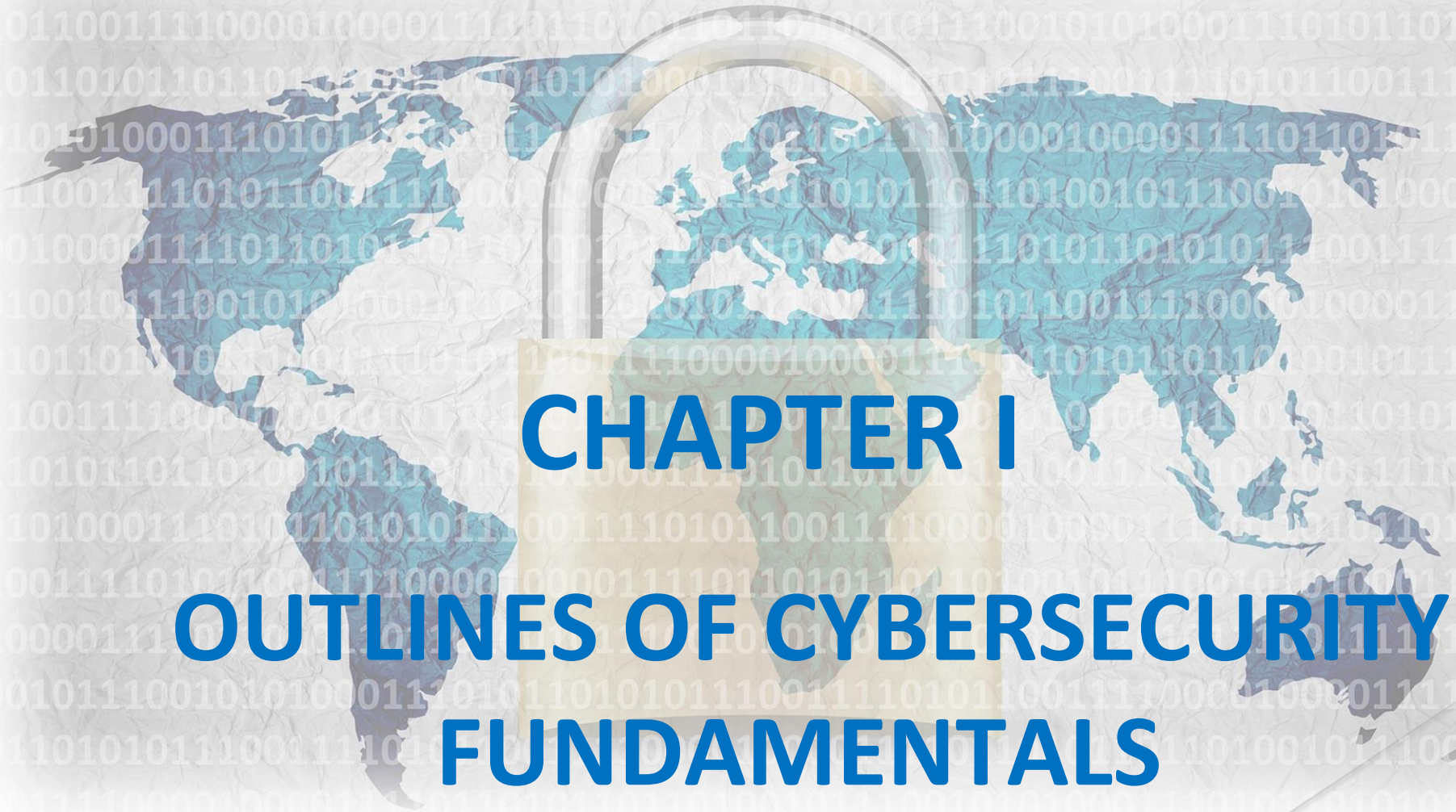
ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union



CHAPTER I

OUTLINES OF CYBERSECURITY FUNDAMENTALS

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

CONTENT

Co-funded by the
Erasmus+ Programme
of the European Union

1) INTRODUCTION TO CYBERSECURITY

Co-funded by the
Erasmus+ Programme
of the European Union

What is cybersecurity?

CYBERSECURITY INVOLVES THE BODY OF TECHNOLOGIES, PROCESSES, AND PRACTICES DESIGNED TO PROTECT NETWORKS, DEVICES, PROGRAMS, AND DATA FROM ATTACK, DAMAGE, OR UNAUTHORIZED ACCESS.

Co-funded by the
Erasmus+ Programme
of the European Union

Definitions from the literature

1. "Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders"[1].

2. "Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption"[2].

3. "Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on"[3].

4. "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets"[4].

1. Kemmerer, R. A. 2003. Cybersecurity. Proceedings of the 25th IEEE International Conference on Software Engineering: 705-715. http://dx.doi.org/10.1109/ICSE.2003.1201257
2. Lewis, J. A. 2006. Cybersecurity and Critical Infrastructure Protection. Washington, DC: Center for Strategic and International Studies. http://csis.org/publication/cybersecurity-and-critical-infrastructure-pr...
3. Amoroso, E. 2006. Cyber Security. New Jersey: Silicon Press.
4. ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). http://www.itu.int/rec/T-REC-X.1205-200804-I/en

5. “The ability to protect or defend the use of cyberspace from cyber-attacks”[5].
6. “The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability”[6].
7. “The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure”[7].
8. “The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this”[8].
9. “The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation”[9].

5. CNSS. 2010. National Information Assurance Glossary. Committee on National Security Systems (CNSS) Instruction No. 4009: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf
6. Public Safety Canada. 2014. Terminology Bulletin 281:Emergency Management Vocabulary. Ottawa: Translation Bureau, Government of Canada. https://publications.gc.ca/collections/collection_2012/tpsgc-pwgsc/S52-2-281-2012.pdf
7. Canongia, C., & Mandarino, R. 2014. Cybersecurity: The New Challenge of the Information Society. In Crisis Management: Concepts, Methodologies, Tools and Applications: 60-80. Hershey, PA: IGI Global. http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003
8. Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014: http://www.oxforddictionaries.com/definition/english/Cybersecurity
9. DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014: https://niccs.us-cert.gov/glossary#letter_c

Co-funded by the
Erasmus+ Programme
of the European Union

How can we define security?

- Computer security, information security, cybersecurity
- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the:
  - **Integrity as the** accuracy and consistency of data stored in a database.
  - **availability**, timeliness and reliability of access to and use of data. It includes data accessibility and continuity of information.
  - **confidentiality** of information system resources (hardware, software, firmware, information/data, telecommunications)[10].
- The security of a system, application, or protocol is always relative to
  - A set of desired properties
  - An adversary with specific capabilities

Refer to slide 23 for further reading

10. Guttman, B. and Roback, E. (1995), An Introduction to Computer Security: the NIST Handbook, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-12r1 (Accessed June 18, 2021)

Co-funded by the
Erasmus+ Programme
of the European Union

Today

- Everything is a computer
- Everything can be connected to the Internet
- Everything can be hacked
- Internet of things' (IoT) security is a public safety issue!
- Digitalization and (embedded) Artificial Intelligence (AI) may make an attractive business case only until one starts thinking about security

A WORLD OF SMART DEVICES MEANS THAT THE INTERNET CAN CONTROL PEOPLE! → WE NEED TO KNOW HOW TO PROTECT OURSELVES

Co-funded by the
Erasmus+ Programme
of the European Union

2) WHY IS CYBERSECURITY IMPORTANT TO *SMES* AND MANAGERS

Co-funded by the
Erasmus+ Programme
of the European Union

Why is cybersecurity important for SMEs?

TODAY EVERYTHING IS ONLINE

- The continuous technological development requires companies to adapt as today's business has moved largely online. Technological renewal is getting faster every day, causing difficulties, especially for SMEs, to protect themselves and protect their business from possible attacks that change and increase daily following the technological trend[13,14].
- Moreover, it would be more profitable for hackers to target firms with large profits but actually small businesses are most at risk with regards to cyber security threats in the present day. With less security architecture and smaller IT teams, small business owners urgently need cyber security solutions that cover the entirety of the threat landscape in the 2020s.

13. https://news.vaimo.com/the-importance-of-cybersecurity-for-small-businesses
14. A. Abdulmajeed, B. Duncan, 2020/06/01, T1 - Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence, conference Paper · June 2020 DOI: 10.1109/CyberSA49311.2020.9139638

Co-funded by the
Erasmus+ Programme
of the European Union

5 Reasons Why Small Companies Need Cyber Security

- Small businesses are moving to the cloud
- Protecting business and the valuable information, preventing spyware (in order to maintain reputation and customer trust)
- Protecting work safety and productivity
- Increasing remote working
- Increasing number of cyber attacks at global level (cyber-criminals are always on the hunt)[15]

15. Ashford, W., 2014. SMEs believes they are immune to cyber attack. Computer Weekly, [online] Available at: https://www.computerweekly.com/news/2240216202/SMEs-believes-it-is-immune-to-cyber-attack-study-shows

Co-funded by the
Erasmus+ Programme
of the European Union

What are the challenges for an organization?

- **NETWORK SECURITY**: you need to protect your network from unwanted users, attacks and intrusions
- **APPLICATION SECURITY**: to ensure security, applications require constant updates and testing
- **ENDPOINT SECURITY**: remote access can be a weak point for data, so you need to develop measures to protect it
- **DATA SECURITY**: actions must be taken to protect company and customer information through separate security measures
- **IDENTITY MANAGEMENT**: control and verification of access by individuals who are members of the organization must be protected
- **DATABASE AND INFRASTRUCTURE SECURITY**: these devices must be protected as well, not only the data
- **CLOUD SECURITY**: files and works stored in digital environments must be protected as well
- **MOBILE SECURITY**: the security of mobile phones and tablets is fundamental
- **DISASTER RECOVERY/BUSINESS CONTINUITY PLANNING**: in the event of a breach, natural disaster or other event it is important to ensure that data are protected and business continues

Co-funded by the
Erasmus+ Programme
of the European Union

ENGINE

How to create a Cyber Security Culture (CSC) in an organization?

Businesses investing heavily in cybersecurity often base their investments on technology, but don't sufficiently attend to the human side of it, which remains the top cybersecurity risk for many organizations.

For this reason, a CSC must be created ad hoc for every organization to match:

- Organization's mission and culture
- Employees' practices and needs

It is crucial to involve employees in developing a CSC in order to guarantee its full adoption[16,17]

16. K. Reegård, C. Blackett, V. Katta, The Concept of Cybersecurity Culture, September 2019, Conference: 29th European Safety and Reliability Conference (ESREL)At: Hannover, DOI:10.3850/978-981-11-2724-3_0761-cd
17. M. Alshaikh, Developing cybersecurity culture to influence employee behavior: A practice perspective, Computers & Security, Volume 98, 2020, 102003, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.102003.

Co-funded by the
Erasmus+ Programme
of the European Union

Steps for CSC creation

1. Create a basic CSC working group[18]
2. Business understanding and risk assessment
3. Define main goals, success criteria and target audiences
4. Calculate the current situation and perform a gap analysis
5. Select one or more activities
6. Run selected activities
7. Rerun current situation metric and analyze the results
8. Review and consider results before deciding on next action

18. A. Georgiadou, S. Mouzakitis, K. Bounas, D. Askounis (2020): A Cyber-Security Culture Framework for Assessing Organization Readiness, Journal of Computer Information Systems.
DOI: 10.1080/08874417.2020.1845583

Co-funded by the
Erasmus+ Programme
of the European Union

Barriers in creating CSC

1) Lack of employee participation[19]
   - Not everyone understands their role in the organization's safety culture
   - Lack of active participation in the change process
   - Insufficient time spent
   - Complexity of the topic
2) Executives do not give due importance
   - Lack of consent and understanding on their part
   - Downplaying of the problem
   - Thinking that bland information is enough (not wanting to invest, even resources, in this)
   - Considering themselves outside the problem

19. https://www.securitymagazine.com/articles/92739-barriers-to-teaching-employees-good-cybersecurity-habits-and-how-to-overcome-them

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

3) BASIC CONCEPTS OF CYBERSECURITY

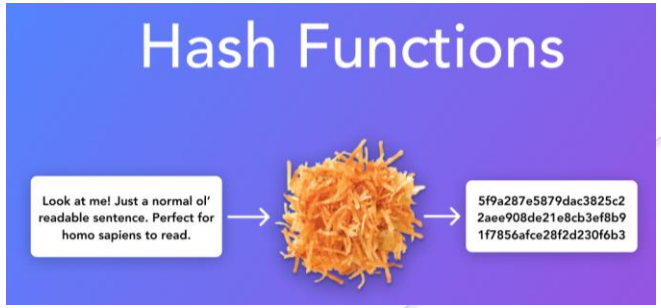
Co-funded by the
Erasmus+ Programme
of the European Union

Basic concepts to get started[20]

FILE: in computer science, it is the main structure used to store data on a specific digital storage medium.
A file can be used to store a wide variety of information, such as a picture, a written message, a video or a song.

WIRELESS: the ability to transfer information or electrical energy between two or more points that are not physically connected by any electrical conductor.
All devices or systems that make use of this mode of communication are also called wireless, while all devices or systems based on wired connections are called wired.

HASH FUNCTIONS: special functions that allow a message to be given a fingerprint that uniquely identifies it.
They create a string associated with the message to be sent and for which, once the function has been applied, it should no longer be possible to revert to the original text.



20. R. Shipsey, Computer security, CO3326 2009, guide prepared for the University of London International Programmes

Co-funded by the
Erasmus+ Programme
of the European Union

ENGINE

ANTIVIRUS: is a software that scans a device or network for security threats. The software warns you if it detects a threat and neutralizes (or blocks) malicious codes.

AUTHENTICATOR: authentication is the way in which a person proves his/her identity, it can take place using different methods such as a password, a fingerprint, a face scan etc.

BLACKLIST: as the term suggests, it is a list of emails or other service providers that spread spam messages. These lists help users prevent the flow of unwanted messages.

BACKUP: is the copy of physical or virtual data. Making backups is important in order to guarantee the recovery and security of the data so that, in the event that they might get deleted or lost, the user can easily recover them.

CLOUD: is a non-physical storage space. It is a vast network of remote servers located around the world, connected together and operating as a single ecosystem. The cloud allows you to access files and services from anywhere in the world as long as you have an internet connection.

Co-funded by the
Erasmus+ Programme
of the European Union

CRYPTOGRAPHY is a method that is used to protect sensitive and confidential information and communications using algorithms that create codes which make messages obfuscated and unrecognizable. In this way, only those to whom the information is intended can read and process it. These two phases are called encryption and decryption.

ENCRYPTION is a process that, thanks to the use of key algorithms, transforms the original information into an unrecognizable form. This way the message is completely different from the original message.

DECRYPTION converts the encrypted data back into a form that can be read and understood by a human or computer.

Co-funded by the
Erasmus+ Programme
of the European Union

Digital signature

A **digital signature** is a technique used to validate the authenticity and integrity of a digital message, software or document[21].

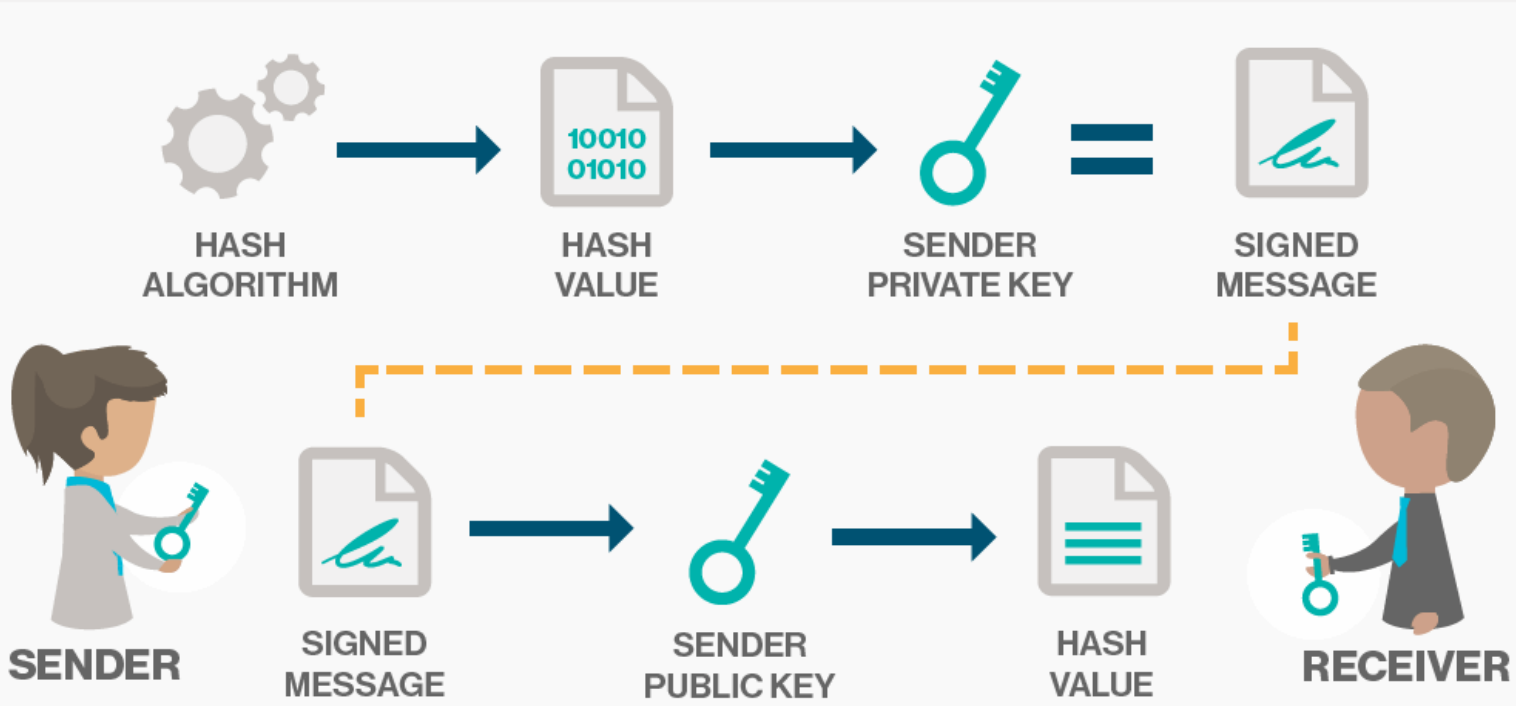
It is the digital equivalent of a handwritten signature or a stamped seal, with the aim of solving the problem of tampering and impersonation in digital communications.

Digital signatures **provide proof** of origin, identity and status of electronic documents, transactions or digital messages.

It guarantees the authenticity of documents in a unique way that achieves **non-repudiation** → the property of authentic statements made by a person or system cannot be denied

Co-funded by the
Erasmus+ Programme
of the European Union

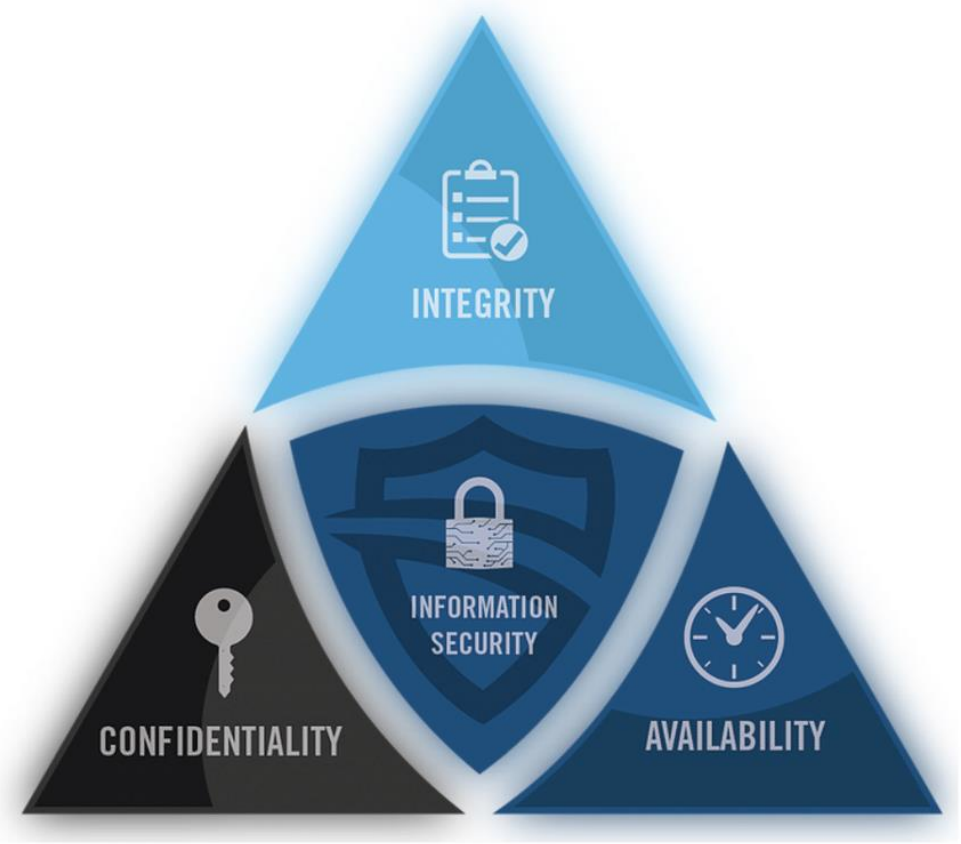
DEFINITION
DIGITAL SIGNATURE



21. Que signifie Signature numérique (signature digitale)? - Definition IT de Whatis.fr (lemagit.fr)

Co-funded by the
Erasmus+ Programme
of the European Union

The CIA Triad



The Cyber Security as a whole is a very broad term which is based on three fundamental concepts known as "**The CIA Triad**"[23,24].

It consists of **Confidentiality, Integrity and Availability**. This model is designed to guide the organization with the policies of Cyber Security within the realm of Information security.

23. https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html
24. D. Popescul, Daniela, The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation, 2011/06/29, Article SP 978, VL - 4

Co-funded by the
Erasmus+ Programme
of the European Union

Confidentiality

Confidentiality defines the rules that limits the access of information in order to avoid the unauthorized disclosure of information.

The term covers two related concepts:

- **Data confidentiality**: assures that private or confidential information is not made available or disclosed to unauthorized individuals
- **Privacy:** assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

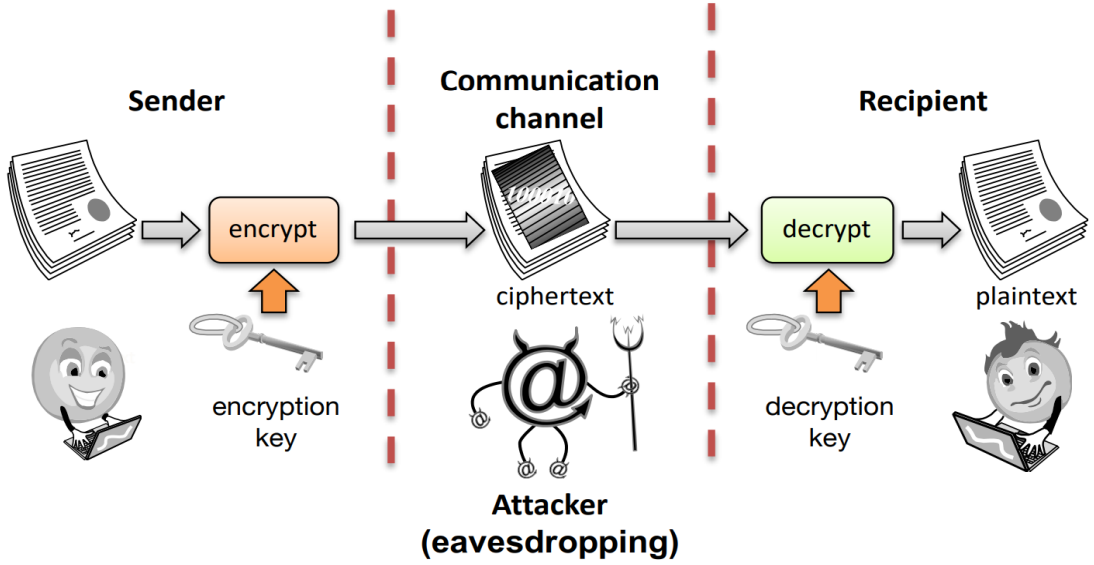
There are various ways to ensure confidentiality, like:

- Physical access restrictions
- Computer theft precautions (alarms etc.)
- Access control in the computer systems
- Encryption in communication and storage
- Bug-free programs

Co-funded by the
Erasmus+ Programme
of the European Union

Tools for Confidentiality:
1) Encryption

Encryption is the method by which information is converted into a secret code, encryption key, that hides the information's true meaning, so that the transformed information can only be read using another secret, called the decryption key (in some cases, it's the same as the encryption key). The science of encrypting and decrypting information is called cryptography.



Co-funded by the
Erasmus+ Programme
of the European Union

2) Access Control

Access Control is the set of rules and policies that limit access to confidential information to those people and/or systems with a “need to know”.

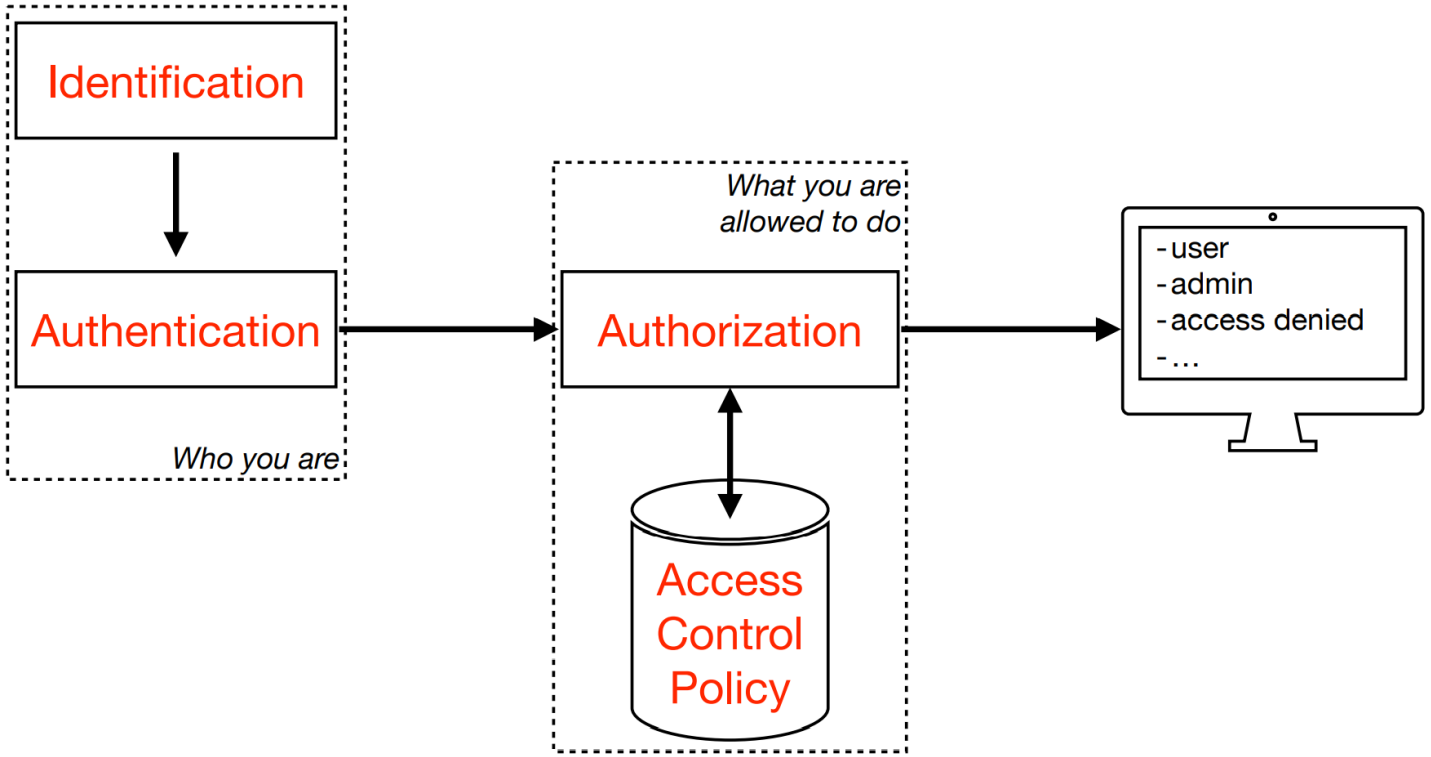
This “need to know” may be determined by

- **identity**, such as a person’s name or a computer’s serial number
- **a role** that a person has, such as being a manager or a computer security specialist

Co-funded by the
Erasmus+ Programme
of the European Union

3) Authorization

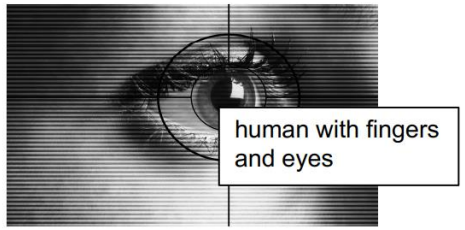
Authorization is the way to determine if a person or system is allowed access to resources, based on an access control policy.



Co-funded by the
Erasmus+ Programme
of the European Union

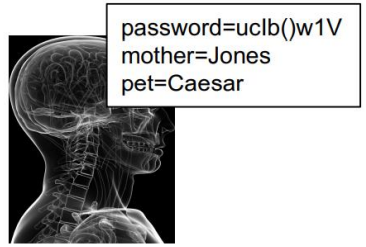
4) Authentication

Authentication is the determination of the identity that someone has. It can be conducted in several different ways, but it is usually based on a combination of:



Something you are

- **Something the person has** (like a smart card or a radio key fob storing secret keys)



Something you know

- **Something the person knows** (like a password)

Something you have

- **Something the person is** (like a human with a fingerprint)

Co-funded by the
Erasmus+ Programme
of the European Union

5) Physical Security

Physical security establishes physical barriers to limit access in order to protected computational resources.

- Barriers may include
  - Locks on cabinets and doors
  - The placement of computers in windowless rooms
  - The use of sound dampening materials
  - The construction of buildings or rooms with walls incorporating copper meshes (called Faraday cages) so that electromagnetic signals cannot enter or exit the enclosure

Co-funded by the
Erasmus+ Programme
of the European Union

6) Steganography

Steganography is the practice of concealing a message within another message or a physical object (a computer file, message, image, or video is concealed within another file, message, image, or video)

- We can have several types:
  - Text steganography
  - Audio steganography
  - Video steganography
  - Protocol steganography
- Example of text steganography:

Since **E**veryone **C**an **R**ead, **E**ncoding **T**ext **I**n **N**eutral **S**entences **I**s **D**oubtfully **E**ffective ———> **SECRET INSIDE**

Co-funded by the
Erasmus+ Programme
of the European Union

Integrity

Integrity assures that the data is consistent, accurate and trustworthy over its time period. It means that the data should not be changed, altered, deleted or illegally being accessed within the transit.

- We want to prevent that unauthorized people write or change data
  - A good example of how difficult this can be is the “Chinese whispers” or telephone game

To cope with data loss or accidental deletion or even cyber attacks, regular backups should be there. Cloud backups are now the most trusted solution for this.

Co-funded by the
Erasmus+ Programme
of the European Union

Tools for Integrity:

1) Backups are the periodic archiving of data. They are used to restore data if unauthorized changes are noticed.

2) Checksums are the computation of a (hash) function that maps the contents of a file to a numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.

3) Data correcting codes are the methods for storing data in such a way that small changes can be easily detected and automatically corrected.

Co-funded by the Erasmus+ Programme of the European Union

Availability

Availability is the feature that information and systems are accessible and usable in a certain time frame by those authorized to do so.

If all necessary components like hardwares, softwares, networks, devices and security equipment are maintained and upgraded, then this will ensure the smooth functioning and access of Data without any disruption.

Utilities like firewalls, disaster recovery plans, proxy servers and a proper backup solution should ensure to cope with Denial-of-Service (DoS) attacks[25].

- Protection against physical and/or cyber attacks:
  - Uninterruptable power supplies
  - Fire precautions
  - Flooding precautions
  - Temperature and humidity control
  - Storm resistant buildings
  - Distributed Denial of Service (DDoS)

25. P. Jasheeda, T.K.P.Rajagopal, R.Subathra, Multivariate Correlation Analysis based detection of DOS with Tracebacking, International Journal On Engineering Technology and Sciences – IJETS™ ISSN (P): 2349-3968, ISSN (O): 2349-3976 Volume 2 Issue 4, April -2015

Co-funded by the
Erasmus+ Programme
of the European Union

Tools for Availability:

1) Physical protections, infrastructure meant to keep information available even in the event of physical challenges

2) Countermeasures against system overload

- Redundancy in server farms, or disks
- Equipment that can detect and counter DOS attacks (i.e., AntibIoTic)

3) Countermeasures against system crashing

- Check all user input for “out of bounds” values
- Switch of unused services and functions
- Follow and install supplier updates and patches

Co-funded by the Erasmus+ Programme of the European Union

A.A.A. concept

AAA in networking terminology is an abbreviation for[22]

ASSURANCE

How **trust** is provided and managed in computer systems. Trust is difficult to quantify, but trust, and management of trust, is essential.

AUTHENTICITY

Ability to determine that statements, policies, and permissions issued by people or systems are **genuine/authentic**. Can be seen as authentication + integrity

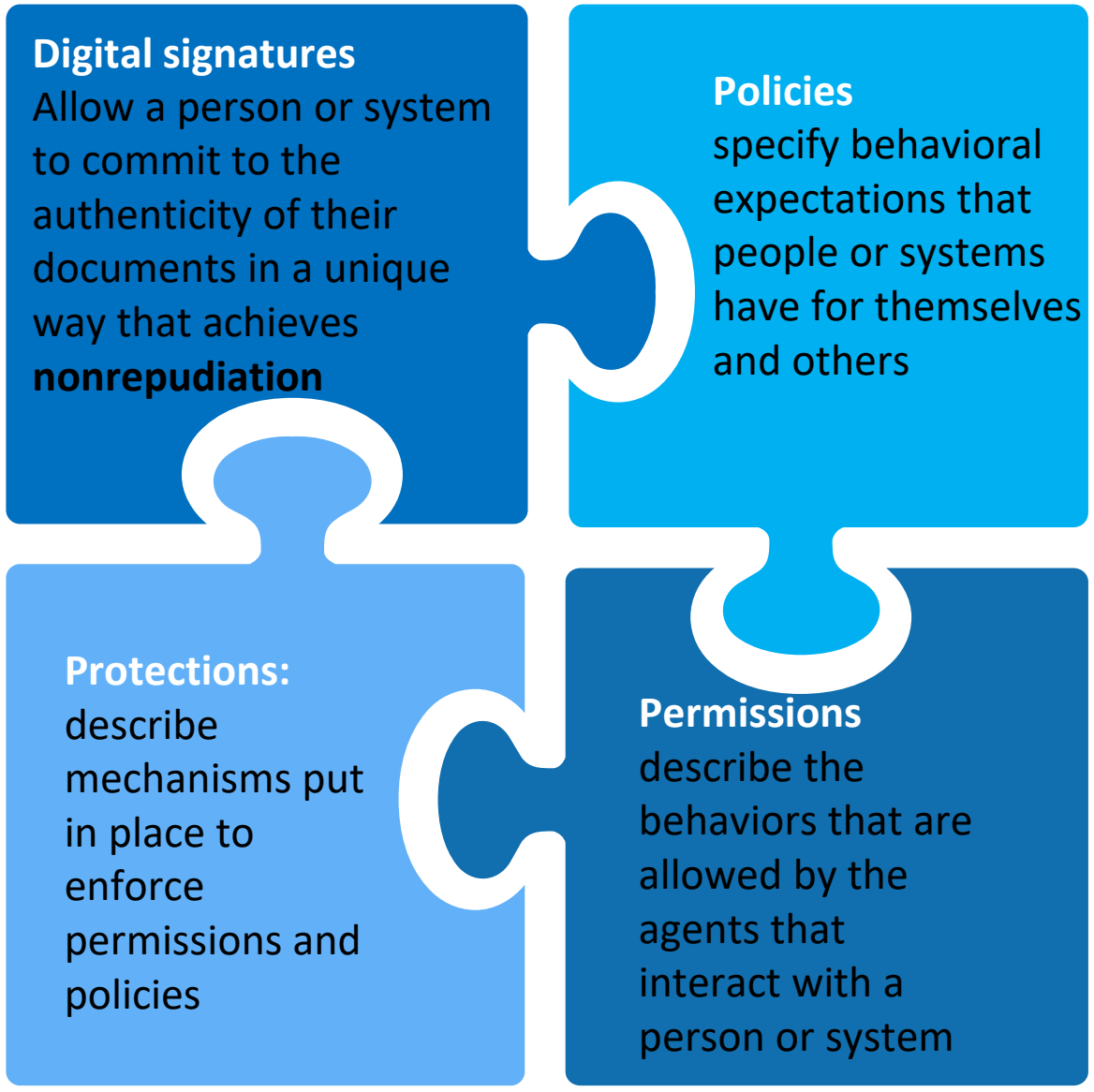
ANONYMITY

The feature of certain records or transactions **not to be attributable** to any individual

22. https://www.geeksforgeeks.org/what-is-aaa-authentication-authorization-and-accounting/

Co-funded by the Erasmus+ Programme of the European Union

Assurance



Co-funded by the
Erasmus+ Programme
of the European Union

Anonymity

TOOLS

Proxies: trusted agents (example: The Onion Router) that engage in actions for an individual in a way that cannot be traced back to that person

Pseudonyms: fictional identities that can fill in for real identities in communications and transactions, otherwise known only by a trusted entity

Aggregation: the combining of data from many individuals so that disclosed sums or averages cannot be tied to any individual

Mixing: the intertwining of transactions, information, or communications in a way that cannot be traced to any individual

Co-funded by the
Erasmus+ Programme
of the European Union

Asset

An asset is defined as any data, device or component of the environment that supports information-related activities[26].

- Assets include:
  - **hardware**
  - **software**
  - **confidential data**

It is important to protect assets against unlawful access, use, disclosure, alteration, destruction and/or theft.

26. https://www.vigilantsoftware.co.uk/blog/risk-terminology-understanding-assets-threats-and-vulnerabilities

Co-funded by the
Erasmus+ Programme
of the European Union

Vulnerability

This is a weakness which can be exploited unintentionally or intentionally to create damage.

It is essential to prevent the hazard with special tools to detect and assess severity, e.g., with vulnerability scanners.

Some examples of vulnerability:

- Admin accounts with default passwords
- Programs with known flaws
- Programs with unnecessary privileges
- Weak access control settings
- Weak firewall configurations

Co-funded by the
Erasmus+ Programme
of the European Union

Threat

A threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to an asset[27].

It can be:

- Intentional: wilfully caused by a human (for example hacking)
- Unintentional: like computer malfunctioning or natural disaster

A threat can be categorised in different ways, for instance by the impact.

Microsoft's **STRIDE** threat model[28]:

- **S**poofing identities
- **T**ampering with data
- **R**epudiation
- **I**nformation disclosure (privacy breach or data leak)
- **D**enial of service (DoS)
- **E**levation of privilege

27. https://csrc.nist.gov/glossary/term/cyber_threat
28. https://www.microsoft.com/security/blog/2007/09/11/stride-chart/

Co-funded by the
Erasmus+ Programme
of the European Union

Stride Threat Model[28]

Spoofing identity

- Illegally accessing and then using another user's authentication information

Tampering with data

- Malicious modification
- Unauthorized changes

Repudiation

- Deny performing an malicious action
- Non-repudiation refers to the ability of a system to counter repudiation threats

Elevation of privilege

- Unprivileged user gains privileged access to compromise the system
- Effectively penetrated and become part of the trusted system

Denial of service

- Deny service to valid users
- Threats to system availability and reliability

Information disclosure

- Exposure of information to individuals not supposed to access

29. Threat Modeling – Avotis

Co-funded by the
Erasmus+ Programme
of the European Union

What are the most serious cybersecurity threats?

1. **MALWARE**: malicious software designed to gain access to a device or to damage it without the owner knowing
2. **WEB-BASED ATTACKS**: various techniques used to redirect web browsers to malicious websites or vulnerable servers and mobile apps where further malware infections may take place to gain confidential data
3. **PHISHING**: the fraudulent attempt to steal user data such as login credentials or credit card information
4. **SPAM**: sending unsolicited messages in bulk

1. Malware

The term **malware** is a contraction of "**malicious software**". It is one of the most common cyber threats and it is intended to damage or cause malfunctioning of a legitimate user's computer. It is often spread via unsolicited e-mail attachments or seemingly legitimate downloads[30,31,32].

There are numerous types of malware:

- **Virus:** A self-replicating program that attaches itself to a file and spreads throughout the computer system, infecting files with its malicious code.
- **Trojan:** This is a type of malware disguised as legitimate software. Cyber criminals trick users into loading Trojans onto their computers, where they can cause damage or collect data.
- **Spyware:** is a program that secretly records the user's actions, allowing cyber criminals to exploit this information to their advantage. For example, it can capture credit card data.
- **Ransomware:** Malware that blocks access to the user's files and data, threatening to delete them if the user does not pay a ransom.
- **Adware:** advertising software that can be used to spread malware.
- **Botnet:** networks of computers infected with malware, used by cyber criminals to perform online tasks without the user's permission.

30. https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html
31. https://www.infosecurity-magazine.com/malware/
32. https://www.forcepoint.com/cyber-edu/malware

Co-funded by the
Erasmus+ Programme
of the European Union

2. Web-based attack

Web-based attacks are an attractive method by which threat actors can deceive victims by using web systems and services as a threat vector[33].
Web-based attacks can affect the availability of websites, applications and application programming interfaces (APIs), violating confidentiality and data integrity.

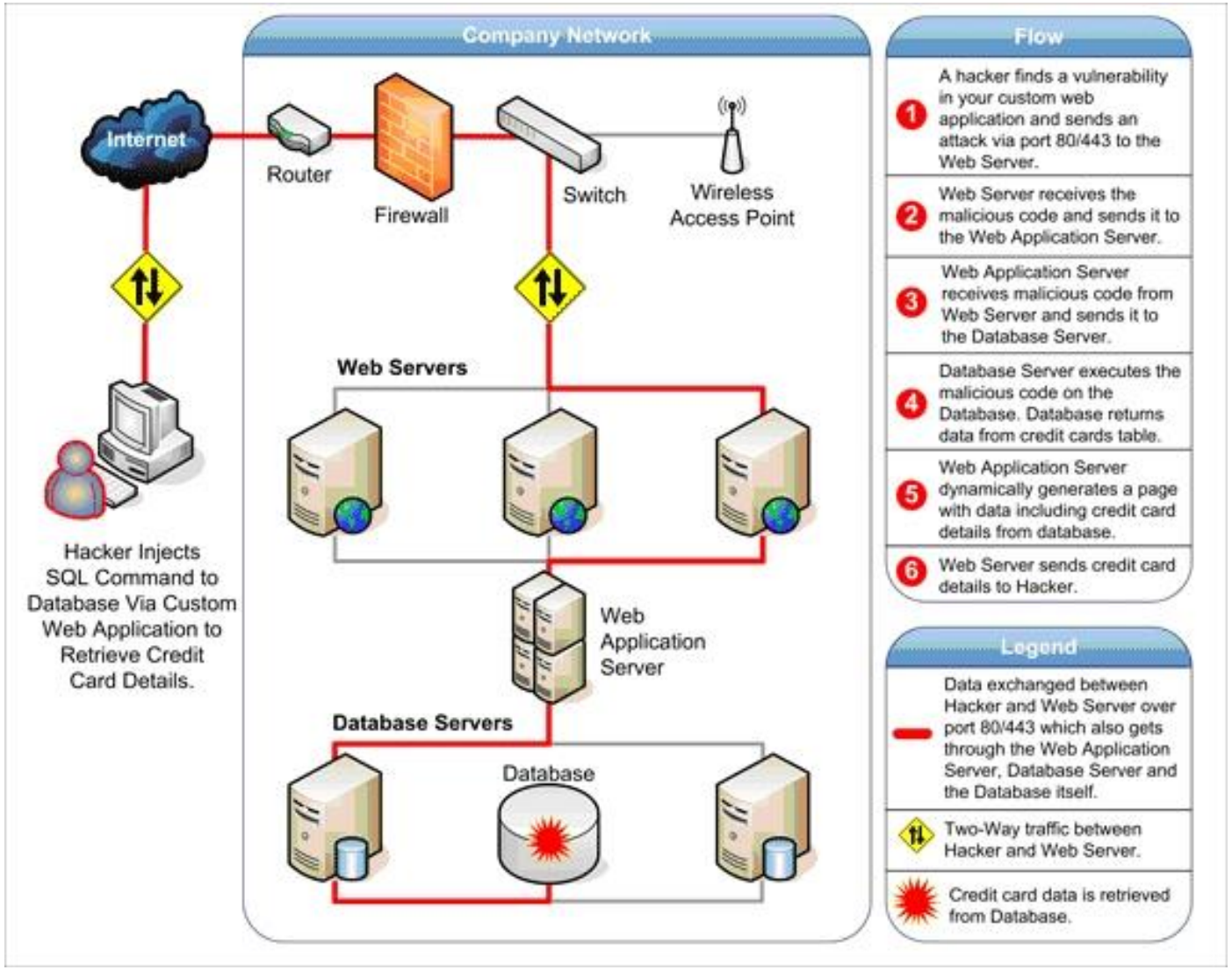
This covers a wide attack surface, for example:

- facilitating malicious URLs or malicious scripts to direct the user or victim to the desired website or download malicious content (watering hole attacks1, drive-by2 attacks)
- injecting malicious code into a legitimate but compromised website to steal information (i.e., formjacking) for financial gain
- stealing information or even extortion through ransomware

33. J. Crist, Web Based Attacks , SANS Institute Information Security Reading Room https://www.sans.org/reading-room/whitepapers/application/web-based-attacks-2053
34. ENISA Threat Landscape 2020 - Web-based attacks https://www.enisa.europa.eu/publications/web-based-attacks

Example of Web-based attack scheme

Co-funded by the Erasmus+ Programme of the European Union



36. Web Application Attack: What Is It and How to Defend Against It? (acunetix.com)

Co-funded by the
Erasmus+ Programme
of the European Union

3. Phishing

Phishing attacks involve a combination of social engineering and deception to persuade potential victims to divulge sensitive information such as credentials or bank and credit card details. The attack usually takes place via SPAM mail, malicious websites, emails or instant messages, which appear to come from a legitimate source such as a bank or social network. Attackers often use scare tactics or urgent requests to entice recipients to respond[35].
Such fraudulent messages are usually not personalised and may share similar generic properties.

There is also a more sophisticated version: **spear phishing**.
In this case the attacks are personalised and tactics such as impersonating the sender are used. Public information found on social media sites such as LinkedIn or Facebook is used to personalise their message or impersonate users so that the spear phishing email is likely enough for users to react to it.

35. https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks

Co-funded by the
Erasmus+ Programme
of the European Union

4. Spam

The term **spam** refers to unsolicited mass messages sent via e-mail, instant messaging or other digital communication tools. It is generally used by advertisers because there are no operational costs beyond those of managing their mailing lists.
However, spam can also be used to collect sensitive information from users and to spread viruses and other malware.

Spam vs Phishing[37,38]

Spam:

- Is a tactic to send unsolicited bulk e-mails to a list of recipients
- Can link the user to a compromised website for installation of malware and theft of personal data

Phishing:

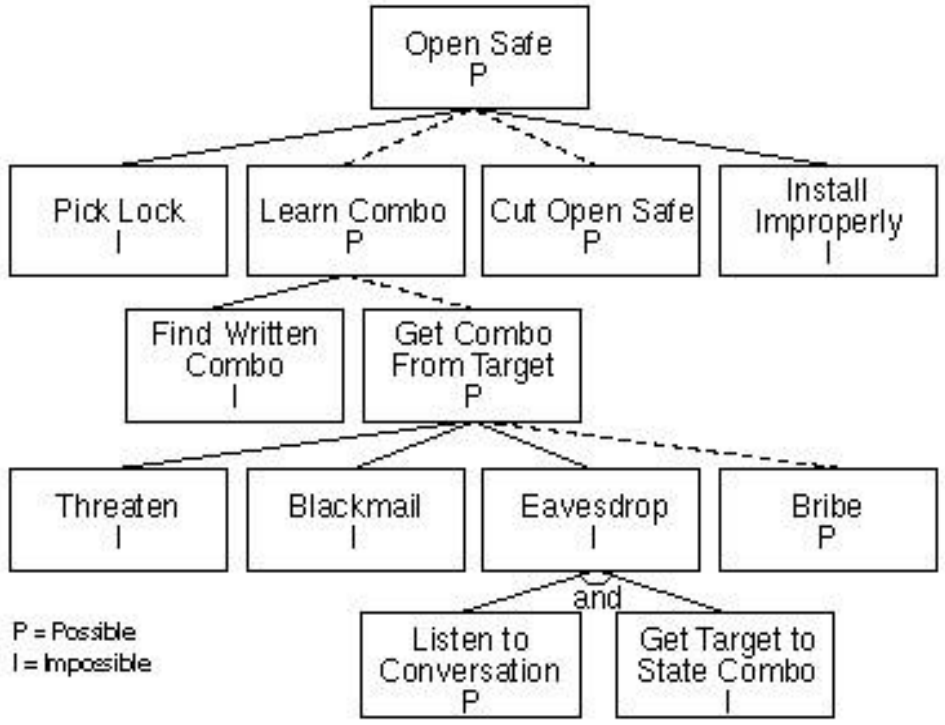
- Uses social engineering tactis and aims to steal user data
- Can use spam tactics to dustribute messages

37. https://www.webroot.com/us/en/resources/tips-articles/spam-vs-phishing
38. https://staysafeonline.org/stay-safe-online/identity-theft-fraud-cybercrime/spam-and-phishing/

Co-funded by the
Erasmus+ Programme
of the European Union

Attack

- Several steps are needed to carry out an attack
- There may be several attacks carrying out a given threat
- Often, an attack tree is built[39]



39. https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Co-funded by the
Erasmus+ Programme
of the European Union

Examples of Attacks[40]

1. **EAVESDROPPING:** the interception of information intended for someone else during its transmission over a communication channel. Threat to confidentiality
2. **MAN-IN-THE-MIDDLE:** occur when a network stream is intercepted, modified, and retransmitted. Threat to confidentiality and integrity
3. **DENIAL-OF-SERVICE (DoS):** is the interruption or degradation of a data service or information access. Threat to availability
4. **MASQUERADING:** is the fabrication of information that is purported to be from someone who is not actually the author. Threat to authentication
5. **REPUDIATION:** is the denial of a commitment or data receipt. It happens when an application or system does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions. Threat to authentication, integrity, availability, access controls, … (depends on the malicious action)
6. **CORRELATION AND TRACEBACK:** the integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information. Threat to authentication

40. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

4) SECURING WEB APPLICATION AND SERVICES

Co-funded by the
Erasmus+ Programme
of the European Union

Web applications, services, and server overview

Web applications, services, and servers, tightly connected and sometimes overlapping, represent a key part of organizational IT infrastructures. However, challenges and issues related to security still exist and must be addressed. Current web applications, services, and server security standards are not sufficient in providing the necessary protection for robust, secure, and reliable platforms.

To tackle this lack of security, implementation of risk management and more advanced security measures are needed. Therefore, fields such security engineering, secure software development, and risk management are gaining importance[41].

41. G. Beuchelt, Chapter 10 - Securing Web Applications, Services, and Servers, Editor J.R. Vacca, Computer and Information Security Handbook (Third Edition), ISBN 9780128038437.
https://www.elsevier.com/books/computer-and-information-security-handbook/vacca/978-0-12-803843-7

Co-funded by the Erasmus+ Programme of the European Union

Definition of web servers

For the latter, (i) a user sends a request for a specific web site via a web browser (e.g., Chrome, Firefox) indicating the Uniform Resource Locator (URL), (ii) the browser sends a request to the Internet for viewing the corresponding web page, (iii) a Domain Name Server (DNS) converts this URL to an Internet Protocol (IP) address (unique code for every website) [42] .

In short, a web server is a combination of hardware and software that stores, processes and delivers web pages to the users upon request[43,44]. In fact, most of the web-based applications use Apache as their standard Web Server environment. Among the different web servers available, Apache, an open-source server, is the most used nowadays, dealing with almost 70% of the websites available today.

Web servers can be dived in INTRANET SERVER, in case of private internal use or INTERNET, if their access is public. At this point, the Web Server shows the chosen website to the user's browser. The requested web pages contain mostly static objects such as HTML documents, images, style sheets[45].

42. https://economictimes.indiatimes.com/definition/web-server
43. https://www.techopedia.com/definition/4928/web-server
44. https://www.copahost.com/blog/ftp-meaning/
45. https://www.webopedia.com/definitions/web-server/

A Web Server is so crucial that without it the whole internet would possibly not exist as we know it.

A Web Server is a combination of both Hardware and Software

- **Hardware** represents any physical part of a computer. In particular, the hardware of a Web Server is made of specific and high-quality computer parts, optimized to run as server. Although we find similar components as a regular computer (HD, motherboard, processors, RAM memory and others), these elements need to support high stress and load. In particular, the Web Servers run 24 hours a day, every day and therefore need a specific and high-performance refrigeration systems to avoid over heating. Connection to the network must always be guaranteed and needs to be of high quality. These devices store all the content of the websites or applications, in addition to the programs responsible for the communication between client and server. A Web Server has a high maintenance cost to ensure a smooth operation which should be operated by trained personnel. For all these reasons, it is more convenient to outsource the serves to Hosting Companies, which are specialized in this field.
- **Software** represents all the programs that perform communication tasks between the server-side and the client-side. This is important in HTTP communication as well as in File Transfer Protocol (FTP), e-mails servers, etc. A computer can host multiple and/or different types of web servers[46].

46. https://www.copahost.com/blog/what-is-web-server/

Co-funded by the
Erasmus+ Programme
of the European Union

Web services

Web services are described as a system of software allowing different machines to interact with each other through network, according to W3C (World Wide Web Consortium). Web services succeed in this goal by using different open standards:

XML or Extensible Markup Language is used to share data on the web in universal format.

SOAP or Simple Object Access Protocol is an application communication protocol that sends and receives messages through XML format. It is considered the most effective way to communicate between applications over HTTP, supported by all browsers and servers.

WSDL or Web Services Description Language is used to describe web service. WSDL includes three units namely Definitions, Operations and Service bindings.

UDDI or Universal Description, Discovery, and Integration describes a set of services supporting the depiction and discovery of businesses, organizations, and other Web Services providers. It uses a common set of industry standards (e.g. HTTP, XML, XML Schema, and SOAP)[47].

47. https://www.carmatec.com/blog/web-services-vs-web-applications/

Co-funded by the
Erasmus+ Programme
of the European Union

The differences between a web server and a web service

To bring clarity over web service and web server, below the main differences between these two concepts are reported:

Web Servers

- Are a piece of software that run on a physical or virtual machine, which designed to serve web pages/web sites/web services.
- Transport channel used by web server necessarily need to be HTTP protocol.
- Accept HTTP requests and respond by giving HTTP responses.

Web Services

- Constitute a standardized way of integrating Web-based applications using XML, SOAP, WSDL and UDDI open standards over an Internet backbone
- As mentioned, they can use any data format
- Transport channels used by web services don’t necessarily need to be the HTTP protocol.
- There are mainly two types of web services within Microsoft: WCF and ASMX. WCF services are "hosted" by IIS, whereas ASMX web services run within IIS.

Co-funded by the
Erasmus+ Programme
of the European Union

Web Application

Traditional applications are stored and run locally via the operating system (OS). On the other hand, any application that a user accesses via internet (e.g., client browser) is referred to as web application. Examples of commonly-used web applications include:

- web-mail, online retail sales, online banking, and online auctions.

In the context of Web Applications, it is important to define what a client is. A 'client' is a piece of computer hardware or software that accesses a service made available by a server as part of the client–server model of computer networks[48].

48. Microsoft Official Academic, Course (8 July 2008). *Exam 70-643 Windows Server 2008 Applications Infrastructure Configuration*. John Wiley & Sons. ISBN 978-0-470-22513-4

Co-funded by the
Erasmus+ Programme
of the European Union

The differences between a web services and a web application

To clarify the difference between web applications and web services, a comparison is reported below:

- **Web Services** can be used to transfer data between Web Applications.
- **Web Services** are accessible from different platforms such as web servers.
- **Web Application** can be accessed through browsers
- **A Web Application** is designed for human interaction, while a Web Service is meant for computers.
- **Web Application** has a Graphical User Interface (GUI) while web services do not[47,50].

47. https://www.carmatec.com/blog/web-services-vs-web-applications/
49. https://www.quora.com/What-is-the-difference-between-web-service-and-web-application

Co-funded by the
Erasmus+ Programme
of the European Union

Security actions for Web Services, Servers and Applications

1. Replicate Data and Services to Improve Availability
2. Use Logging of Transactions to Improve Nonrepudiation and Accountability
3. Use Threat Modeling and Secure Software Design Techniques to Protect from Attacks.
4. Use Performance Analysis and Simulation Techniques for End-to-End Quality of Service (QoS) and Quality of Protection.
5. Digitally Sign UDDI Entries to Verify the Author of Registered Entries.
6. Enhance Existing Security Mechanisms and Infrastructure[41].

41. G. Beuchelt, Chapter 10 - Securing Web Applications, Services, and Servers, Editor J.R. Vacca, Computer and Information Security Handbook (Third Edition), ISBN 9780128038437.
https://www.elsevier.com/books/computer-and-information-security-handbook/vacca/978-0-12-803843-7

Co-funded by the
Erasmus+ Programme
of the European Union

An Agenda for Action for Security Actions That Web Applications, Services, and Servers Need to Consider

The items in this section are possible actions that organizations should consider; some of the items may not apply to all organizations. In particular, it is necessary to balance these actions against budget requirements and the potential risks an organization's Web applications, services, and servers may face (check all tasks completed):

_____1. **Replicate Data and Services to Improve Availability**. Since web applications, services, and servers are susceptible to denial-of-service (DoS) attacks, it is important to replicate data and applications in a robust manner. Replication and redundancy can ensure access to critical data in the event of a fault. It will also enable the system to react in a coordinated way to deal with disruptions.

_____2. **Use Logging of Transactions to Improve Nonrepudiation and Accountability**. Nonrepudiation and accountability require logging mechanisms involved in the entire Web applications, services, and server transaction. In particular, the level of logging provided by various UDDI registries, identity providers, and individual web services varies greatly. Where the provided information is not sufficient to maintain accountability and nonrepudiation, it may be necessary to introduce additional software or services into the SOA to support these security requirements.

_____3. **Use Threat Modeling and Secure Software Design Techniques to Protect from Attacks**. The objective of secure software design techniques is to ensure that the design and implementation of web applications, services, and server software does not contain defects that can be exploited. Threat modeling and risk analysis techniques should be used to protect the web services application from attacks. Used effectively, threat modeling can find security strengths and weaknesses, discover vulnerabilities, and provide feedback into the security life cycle of the application. Software security testing should include security-oriented code reviews and penetration testing. By using threat modeling and secure software design techniques, web applications, services, and servers can be implemented to withstand a variety of attacks.

_____4. **Use Performance Analysis and Simulation Techniques for End-to-End Quality of Service (QoS) and Quality of Protection**. Queuing networks and simulation techniques have long played critical roles in designing, developing, and managing complex information systems. Similar techniques can be used for quality assured and highly available web applications, services, and servers. In addition to QoS of a single service, end-to-end QoS is critical for most composite services. For example, enterprise systems with several business partners must complete business processes in a timely manner to meet real-time market conditions. The dynamic and compositional nature of web applications, services, and servers makes end-to-end QoS management a major challenge for service-oriented distributed systems.

_____5. **Digitally Sign UDDI Entries to Verify the Author of Registered Entries**. UDDI registries openly provide details about the purpose of a web service as well as how to access it. Web applications, services, and servers use UDDI registries to discover and dynamically bind to web applications, services, and servers at run time. Should an attacker compromise a UDDI entry, it would be possible for requesters to bind to a malicious provider. Therefore, it is important to digitally sign UDDI entries so as to verify the publisher of these entries.

_____6. **Enhance Existing Security Mechanisms and Infrastructure**. Web applications, services, and servers rely on many existing Internet protocols and often coexist with other network applications on an organization's network. As such, many web applications, services, and server security standards, tools, and techniques require that traditional security mechanisms, such as firewalls, intrusion detection systems (IDS), and secured operating systems, are in effect before implementation or deployment of web services applications.

41. G. Beuchelt, Chapter 10 - Securing Web Applications, Services, and Servers, Editor J.R. Vacca, Computer and Information Security Handbook (Third Edition), ISBN 9780128038437.
https://www.elsevier.com/books/computer-and-information-security-handbook/vacca/978-0-12-803843-7

Co-funded by the
Erasmus+ Programme
of the European Union

5) CYBERSECURITY COMMON TAXONOMY

Co-funded by the
Erasmus+ Programme
of the European Union

The EU strategy for cybersecurity

Launched in December 2020, the EU strategy for Cybersecurity aims at improving Europe's resilience against cyber attacks and to ensure that all European citizens and organizations can have a trustworthy and reliable services and digital tools.

The Cybersecurity Strategy allows Europe **to become a leader in international regulations and standards** concerning cyberspace. The Strategy improves the cooperation between partners to promote a global, open, stable and secure cyberspace, founded on the rule of law, human rights, fundamental freedoms and democratic values[50].

The EU Strategy for Cybersecurity aims to:

- ❑ Enhance cyber resilience
- ❑ Fight cybercrime
- ❑ Boost cyber diplomacy
- ❑ Reinforce cyber defense
- ❑ Boost research and innovation
- ❑ Protect critical infrastructure

50. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

Co-funded by the
Erasmus+ Programme
of the European Union

The EU Cybersecurity Strategy - Background

- Cybersecurity is one of **the Commission's priorities** for a digital Europe.
- The EU Cybersecurity strategy is a part of the Shaping Europe's digital future[51] and the EU security union strategy[53].
- The NIS Directive[53] (Directive on security of network and information systems) was the first EU law about cybersecurity. The Directive is now under reviewing process;
- The EU Cybersecurity act[54] is a European legal framework that has been providing, since 2019, cybersecurity certification of products, services and processes and reinforcing the mandate of the EU Agency for Cybersecurity (ENISA).
- The EU 5G toolbox[55], adopted in 2020, created a comprehensive risk-based approach on 5G and Cybersecurity;
- The Digital Europe[56] program is the European funding program that support cybersecurity research and innovation ,cyber defense, and the cybersecurity industry in general.

51. Shaping Europe's digital future | European Commission (europa.eu)
52. European Security Union | European Commission (europa.eu)
53. EUR-Lex - 32016L1148 - EN - EUR-Lex (europa.eu)
54. Cybersecurity Act | Shaping Europe's digital future (europa.eu)
55. Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures | Shaping Europe's digital future (europa.eu)
56. Digital Programme | Shaping Europe's digital future (europa.eu)

Co-funded by the
Erasmus+ Programme
of the European Union

The NIS Directive

The NIS Directive (*Directive on security of network and information systems*) provide measures to **improve the general level of cybersecurity in Europe**.

The legal measures contained in the NIS Directive aims at ensuring:

- Member States' preparedness. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority.
- Cooperation among the Member States, creating a Cooperation Group to facilitate cooperation and the exchange of information among Member States.
- A culture of security across sectors such as energy, transport, banking, financial market infrastructures and digital infrastructure[57].

57. NIS Directive | Shaping Europe's digital future (europa.eu)

Co-funded by the
Erasmus+ Programme
of the European Union

The NIS Directive toolkit

The European Commission adopted a communication[57] to **support Member States in implementing the NIS Directive**. This was necessary for the very fast evolving of the Cybersecurity landscape.

The toolkit provides **practical information** to Member States on the implementation of the Directive, presenting best practices on implementing the Directive, explaining and interpreting specific provisions to clarify how the NIS Directive should work in practice[58].

57. NIS Directive | Shaping Europe's digital future (europa.eu)
58. EUR-Lex - 52017DC0476 - EN - EUR-Lex (europa.eu)

Co-funded by the
Erasmus+ Programme
of the European Union

Review of the NIS Directive

- ✓ The NIS Directive, under the art. 23, requires the **European Commission to review** the functioning of the Directive periodically.
- ✓ The Commission announced in its 2020 work program that it would **conduct the review of the Directive by the end of 2020**. With this scope the European Commission opened a consultation on 7th of July 2020, which was closed on the 2nd of October 2020.
- ✓ As a result of this process, the **new legislative proposal** was presented on the **16th December 2020**

Co-funded by the
Erasmus+ Programme
of the European Union

The new NIS proposal

The new NIS Directive proposal:

- Expands the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap.
- Eliminates the distinction between operators of essential services and digital service providers.
- Strengthens security requirements for the companies, by imposing a risk management approach providing a minimum list of basic security elements that must be applied.
- Addresses the security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in supply chains and supplier relationships.
- Introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonizing sanctions regimes across Member States.
- Enhances the role of the Cooperation Group[59].

59. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

Co-funded by the
Erasmus+ Programme
of the European Union

The New NIS Directive proposal next steps

- The Proposal will be subject to **negotiations** between the Council of the EU and the European Parliament (co-legislators).
- Once the proposal is agreed on and adopted, Member States will have to transpose the Directive in 18 months maximum.
- The Commission must periodically review the NIS2 Directive[59].

59. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

Co-funded by the
Erasmus+ Programme
of the European Union

The European Cybersecurity Act

In 2019 the **EU Cybersecurity act**[60] was adopted, with the aim to:

1. **STRENGTHEN THE ROLE OF THE EU AGENCY FOR CYBERSECURITY** (ENISA), giving to the agency a permanent mandate and more resources and tasks.
2. **ESTABLISH A CYBERSECURITY CERTIFICATION** framework for products and services.

60. EUR-Lex - 32019R0881 - EN - EUR-Lex (europa.eu)

Co-funded by the
Erasmus+ Programme
of the European Union

ENISA - The European Union Agency for Cybersecurity

"Established in 2004, the European Union Agency for Cybersecurity is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow"[61].

The EU Cybersecurity act reinforced the role of ENISA, giving a permanent mandate to the agency. In addition, ENISA has an important role in setting up the European cybersecurity certification framework by preparing the basement for the certification schemes. ENISA oversees the cooperation at EU level, helping EU Member States in handling their cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross-border cyberattacks and crises.

61. About ENISA - The European Union Agency for Cybersecurity — ENISA (europa.eu)

Co-funded by the
Erasmus+ Programme
of the European Union

Cybersecurity act - The European cybersecurity certification framework

The EU Cybersecurity Act introduces an **EU cybersecurity certification framework** for ICT products, services and processes.

Nowadays, different security certification schemes for ICT products exist in Europe. Without a common framework there is a high risk of fragmentation and barriers between Member States.

The certification framework provides EU certification schemes as a common set of rules, technical requirements, standards and procedures.

Each European scheme should specify:

- the categories of products and services covered;
- the cybersecurity requirements, such as standards or technical specifications;
- the type of evaluation, such as self-assessment or third party;
- the intended level of assurance[62].

62. Cybersecurity certification framework | Shaping Europe's digital future (europa.eu)

Co-funded by the
Erasmus+ Programme
of the European Union

The Digital Europe Program

The Digital Europe Programme (DIGITAL) is the **EU funding program** focused on "bringing digital technology to businesses, citizens and public administrations"[56].

It supports projects in 5 main areas:

- supercomputing,
- artificial intelligence,
- cybersecurity,
- advanced digital skills,
- ensuring a wide use of digital technologies across the economy and society, including through Digital Innovation Hubs.

The total budget for the program is €7.5 billion.

56. Digital Programme | Shaping Europe's digital future (europa.eu)

Co-funded by the
Erasmus+ Programme
of the European Union

European Cybersecurity Taxonomy

The European Cybersecurity taxonomy aims at providing **a definition of the cybersecurity context, its application, research and knowledge**.

The Joint Research Centre (JRC) published a study proposing the alignment of cybersecurity definitions and domains to create a comprehensive taxonomy.
This will facilitate the categorization of EU cybersecurity competencies.

The work was undertaken in the context of the Commission's Communication on the establishment of the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (COM(2018) 630 final, 12.9.2018)[63].

63. https://digital-strategy.ec.europa.eu/en/news/european-commission-publishes-eu-cybersecurity-taxonomy

Co-funded by the
Erasmus+ Programme
of the European Union

What is a taxonomy and why it is important

Taxonomy is defined as "**the practice of classification of things or concepts, including the principles that underlie such classification**"[64].

The traditional approach towards the definition of a taxonomy follows the following steps:

(i) Define subject

(ii) Identify sources

(iii) Collect terms and concepts

(iv) Group similar concepts together

(V) Add other term relationships and details[65]

Taxonomy is important because:

- The EU standard on Cybersecurity are different from Country to Country, there are different kinds of approaches, implementations and thresholds.
- The coronavirus crisis saw an important reduction of Cybercrimes.
- Cybersecurity combines a multiplicity of disciplines, from the technical to the cultural ones: today there is no global definition of cybersecurity.

64. https://km4ard.cta.int/2016/11/27/developing-a-taxonomy-for-agriculture-and-rural-development/index.html
65. N. Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G., Figwer, M. and Lazari, A., A Proposal for a European Cybersecurity Taxonomy, EUR 29868 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11603-5, doi:10.2760/106002, JRC118089, Pag. 8 https://publications.jrc.ec.europa.eu/repository/handle/JRC118089

Co-funded by the
Erasmus+ Programme
of the European Union

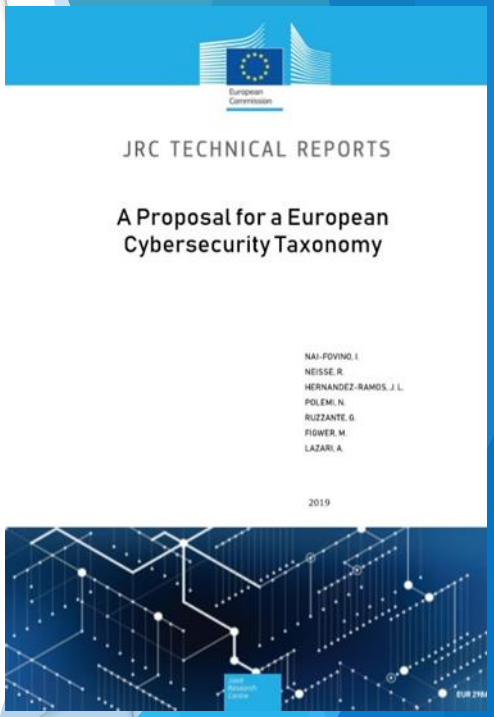
European Cybersecurity taxonomy contents

The JRC proposes a common European Cybersecurity Taxonomy in order:

- to support knowledge management activities
- to enable effective communication among EU institutions and the cybersecurity community
- to serve as a cornerstone in future cooperation efforts among cybersecurity stakeholders
- to support the governance of future EU cybersecurity initiatives

The taxonomy is based on a comprehensive set of standards, regulations and best practices, and has been validated by different EU cybersecurity stakeholders, such as the European Cyber Security Organization (ECSO). It was further enhanced based on feedback provided by the cybersecurity research and competence network pilot projects (CONCORDIA, ECHO, SPARTA and CyberSec4Europe), which embrace over 160 partners including companies, SMEs, universities and research institutes"[65].

The proposal is available at this link.



65. N. Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G., Figwer, M. and Lazari, A., A Proposal for a European Cybersecurity Taxonomy, EUR 29868 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11603-5, doi:10.2760/106002, JRC118089. https://publications.jrc.ec.europa.eu/repository/handle/JRC118089

Co-funded by the
Erasmus+ Programme
of the European Union

European Cybersecurity taxonomy

"The proposed taxonomy report analyzed the different dimensions of the cybersecurity domain and used as sources some of the most widely accepted standards, international working group classification systems, regulations, best-practices, and recommendations in the cybersecurity domain"[66].

High level set of categorization and definition provided are proposed so that they:

- Can be used by a broad range of EU cybersecurity initiatives.
- Become a point of reference for the cybersecurity activities (research, industrial, marketing, operational, training, education) in the DSM by all sectors/industries (health, telecommunication,, finance, transport, space, defense, banking etc.).
- Can be used to index the cybersecurity research entities (e.g., research organizations/laboratories/ associations/academic institutions/groups, operational centers/academies) in Europe.
- Meet compliance with international cybersecurity standards.
- Can be sustainable, easily modifiable and extensible[66].

66. https://digital-strategy.ec.europa.eu/en/news/european-commission-publishes-eu-cybersecurity-taxonomy

Co-funded by the
Erasmus+ Programme
of the European Union

Holistic Taxonomy for Cybersecurity

"A taxonomy trying to cluster a complex and multifaceted discipline as cybersecurity needs to be structured on multiple dimensions"[65].

The JPC group proposed a **three-dimensional taxonomy** based on:

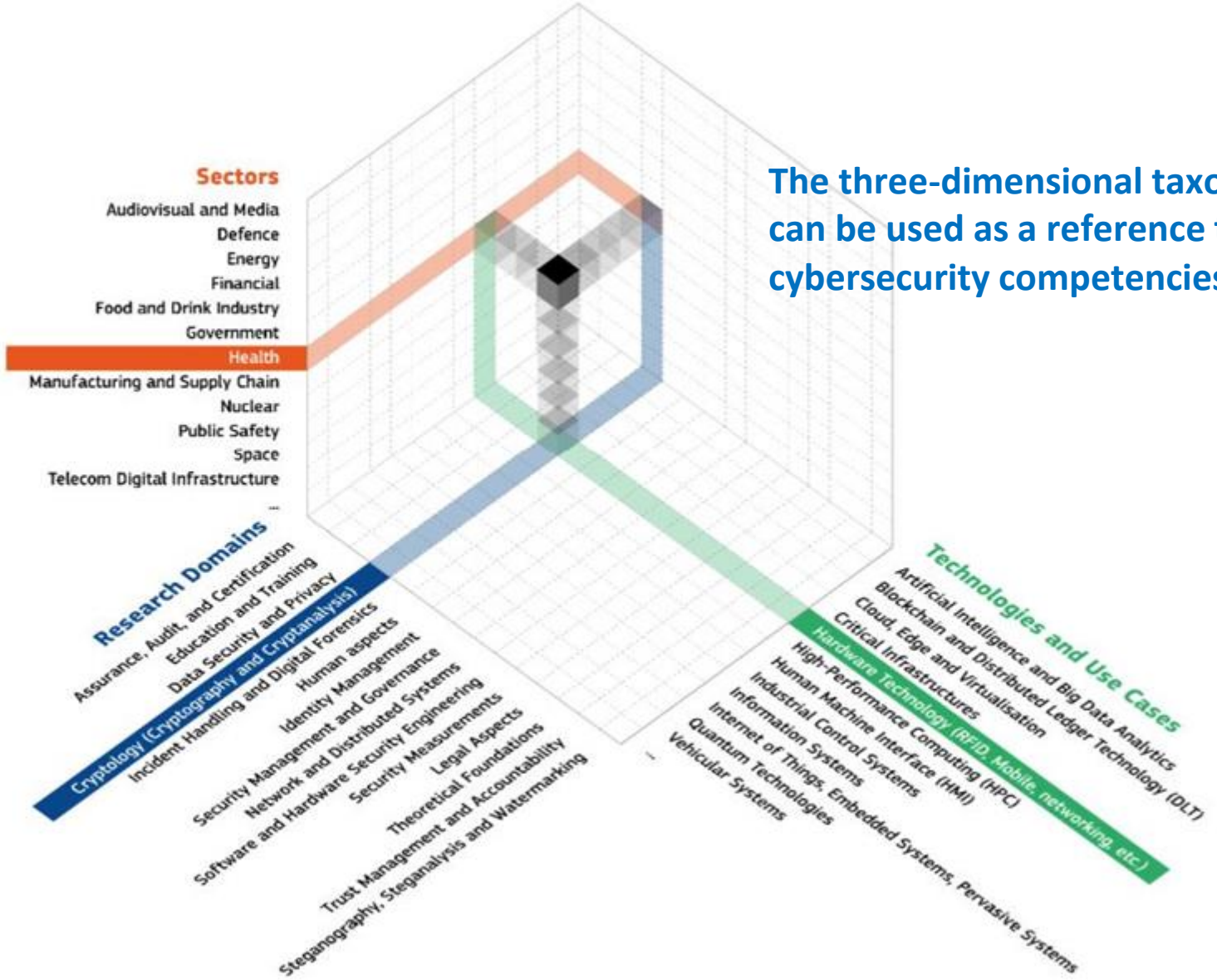
- Research domains represent areas of knowledge related to different cybersecurity aspects (human, legal, ethical and technological aspects).
- Sectors are proposed to highlight the need for considering different cybersecurity requirements (from a human, legal and ethical perspective) in different scenarios.
- Technologies and Use Cases represent the technological enablers to enhance the development of the different sectors. They are related to cybersecurity domains covering technological aspects.

The three-dimensional taxonomy can be used as a reference to map cybersecurity competencies.

65. N. Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G., Figwer, M. and Lazari, A., A Proposal for a European Cybersecurity Taxonomy, EUR 29868 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11603-5, doi:10.2760/106002, JRC118089, Pag. 27 https://publications.jrc.ec.europa.eu/repository/handle/JRC118089

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union



The three-dimensional taxonomy can be used as a reference to map cybersecurity competencies[64].

65. N. Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G., Figwer, M. and Lazari, A., A Proposal for a European Cybersecurity Taxonomy, EUR 29868 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11603-5, doi:10.2760/106002, JRC118089, Pag. 28 https://publications.jrc.ec.europa.eu/repository/handle/JRC118089

Bibliography

Co-funded by the Erasmus+ Programme of the European Union

A. Abdulmajeed, B. Duncan, 2020/06/01, T1 - Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence, conference Paper · June 2020 DOI: 10.1109/CyberSA49311.2020.9139638

M. Alshaikh, Developing cybersecurity culture to influence employee behavior: A practice perspective, Computers & Security, Volume 98, 2020, 102003, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.102003.

E. Amoroso, 2006, Cyber Security. New Jersey: Silicon Press, first edition, ISBN 0929306384

W. Ashford, 2014. SMEs believes they are immune to cyber attack. Computer Weekly, [online] Available at: https://www.computerweekly.com/news/2240216202/SMEs-believes-it-is-immune-to-cyber-attack-study-shows

G. Beuchelt, Chapter 10 - Securing Web Applications, Services, and Servers, Editor J.R. Vacca, Computer and Information Security Handbook (Third Edition), ISBN 9780128038437. https://www.elsevier.com/books/computer-and-information-security-handbook/vacca/978-0-12-803843-7

C. Canongia, R. Mandarino, 2014. Cybersecurity: The New Challenge of the Information Society. In Crisis Management: Concepts, Methodologies, Tools and Applications: 60-80. Hershey, PA: IGI Global. http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003

CNSS. 2010. National Information Assurance Glossary. Committee on National Security Systems (CNSS) Instruction No. 4009: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

J. Crist, Web Based Attacks , SANS Institute Information Security Reading Room https://www.sans.org/reading-room/whitepapers/application/web-based-attacks-2053

DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014: http://niccs.us-cert.gov/glossary#letter_c 8. Oxford University Press. 2014.

ENISA Threat Landscape 2020 - Web-based attacks https://www.enisa.europa.eu/publications/web-based-attacks

Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G., Figwer, M. and Lazari, A., A Proposal for a European Cybersecurity Taxonomy, EUR 29868 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11603-5, doi:10.2760/106002, JRC118089, Pag. 8

A. Georgiadou, S. Mouzakitis, K. Bounas, D. Askounis (2020): A Cyber-Security Culture Framework for Assessing Organization Readiness, Journal of Computer Information Systems, DOI: 10.1080/08874417.2020.1845583

B. Guttman, E. Roback, (1995), An Introduction to Computer Security: the NIST Handbook, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-12r1 (Accessed June 18, 2021)

ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). http://www.itu.int/rec/T-REC-X.1205-200804-I/en

P. Jasheeda, T.K.P.Rajagopal, R.Subathra, Multivariate Correlation Analysis based detection of DOS with Tracebacking, International Journal On Engineering Technology and Sciences – IJETS™ ISSN (P): 2349-3968, ISSN (O): 2349-3976 Volume 2 Issue 4, April -2015

R. A. Kemmerer, 2003. Cybersecurity. Proceedings of the 25th IEEE International Conference on Software Engineering: 705-715. http://dx.doi.org/10.1109/ICSE.2003.1201257

J. A. Lewis, 2006. Cybersecurity and Critical Infrastructure Protection. Washington, DC: Center for Strategic and International Studies. http://csis.org/publication/cybersecurity-and-critical-infrastructure-pr...

Microsoft Official Academic, Course (8 July 2008). *Exam 70-643 Windows Server 2008 Applications Infrastructure Configuration*. John Wiley & Sons. ISBN 978-0-470-22513-4

Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014: http://www.oxforddictionaries.com/definition/english/Cybersecurity

D. Popescul, Daniela, The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation, 2011/06/29, Article SP 978, VL - 4

Public Safety Canada. 2014. Terminology Bulletin 281:Emergency Management Vocabulary. Ottawa: Translation Bureau, Government of Canada. http://www.bt-tb.tpsgc pwgsc.gc.ca/publications/documents/urgence-emerge...

K. Reegård, C. Blackett, V. Katta, The Concept of Cybersecurity Culture, September 2019, Conference: 29th European Safety and Reliability Conference (ESREL)At: Hannover, DOI:10.3850/978-981-11-2724-3_0761-cd

R. Shipsey, Computer security, CO3326 2009, guide prepared for the University of London International Programmes

A. Vishwanath, L. Seng Neo, P. Goh, S. Lee, M. Khader, G. Ong, J. Chin, Cyber hygiene: The concept, its measure, and its initial tests, Decision Support Systems, Volume 128-2020, 113160, ISSN 0167-9236, https://doi.org/10.1016/j.dss.2019.113160.

ENGINE

Co-funded by the Erasmus+ Programme of the European Union

Online references

https://resources.infosecinstitute.com/topic/the-importance-of-cyber-hygiene-in-cyberspace/#gref

https://news.vaimo.com/the-importance-of-cybersecurity-for-small-businesses

https://www.securitymagazine.com/articles/92739-barriers-to-teaching-employees-good-cybersecurity-habits-and-how-to-overcome-them

Que signifie Signature numérique (signature digitale)? - Definition IT de Whatis.fr (lemagit.fr)

https://www.geeksforgeeks.org/what-is-aaa-authentication-authorization-and-accounting/

https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

https://www.vigilantsoftware.co.uk/blog/risk-terminology-understanding-assets-threats-and-vulnerabilities

https://csrc.nist.gov/glossary/term/cyber_threat

https://www.microsoft.com/security/blog/2007/09/11/stride-chart/

Threat Modeling – Avotis

https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html

https://www.infosecurity-magazine.com/malware/

https://www.forcepoint.com/cyber-edu/malware

https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks

Web Application Attack: What Is It and How to Defend Against It? (acunetix.com)

https://www.webroot.com/us/en/resources/tips-articles/spam-vs-phishing

https://staysafeonline.org/stay-safe-online/identity-theft-fraud-cybercrime/spam-and-phishing/

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

https://economictimes.indiatimes.com/definition/web-server

https://www.techopedia.com/definition/4928/web-server

https://www.copahost.com/blog/ftp-meaning/

https://www.webopedia.com/definitions/web-server/

https://www.copahost.com/blog/what-is-web-server/

https://www.carmatec.com/blog/web-services-vs-web-applications/

https://www.carmatec.com/blog/web-services-vs-web-applications/

https://www.quora.com/What-is-the-difference-between-web-service-and-web-application

https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

Shaping Europe's digital future | European Commission (europa.eu)

European Security Union | European Commission (europa.eu)

EUR-Lex - 32016L1148 - EN - EUR-Lex (europa.eu)

Cybersecurity Act | Shaping Europe’s digital future (europa.eu)

Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures | Shaping Europe’s digital future (europa.eu)

Digital Programme | Shaping Europe’s digital future (europa.eu)

NIS Directive | Shaping Europe’s digital future (europa.eu)

EUR-Lex - 52017DC0476 - EN - EUR-Lex (europa.eu)

Co-funded by the
Erasmus+ Programme
of the European Union

https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

EUR-Lex - 32019R0881 - EN - EUR-Lex (europa.eu)

About ENISA - The European Union Agency for Cybersecurity — ENISA (europa.eu)

https://digital-strategy.ec.europa.eu/en/news/european-commission-publishes-eu-cybersecurity-taxonomy

https://km4ard.cta.int/2016/11/27/developing-a-taxonomy-for-agriculture-and-rural-development/index.html

https://publications.jrc.ec.europa.eu/repository/handle/JRC118089

https://digital-strategy.ec.europa.eu/en/news/european-commission-publishes-eu-cybersecurity-taxonomy
https://www1.udel.edu/security/data/availability.html

Co-funded by the
Erasmus+ Programme
of the European Union

Self assessment

Question 1

What are the components of the "The CIA Triad?"

A. Cryptography, Integrity and Availability

B. Confidentiality, Integrity and Authenticity

C. Confidentiality, Integrity and Availability

D. Confidentiality, Information and Authenticity

Co-funded by the
Erasmus+ Programme
of the European Union

Self assessment

Question 2

Identify examples of cyber-attacks:

A. Repudiation, Correlation and traceback and WSDL.

B. Masquerading, W3C and HTTP protocol

C. Man-in-the-middle, Masquerading and Eavesdropping

D. Simple Object Access Protocol, Denial-of-service and Computer Security Incident Response Team

Co-funded by the
Erasmus+ Programme
of the European Union

Self assessment

Question 3

What is a "Web service"?

A. It is a piece of computer hardware or software that accesses a service made available by a server as part of the client–server model of computer networks

B. A system of software allowing different machines to interact with each other through network

C. The Strategy that improves the cooperation between partners to promote a global, open, stable and secure cyberspace, founded on the rule of law, human rights, fundamental freedoms and democratic values

D. Are various techniques used to redirect web browsers to websites

Co-funded by the
Erasmus+ Programme
of the European Union

Self assessment

Question 4

What is a "Web Server"?

A. The feature of certain records or transactions not attributable to any individual

B. Is a combination of hardware and software that stores, processes and delivers web pages to the users upon request

C. A server stored designed for human interaction that runs locally via the operating system (OS) and can be accessed through browsers.

D. The computation of a (hash) function that maps the contents of a file to a numerical value.

Co-funded by the
Erasmus+ Programme
of the European Union

Self assessment

Question 5

Assets include:

A. Software, Hardware and Confidential data

B. Hardware, Software and Public data

C. Software, Hardware and Encrypted data

D. Firmware, Software and Hardware

Co-funded by the
Erasmus+ Programme
of the European Union

Self assessment

Question 6

The Software represents any physical part of a computer.

A. True

B. False

Co-funded by the
Erasmus+ Programme
of the European Union

Self assessment

Question 7

NIS Directive proposal establishes a cybersecurity certification framework for products and services.

A. True

B. False

Co-funded by the
Erasmus+ Programme
of the European Union

Self assessment

Question 8

The copy of physical or virtual data is named:

A. Steganography

B. Blacklist

C. Backup

D. Digital Signature

Co-funded by the
Erasmus+ Programme
of the European Union

Self assessment

Question 9

A spear-phishing attack

A. Just involves a combination of social engineering and deception to persuade potential victims to divulge sensitive information
B. Is a phishing attack that employs personalized and more sophisticated tactics
C. Is a type of malware disguised as legitimate software that can cause damage in the computer
D. Is an attack based on unsolicited mass messages sent via e-mail, instant messaging or other digital communication tools

Co-funded by the
Erasmus+ Programme
of the European Union

Self assessment

Question 10

The digital signature:

A. Converts data back into a form that can be read and understood by a human or computer
B. Creates basic CSC in a working group
C. Validates the authenticity and integrity of a digital message, software or document
D. Protects or defends the use of cyberspace from cyber-attacks