kriativ.tech

Edição Nº 9
ISSN Print: 1646-9976 | ISSN Online: 2184-223X |
http://www.kriativ-tech.com
DOI: 10.31112/kriativ-tech-2023-06-92

Information Technologies and Cybersecurity

Luísa Orvalho
Professor Coordinator and Research at CITECA - ISTEC Porto - luisa.orvalho@my.istec.pt
Researcher at CEDH - Portuguese Catholic University - lorvalho@ucp.pt

Mariana Lopes
3rd year Student of the degree in Multimedia Engineering - ISTEC Porto
mariana.lopes.70064@my.istec.pt

Francisco Santos
3rd year Student of the degree in Multimedia Engineering - ISTEC Porto
francisco.santos.70061@my.istec.pt

Abstract: *The rapid evolution of Information Technology (IT) and the growing use of connected devices have driven the need for enhanced cybersecurity measures. This scientific article examines the interaction between IT and cybersecurity, highlighting the challenges faced in the current era due to the emergence of cyber threats and the need to protect data and systems. It emphasizes best practices in cybersecurity, including technical measures, awareness and training, as well as the industry standards, legislation, and regulations in this field. The article concludes that a holistic approach is essential to address the challenges of cybersecurity and ensure trust in the digital era.*

Keywords: *Information Technologies, Cybersecurity, Data Security, Types of Cyber Attacks, Security measures, GDPR, CNCS, C-DAYS*

1. Introduction

Information technology (IT) and cybersecurity play a key role in society. Cybersecurity refers to the set of tools, practices and measures adopted to protect information, computer systems and networks against cyber threats, ensuring the confidentiality, integrity and availability of data.

With the evolution of IT, cybersecurity has become a concern for everyone, bringing new challenges and threats, such as the possibility of data theft, unauthorized access, malware and hacker attacks, among others.

Cybersecurity involves a series of practices and techniques that aim to identify, prevent, and respond to these threats. It includes the implementation of firewalls, intrusion detection systems, encryption, user authentication, regular backups, security policies, and user awareness.

In addition, cybersecurity also covers the protection of critical infrastructure, such as power grids, transportation systems, and financial services, which are frequent targets of cyberattacks. In particular, this article studies the topic of information technology and cybersecurity, presents the differences between the two concepts, security measures for protection against cyberattacks, the General Data Protection Regulation (GDPR), the main standards and frameworks for the industry's approach to information technology and cybersecurity. The article concludes with the vision and identification of the challenges faced by Portugal within the National Center for Cybersecurity (CNCS).

With the growing threat of cyberattacks, it is critical to implement effective security measures to protect systems and data. Cybersecurity is not only the responsibility of organizations, but also of each individual who uses technology.

2. Information Technology and Cybersecurity

IT and Cybersecurity are areas that aim to protect information systems and ensure the security of data and digital communications. They involve the use of technologies, processes and practices to protect networks, devices, programs and data from cyber threats.[1].

IT refers to the use of hardware, software, networks and infrastructure to store, transmit, process and manage information. It includes computers, servers, databases, operating systems, software applications and network services. Cybersecurity, in turn, concerns the practices and measures adopted to protect information systems against cyber-attacks, which may include malware, phishing, hacking, DDoS attacks and data theft. Cybersecurity aims to ensure the confidentiality, integrity and availability of data, as well as protecting an organisation's IT infrastructure.

Cybersecurity technologies include firewalls, intrusion detection and prevention systems, encryption, user authentication, identity management systems, security analysis and network monitoring [1].

3.Difference between Information Technology and Cybersecurity

Information Technology and Cybersecurity are two related but differentiated areas within the field of technology. The main differences can be summarised:

Information Technology:

- Management and support of an organisation's information-related technologies.
- It involves the implementation, maintenance and support of computer systems, networks, hardware, software and IT infrastructure.

- IT professionals are responsible for ensuring that information systems function properly, are available to users, and meet the organisation's needs.
- Their activities involve server configuration and maintenance, database administration, network management, technical support to users, software development, among others.

Cybersecurity:

- A specialized discipline within IT that focuses on protecting information systems from cyber threats.
- It involves the implementation of security measures to protect systems, networks, data and information against cyber-attacks such as malware, hacking, data theft, phishing, among others.
- Cybersecurity professionals are responsible for identifying vulnerabilities, implementing security controls, monitoring threats, responding to security issues and developing strategies to protect an organisation's data.
- Their activities include configuring firewalls, detecting and explaining security issues, encrypting data, implementing security policies, among others [2].

In summary, IT is a broader area that covers all aspects related to information technologies, while cybersecurity is a specialised discipline within IT, specifically focused on cyber threat protection and information systems security. Both are important areas to ensure the efficiency, safety and security of an organisation's information resources [3].

4. General Data Protection Regulation

The General Data Protection Regulation (GDPR), known in English as the General Data Protection Regulation (GDPR), is European Union legislation that came into force on 25 May 2018. It sets out rules and regulations for the protection and processing of personal data of European Union (EU) citizens.

The main aim of the GDPR is to provide greater control and privacy to individuals over their personal data, as well as to reconcile data protection laws across the EU. It also applies to all organisations that check the personal data of every individual in the EU, regardless of whether they are located in the EU or not.

The GDPR sets out a number of rights for individuals, including the right to access their personal data, the right to correct undetermined data, the right to have their data deleted and the right to data portability, etc.

In addition to the rights of each individual, the GDPR also places obligations on organisations to let the personal data of each individual be exposed. This includes obtaining individuals'

explicit consent to process their data, implementing appropriate security measures to protect personal data, notifying data breaches to authorities and affected individuals, and appointing a Data Protection Officer (EPD/DPO) in certain cases.

Organisations that do not comply with the RGPD can face significant fines, which can be as high as 4% of the company's annual global turnover or €20 million.

Importantly, the RGPD does not only apply to companies established in the EU, but also to companies outside the EU that offer goods or services to EU citizens, or monitor the behaviour of individuals in the EU.

The RGPD represents a significant change in the way personal data is handled and protected in the EU, and has influenced other data protection legislation around the world [4].

5. Most common types of cyberattacks

There are various types of cyberattacks.

Some of the frequent types are [5]:

Phishing: type of attack where hackers impersonate a trusted entity, usually by email, instant messaging or fake websites, to trick people into obtaining personal information such as passwords, credit card numbers, etc.

Malware: Malicious software designed to infect computers and devices, compromising their security and privacy. The most common types of malware include viruses, ransomware and trojans.

DDoS attack: hackers overload a system or network with excessive traffic, making it inaccessible to legitimate users. These attacks are usually carried out using botnets, remotely controlled networks of infected devices.

Injection attacks: in this attack, hackers exploit vulnerabilities in web applications that do not properly validate or filter user input. One of the most common examples is the SQ injection attack, in which they insert malicious SQL commands into input fields to gain unauthorized access to the database.

Brute force attacks: in this attack, hackers try to guess passwords or combinations until they find the correct one. They usually use authorized programs and test several combinations at a very high speed.

Unsecured Wi-Fi attacks: occurs when criminals prevent traffic on an unprotected Wi-Fi network, capture confidential information such as passwords or personal data, transmitted over the network.

Ransomware: the famous data hijackers, prevent access to data, request a payment to ransom and release files, often under the threat of leakage, publication or deletion.

SMShing: attack using fake text messaging with malicious links.

6. Security Measures to protect against cyberattacks.

For organisations and information systems to protect themselves against cyberattacks they need to implement some security measures. Listed below are some of them:

Software update: keep your operating system, applications and security software up to date with the latest versions. Frequent updates include important security patches that help protect against known vulnerabilities.

Firewall: use a firewall to control network traffic and block unauthorized access to your systems. A well-configured firewall helps filter malicious traffic and reduces the attack surface.

Antivirus and anti-malware: install an antivirus and anti-malware that you trust on all your devices to protect against malware, viruses and other threats. Keep these tools up to date to get the latest protection.

Strong passwords: use strong passwords for all accounts and change them regularly. Avoid obvious or common passwords, and consider using a password management solution to securely generate and store passwords [6].

Two-factor authentication: enable two-factor authentication whenever you can. This strengthens the security of your account, as a second form of verification besides the password is recommended, such as a code sent to your mobile phone.

Data backup: back up your data habitually and check that the backups are being carried out correctly. This will help minimize damage in the event of a data breach or ransomware attacks [7].

7. Different standards relating to information technology and cybersecurity in industry

Some of the most significant standards and frameworks for addressing information technology and cybersecurity in the industry are:

ISO/IEC 27001 standard: this standard sets out the requirements for an information security management system (ISMS). It is adopted in various industries and provides guidelines for identifying, assessing and addressing information security risks, as well as establishing control measures and improving information security in an organization.

NIST Cybersecurity Framework (CSF): framework developed by the National Institute of Standards and Technology (NIST) in the United States, the same provides guidelines for organisations to improve all their sectors and their security posture and culture. This framework provides a risk-based approach, identifying cybersecurity roles, categories and controls.

COBIT (Control Objectives for Information and Related Technologies): is a framework developed by ISACA (Information Systems Audit and Control Association) that provides guidance to govern information technology management. It

helps organisations to establish and control security effects, managing technology-related risks.

PCI DSS (Payment Card Industry Data Security Standard): is a set of security requirements for organisations to keep payment card data secure. It is maintained by the Payment Card Industry Security Standards Council and aims to protect payment card information from theft and fraud.

HIPAA (Health Insurance Portability and Accountability Act): is a USA legislation that establishes security and privacy requirements to protect health information. It is applied to healthcare organisations and their business partners and sets standards for the protection of patient health data.

These are just some of the most widely used standards and frameworks in the industry to address information technology and cybersecurity issues. The choice of the most appropriate standards and frameworks depends on the specific industry requirements, applicable regulations and needs of the organisation. [1].

8. Cybersecurity in Portugal

According to the latest cybersecurity forecasts from Canalys, global spending on cybersecurity will be around 13.2% by 2023, including services and products. Total spending by year-end 2023 is expected to reach $223.8 billion [8].

Ransomware remains the biggest threat to organisations from an operational, financial and branding perspective. But the emergence and abuse of generative AI models such as ChatGPT will raise the risk to another level by 2023.

Canalys' chief analyst said that the emergence of this and other new technologies:

> (...) will enable and accelerate the creation of malicious code on an industrial scale by more threat actors and increase the frequency and scope of attacks. Organisations are already struggling to cope with current threat levels and cannot cut spending as this will leave them even more vulnerable. Instead, they will need to work closer with Channel Partners to make smarter investments [9].

Security services include implementation, integration and maintenance with the possibility of growing by 14.1% to $144.3 billion by 2023. The value represents about 64.5% of the global cybersecurity market in 2023. Srikara Upadhyaya, research analyst at Canalys noted:

> Organisations will continue to transform their cybersecurity strategies to increase their resilience during the year. Implementing Zero Trust architectures to address vulnerabilities successfully exploited in the last three years since the pandemic began will be the central theme, noted Srikara Upadhyaya, research analyst at Canalys.
>
> (…) This will generate more consulting engagements for Channel Partners, as well as create opportunities to implement and integrate multiple products from different vendors, reducing operational complexity for managed services. Overall, more than 90% of total spending on cybersecurity products and

services will go through Channel Partners by 2023 [9].

Sales of cybersecurity products, including endpoint security, network security, email web security and data security will increase by 11.7% to 79.5 billion in 2023. Portugal ranks 31st of the most affected countries in the world due to ransomware attacks, out of 101 countries [10].

In Portugal, the body responsible for cybersecurity is the National Centre for Cybersecurity **(CNCS).** The CNCS is a government entity that aims to protect and strengthen cybersecurity in Portugal. Its main role is to coordinate, monitor and respond to cybersecurity incidents across the country's critical infrastructure, including government, financial, healthcare and transport sectors. In addition, CNCS also promotes cybersecurity awareness and training, collaborates with public and private entities and develops strategies to address cyber threats in Portugal.

9. Conclusion

Information technology and cybersecurity play a crucial role in protecting organisations' systems and data. The evolution of technology has brought numerous benefits, but it has also increased the risks associated with information security.

To mitigate these risks, it is essential that organisations adopt specific approaches and standards for information security. Standards such as ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, PCI DSS and HIPAA provide guidance to ensure systems and data are adequately protected. However, it is important to remember that cybersecurity should be checked on a daily basis.

Threats and challenges constantly change, requiring greater security. As well as adopting the right standards, organisations must invest in training and awareness for their staff and employees, conduct regular security testing, stay up-to-date on the latest threats and vulnerabilities, and be prepared to respond to and recover from security incidents. By taking a comprehensive approach to information technology and cybersecurity, organisations can mitigate risk and protect themselves by ensuring confidentiality and integrity in their data. By 2021 cybersecurity spending has increased by between 6% and 10%, [11] and is an opportunity for growth.

In the enterprise, experts predicted growth of a 10% increase in cyber spending. [12] Even so, there are worrying factors and a study that the same company conducted concluded if 36% of companies are not sure if their employees would be able to prevent and detect a cyberattack. [12]

2022 was a terrible year for Portugal in terms of cybersecurity as many companies and organisations ended up being attacked, such as: Impresa, Vodafone, Hospital Garcia de Horta, Sonae, BCP, EMGFA, TAP, Germano de Sousa clinic, Lusa Agency, FC Porto, etc. These are some of the organisations that last year suffered large-scale attacks and were targeted for information theft, many without recovery, this situation is seen

as an alert to the need for Portugal to continue investing in cybersecurity [13].

10. References

[1] Martins, J. C. (2021). *Gestão de Segurança da Informação e cibersegurança nas organizações* (1ª Edição). Silabas & Desafios.

[2] Infoprotect. (2023). *5 maiores tecnologias de cibersegurança.* [Web Page]. https://infoprotect.com.br/5-maiorestecnologias-da-ciberseguranca/.

[3] Cecyber. (2022). *Diferenças entre TI e Cibersegurança.* [Web Page]. https://cecyber.com/diferencas-entre-ti-eciberseguranca/

[4] Iubenda. (2023). *O que é GDPR? Um guia completo com tudo que você precisa saber para estar em conformidad*e. [Web Page]. https://www.iubenda.com/pt-br/help/43925-oque-e-o-gdpr-um-guia-completo-sobre-tudo-oque-voce-saber-para-estar-em-conformidade

[5] Kelvin Zimmer. (2020, setembro 9). *8 tipos de ataques cibernéticos e como se proteger.* [Web Page]. https://www.lumiun.com/blog/8-tiposde-ataques-ciberneticos-e-como-se-proteger/

[6] NAU. (2021, 30 de novembro). *Boas práticas de cibersegurança – os cinco pontos críticos* [Web Page].https://www.nau.edu.pt/pt/2021/11/30/boaspraticas-de-ciberseguranca-os-cinco-pontoscriticos/

[7] CGD. (2020 setembro 25). *Como minimizar os efeitos dos ciber-riscos: seguros e medidas.* Lumiun. [Web Page]. https://www.cgd.pt/Site/SaldoPositivo/protecao/Pages/ciber-riscos-segurose-medidas.aspx.

[8] Álvarez, Irene Iglesias (2023). *Investimentos em cibersegurança deverão crescer 13% em 2023. Computerworld.* [Web Page]. https://www.computerworld.com.pt/2023/01/19/investimento-em-ciberseguranca devera-crescer-13-em-2023/

[9] Bruce, G., & Dempsy, R. (1997). *Security in Distributed Computing.* Hewllett Packard Professional Books.

[10] Pplware (2022). *Ciberataques – Portugal é um alvo preferido dos criminosos?* [Web Page]. https://pplware.sapo.pt/informacao/ciberataque s-portugal-e-um-alvo-preferido-doscriminosos/

[11] Forbes Portugal (2020*). Gastos com cibersegurança aumentam cerca de 10% em 2021*. [Web Page] https://www.forbespt.com/gastos-com-ciberseguranca-aumentam-cerca-de-10-em-2021/

[12] Antunes, M., & Rodrigues, B. (2018). *Introdução à Cibersegurança*. FCA

[13] Agência Lusa. (2022*). Ciberataques: cronologia de outros ataques em Portugal além da Vodafone*. CNN Portugal. [Web Page]. https://cnnportugal.iol.pt/mariovaz/ataqueinformatico/vodafone-e-a-maisrecente-vitimaemseis-anos-de-ciberataques/%2020500208/62028bd00cf21847f0a9ddfa