified key. 01 2002.

[69] W. G. J. Halfond, S. R. Choudhary, and A. Orso. Penetration testing with improved input vector identification. pages 346–355, 2009. doi: 10.1109/ICST.2009.26.

[70] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta. Effective penetration testing with metasploit framework and methodologies. pages 237–242, 2014. doi: 10.1109/CINTI.2014.7028682.

[71] CVE Details. https://www.cvedetails.com/vulnerability-list/vendor_id-185/product_id-316/version_id-61898/Mysql-Mysql-5.1.html, visited 2020-11-26.

[72] . A. J. A. Najera-Gutierrez, G. *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux*. Packt Publishing Ltd, 2018.

[73] J. Kelsey. Compression and information leakage of plaintext. 2365:263–276, 2002. doi: 10.1007/3-540-45661-9_21. URL `https://iacr.org/archive/fse2002/23650264/23650264.pdf`.

[74] D. Lee, J. Rowe, C. Ko, and K. Levitt. Detecting and defending against web-server fingerprinting. pages 321–330, 2002. doi: 10.1109/CSAC.2002.1176304.

[75] J. A. Shamsi, S. Hameed, W. Rahman, F. Zuberi, K. Altaf, and A. Amjad. Clicksafe: Providing security against clickjacking attacks. pages 206–210, 2014. doi: 10.1109/HASE.2014.36.

[76] H. Z. N. A. Isatou Hydara, Abu Bakar Md. Sultan. Current state of research on cross-site scripting (xss). pages 170–186, 2015. doi: /10.1016/j.infsof.2014.07.010.

[77] L. K. Shar and H. B. K. Tan. Defeating sql injection. *Computer*, 46(3):69–77, 2013. doi: 10.1109/MC.2012.283.

[78] K.-S. Lhee and S. J. Chapin. Buffer overflow and format string overflow vulnerabilities. *Software: Practice and Experience*, 33(5):423–460. doi: https://doi.org/10.1002/spe.515. URL `https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.515`.

[79] Y. Sun, Z. Zhuang, and C. L. Giles. A large-scale study of robots.txt. 2007. doi: 10.1145/1242572.1242726. URL `https://doi.org/10.1145/1242572.1242726`.

[80] K. E. Silaen and C. Lim. A novel countermeasure to prevent xmlrpc wordpress attack. pages 1–6, 2016. doi: 10.1109/ICODSE.2016.7936147.

[81] J. A. P. Savan K. Patel and A. V. Patel. Statistical analysis of seo for joomla, drupal and wordpress. 52:1–5, August 2012. doi: 10.5120/8179-1502.

[82] A. F. Peter W. Singer. *Cybersecurity: What Everyone Needs to Know*. 2014. `https://www.microfocus.com/media/flyer/arcsight_enterprise_security_manager_ds.pdf`.

[83] S. L. T. Kaushalya, R. Randeniya. An overview of social engineering in the context of information security. *IEEE 5th International Conference on Engineering Technologies and Applied Sciences*, 58:1–6, 2018. doi: 10.1109/ICETAS.2018.8629126.

[84] K. R. Sarkar. Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report*, 15:112–133, 2010. doi: 10.1016/j.istr.2010.11.002.

[85] T. Kaushalya, R. Randeniya, and S. Liyanage. An overview of social engineering in the context of information security. pages 1–6, 11 2018. doi: 10.1109/ICETAS.2018.8629126.

[86] W. Maconachy, C. Schou, D. Ragsdale, and D. Welch. A model for information assurance:an integrated approach. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, January 2001.

[87] B. C. Quantitative and qualitative research: Perceptual foundations. *International Journal of Market Research*, 57:837–854, 2015. doi: 10.2501/IJMR-2015-070.

[88] K. Mccusker and S. Gunaydin. Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion*, 30, 11 2014. doi: 10.1177/0267659114559116.

[89] F. Mouton, M. Malan, L. Leenen, and H. Venter. Social engineering attack framework. *Information Security for South Africa*, 08 2014. doi: 10.1109/ISSA.2014.6950510.

[90] F. Aloul, S. Zahidi, and W. El-Hajj. Two factor authentication using mobile phones. *2009 IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2009*, pages 641–644, 05 2009. doi: 10.1109/AICCSA.2009.5069395.

[91] B. Schneier. Two-factor authentication: Too little, too late. *Commun. ACM*, 48(4):136, Apr. 2005. doi: 10.1145/1053291.1053327. URL `https://doi.org/10.1145/1053291.1053327`.

[92] K. Krol, E. Philippou, E. De Cristofaro, and A. Sasse. ”they brought in the horrible key ring thing!” analysing the usability of two-factor authentication in uk online banking. 01 2015. doi: 10.14722/usec.2015.23001.

[93] J. F. R. P. Paul Grassi, Elaine Newton. *Digital Identity Guidelines: Authentication and Lifecycle Management*. NIST - National Institute of Standards and Technology, 2017.

[94] J. Kornblum. Implementing bitlocker drive encryption for forensic analysis. *Digital Investigation*, 5: 75–84, 03 2009. doi: 10.1016/j.diin.2009.01.001.

[95] R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee. Access control policy enforcement for zero-trust-networking. pages 1–6, 2018. doi: 10.1109/ISSC.2018.8585365.

[96] S. Mehraj and M. T. Banday. Establishing a zero trust strategy in cloud computing environment. pages 1–6, 2020. doi: 10.1109/ICCCI48352.2020.9104214.

Appendix A

On this appendix it is presented the survey that the collaborators of the IT Department of the Municipality of Oeiras answered.

Inquérito de Cibersegurança

No âmbito da minha tese de Mestrado em Engenharia de Telecomunicações e Informática e com vista a suprimir a constante necessidade e desejo de melhorar a postura do Departamento de Informática do Município de Oeiras face à materia de cibersegurança , foi desenvolvido este questionário para aferir o conhecimento e comportamento dos seus colaboradores.
As respostas são completamente anónimas e pede-se que seja respondido com a maior das sinceridades porque só assim é possível entender e melhorar as aspetos que precisam de tal melhoria.
Este inquérito foi desenvolvido pelo Núcleo de Segurança e Monitorização e qualquer dúvida deve ser dirigida ao mesmo através de: nsm@cmoeiras.pt.
*Obrigatório

1. Género: *

Marcar apenas uma oval.

○ Feminino
○ Masculino
○ Outro

2. Idade: *

Marcar apenas uma oval.

○ Abaixo de 30 anos
○ Entre 30 e 39 anos, inclusivé
○ Entre 40 e 49 anos, inclusivé
○ Entre 50 e 64 anos, inclusivé
○ Mais de 65 anos

3. Descrição do seu trabalho: *

Marcar apenas uma oval.

○ Apoio-local

○ Desenvolvimento de software

○ Executivo

○ Coordenação

○ Administrativo

○ Gestão de infraestruturas

○ Segurança

○ Outro

4. Alguma vez participou numa ação de sensibilização ou formação sobre cibersegurança? *

Marcar apenas uma oval.

○ Sim, mais que uma vez.

○ Sim, uma vez.

○ Não.

5. Acha que este tópico é importante e os funcionários do Município devem ser formados nesse sentido? *

Marcar apenas uma oval.

○ Discordo.

○ Concordo.

○ Não tenho a certeza.

6. Considera ter conhecimento suficiente sobre a matéria para executar a sua função? *

Marcar apenas uma oval.

○ Sim.

○ Não.

○ Não tenho a certeza.

7. Possui as instruções sobre como proceder na ocorrência de um incidente de cibersegurança? *

Marcar apenas uma oval.

○ Sim.

○ Não.

○ Algumas.

8. Responda agora a algumas questões sobre cenários hipotéticos. Quando não está no computador: *

Marcar apenas uma oval.

○ Faz logout da sua sessão.

○ Desliga-o completamente.

○ Deixa o computador desbloqueado.

○ Desliga apenas os monitores.

○ Bloqueia a sua sessão.

9. Encontrou uma pen USB no estacionamento. O que faz a seguir? *

Marcar apenas uma oval.

○ Abro no meu computador pessoal para perceber a quem pertence.

○ Abro no meu computador de trabalho para perceber a quem pertence.

○ Entrego a mesma no Departamento de Informática.

○ Nenhuma das anteriores.

10. Recebeu um email suspeito. Como procede? *

Marcar apenas uma oval.

○ Elimino-o.

○ Movo-o para a pasta do SPAM.

○ Reencaminho-o para o Núcleo de Segurança e Monitorização.

○ Não tenho a certeza.

11. Utiliza o seu email profissional em logins de plataformas não relacionadas com trabalho? *

Marcar apenas uma oval.

○ Sim.

○ Não.

○ Não me lembro.

12. Considera segura a utilização de Wifi's de espaços públicos, com e sem autenticação? *

Marcar apenas uma oval.

○ Sim.

○ Nada seguro.

○ Parcialmente seguro.

13. Escolha a palavra passe mais segura: *

Marcar apenas uma oval.

○ Malafana1!

○ 1234567890

○ Phirikitahaaste

○ 7Kxl9uy”9o

14. Usa a mesma palavra passe para várias sessões em dispositivos ou plataformas diferentes? *

Marcar apenas uma oval.

○ Sim.

○ Não.

○ Não tenho a certeza.

15. Como faz a gestão das suas passwords? *

Marcar apenas uma oval.

○ Memorização.

○ Software de gestão de passwords.

○ Escrevo num documento que guardo comigo.

16. Durante a situação de teletrabalho tem necessidade de utilizar algum dispositivo pessoal para aceder a materiais de teletrabalho? *

Marcar apenas uma oval.

○ Sim.

○ Não.

○ Talvez.

17. Partilhava o seu computador profissional com alguém na sua casa? *

Marcar apenas uma oval.

○ Sim.

○ Não.

○ Talvez.

18. Considera que enquanto esteve em situação de trabalho remoto teve em atenção as boas práticas de cibersegurança? *

Marcar apenas uma oval.

○ Sim.

○ Não.

○ Não sei que boas práticas são essas.

19. Como classifica o ecossistema de trabalho no que toca à matéria de Cibersegurança? (Isto inclui aspetos do ponto de vista computacional, comportamental e físico). *

Marcar apenas uma oval.

○ Seguro.

○ Inseguro.

○ Há bastantes melhorias a fazer.

○ Há algumas melhorias a fazer.

○ Não é preciso melhorar nada.

Obrigado pela sua participação.

OEIRAS VALLEY PORTUGAL | MUNICÍPIO OEIRAS

Este conteúdo não foi criado nem aprovado pela Google.

Google Formulários