FRI-1.414-MIP-05

CYBER SECURITY - MAIN DIRECTIONS[5]

Pr. Assist. Prof. Valentin Velikov, PhD
Department of Informatics and Information Technologies,
University of Ruse "Angel Kanchev"
Tel.: +359 886 011 544
E-mail: vvelikov@ami.un-ruse.bg

Abstract: *The article examines the main directions in the field of cyber security.*

There are explore and summare what cyber security is from several perspectives, the main directions out of dozens of possible ones. Fundamentals of network security and standards, information security, public opinion management, physical security, industrial security, risk management, access control, project management, risk assessment, and more are covered.

Some tools for monitoring traffic, defining vulnerabilities and protecting information in network security are implied. Some good practices and standards for data protection are discussed.

Keywords: Cybersecurity, *Software Engineering, Information systems.*

INTRODUCTION

Cybersecurity is an extremely relevant topic in recent times, especially in our hectic everyday life. A lot is written and a lot is commented on. However, many people think of cyber security as network security, when in fact it is a combination of different fields, only one of which is network security. This gave the idea of a study and summary on the topic of what is cyber security and its directions, which turned out to be so many that only the main ones will be touched on in this overview.

The term Cybersecurity - directly can be categorized with two different words: 'cyber' - means "things directly or indirectly related to computers and information processing and 'securities' - means security or "protection of types of things from abuse"[1].

EXPOSITION

1. Cybersecurity Domains [6].

Major areas of cybersecurity are presented in Henry Jiang's Cybersecurity Domains map [6]. Cybersecurity domains - represent a complex network of multiple cybersecurity measures working together to protect a given system [7] [5]. They are also called cybersecurity categories, focus areas, and levels [5]. Depending on the direction and needs, different domains can be considered and represented, and even Henry Jiang's has 3 versions. Main directions:

1. Network Security;
2. Telecommunication Security;
3. Information Security – ISO 27001;
4. Industrial Cybersecurity;
5. Social Engineering;
6. Physical Security;
7. Security Architectures;
8. Frameworks and Standarts;
9. Risk Assessment;
10. Enterprise Risk Management;
11. Aplication security;
12. Governmance;
13. Identity Management;
14. Threat Intelligence;

[5] Докладът е представен на конференция на Русенския университет на 27 октомври 2023 г. в секция „Математика, информатика и физика".

15. Security Operation;
16. Incident response;
17. Career development;
18. User Education etc.

From Henry Jiang's diagram (Fig.1), it can be seen that each of the main lines has at least 10 branches, and each of them can be described with its purposes, features, service and development.

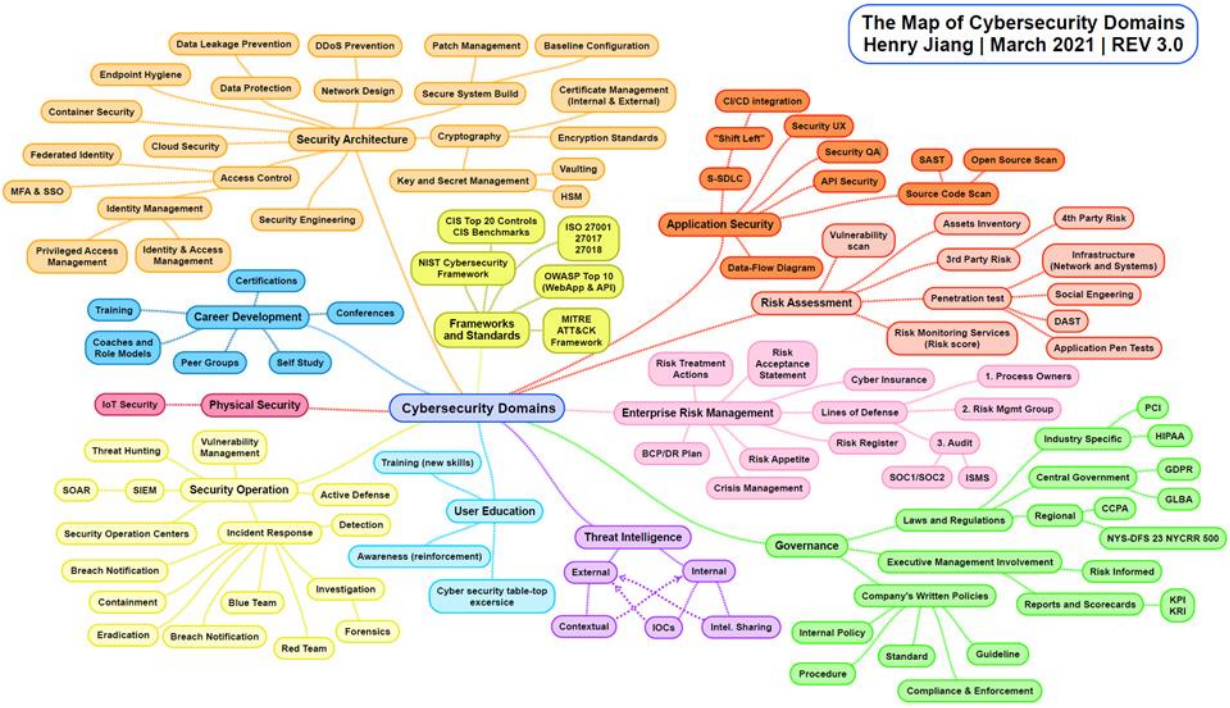

Fig. 1 – The map of Security Domains – Henry Jiang, rev.3

2. Cybersecurity [2]

Some authors [2] explore cybersecurity (also known as digital security) as the practice of protecting digital information, devices, and assets. This includes personal information, accounts, files, photos, money, and more.

Many business models are built on the continuity of Internet access and flawless functioning of information systems.

Cybersecurity is a set of principles, strategies, means and approaches for managing risks to the functioning of the cyber environment and actions aimed at protecting the cyber resources of the organization and the user.

Cyber security consists in ensuring the safety and operability of the user's resources in the conditions of a multitude of threats. It aims to organize the safety of the cyber environment in which the organization and the user operate. In this case, it is a set of policies and actions, hardware and software tools that are designed and used to protect the infrastructure of computer networks from unauthorized access, theft, deformation, destruction and other threats. It provides monitoring and evaluation of the cyber environment in order to guarantee the quality of its functioning.

3. CIA

The acronym "CIA" (Confidentiality, Integrity, Aviability) is often used to represent the three pillars of cybersecurity. It is based on three main concepts known as "The CIA Triad":

3.1. Confidentiality – storing the data and ensuring that only authorized people have access to relevant files and accounts. This is where the rules that limit access to information are defined. Privacy means taking measures to limit access to sensitive information from cyberattacks and hackers. In an organization, people are allowed or denied access to information according to its category by authorizing certain individuals in the relevant department. They should receive proper training on sharing information and securing their accounts with strong passwords. They can change the way

data is processed within an organization to ensure data protection. Different ways to ensure privacy can be two-factor authentication, data encryption, data classification, biometric verification, security tokens.

3.2. Integrity – it must be certain that the information is what it is expected to be and that no file is inserted, modified or deleted without the appropriate permission. It must be ensured that the data is consistent, accurate and reliable over the relevant time period. This means that data in transit must not be altered, deleted or illegally accessed.

Actions must be taken within the organization to ensure its safety. File permissions and user access control are among the data breach control measures. There should also be tools and technologies in place to detect any data alteration or breach. Various organizations use checksum and even cryptographic checksum to verify data integrity. To deal with data loss or accidental deletion or even cyber attacks, regular backups should be in place.

3.3. Aviability – ensuring that access to relevant information and systems exists when required. An example of an access problem would be a denial of service attack, where hackers clog the system with network traffic to make it nearly impossible to access; or ransomware that encrypts the system and prevents its use. The security equipment available for all required components (such as hardware, software, networks, devices) must be maintained and upgraded. It should ensure smooth operation without disrupting data access. Constant communication between components must be ensured by providing sufficient bandwidth. Also included here is a selection of additional safety equipment in case of disaster or difficulty. Utilities such as firewalls, disaster recovery plans, proxy servers and a suitable backup solution should ensure DoS attacks are dealt with. For a successful approach, access must pass through multiple layers of security to ensure the protection of each CyberSecurity component. This includes computers, hardware systems, networks, software programs and data shared between them.

It should be borne in mind, however, that the higher the security and the more layers of protection are passed, the more the time to access the data and its availability at the required time increases (Fig. 2). This should be closely linked with risk assessment, data integrity verification and rapid and adequate response in the event of an incident.

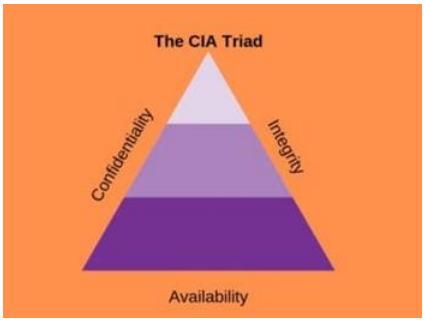

Fig. 2 - „Триадата на ЦРУ“

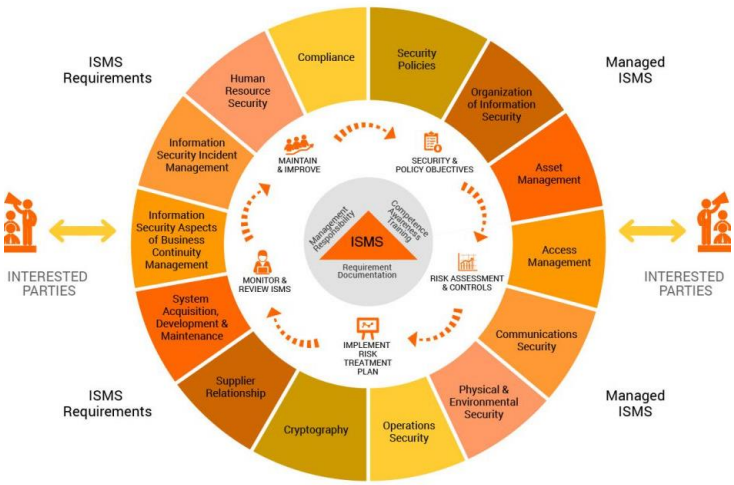

Fig. 3 - ISO/IEC 27001 Information Security Management System [9]

Some of the main cybersecurity categories:

- Network security – usually consists of regulations and internal organizational policies adopted and enforced by the network administrator for the purpose of preventing and monitoring unauthorized access, misuse, modification or causing a denial of service of a computer network and resources that are network accessible. Requirements and practices are usually based on various documents at national and European level. The most common and simple way to protect network resources is by assigning a unique username and password to the respective users.

- Telecomunication security – telecommunications networks include analog, digital and mobile networks (also known as Next Generatin Network (NGN)). In one network, all information and services (voice, video, data) are carried using Internet Protocol (IP) packets. With their continuous development, the inclusion of new device types and protocols (IPv6), the transition from 4G/LTE to 5G and the pending 6G mobile standards, there are increased security risks.
- Frameworks and standarts - these are a set of good practices for controlling risk. They offer the ability to determine the degree of risk tolerance and set controls for business management. Many frameworks and standards are combinations of other frameworks. Leading in Europe is the ISO 27001 standard. Some of the most popular frameworks and standards are:
  - ASD (Australian Signals Directorate) Essential 8
  - CIS (Center for Internet Security) Controls
  - CISA (Cybersecurity and Infrastructure Security Agency) TSS (Transportation Systems Sector) Cybersecurity Framework
  - ETSI (European Telecommunications Standards Institute)
  - HITRUST CSF (Cybersecurity Framework)
  - ISA/IEC (International Society of Automation) 62443
  - IoTSF (Internet of Things Security Foundation) Security Compliance Framework
  - MITRE ATT&CK
  - NIST (National Institute of Technologies) CSF (Cybersecurity Framework)
  - NIST SP (Special Publication) 800-82 Guide to ICS (Industrial Control Systems) Security
  - OASIS SAML (Security Assertion Markup Language)
  - PCI DSS (Payment Card Industry Data Security Standard)
- Aplication security – installing various forms, software and services in the organization to protect against a diverse set of threats. Taking various measures to limit unwanted access, implementing strong input validation, threat modeling, writing secure code, etc.
- Risk Assessment – risk assessment is the careful analysis of the workplace to identify scenarios, processes, etc. that may harm various assets (people and systems) belonging to the organization. Consists of:
  - Hazard identification
  - Risk analysis and risk assessment
  - Risk control

Risk assessment identifies hazards and risk factors that may cause some harm. The analysis and assessment is done to analyze and assess the risks associated with the identified hazards and risk factors. Risk control is concerned with determining the best ways to eliminate hazards or control them when they cannot be eliminated. This includes asset inventory, penetration testing, risk monitoring services, vulnerability scanning.

- Enterprise Risk Management - ERM - Enterprise risk management or ERM is an organization-specific strategy that aims to identify risks and prepare for hazards within the organization, within the allocated budget. The sub-domains of enterprise risk management include:
  - Crisis management
  - Cyber inshurance
  - Lines of defence
  - Risk acceptance statement
  - Risk appetite

ERM is a process developed and maintained over time, not a product or service. To be effective, it must be part of the work culture of an organization. It is essential to maintain the brand's reputation and ensure the long-term viability of the business.

- Governmance – Cybersecurity governance offers a strategic view of how an organization determines its risk appetite, develops accountability frameworks and establishes the decision-making process. This includes making decisions about applying security policies. The standards developed and offered at the state and European level (ISO 27001, [1], [3], [4]) are of great importance here. Governance aims to ensure that the organization manages to make the right decisions most of the

time and puts in place effective and cost-effective policies to reduce risk. This includes written company policy, executive management involvement, laws and regulations.

- Cyber Threat Intelligence - CTI - threat intelligence is the process of gathering information from a wide range of resources pertaining to existing or potential attacks against the organization. Collected information is analyzed and refined to minimize and mitigate cybersecurity risks. Along with other cybersecurity tools, CTI is used to protect the organization from cyber attacks. Intelligence can be external or internal.
- Security Operation - refer to the tasks that put security plans into action. These cover the application of resource protection techniques, disaster recovery, incident management, physical security management and understanding and supporting investigations. This includes logging and monitoring services, requirements for investigation types, ensuring the provision of resources.
- Social engineering – a set of tactics that are used to manipulate people and/or their minds into sharing sensitive information or changing their behavior. One way of manipulation is for someone to pose as a trusted person (relative, colleague, superior) who is trusted and on their behalf information is requested to access a file, website or mail. It can often look like a tech support call asking for login, profile or personal information. Fraudsters often conduct extensive preliminary research on the site in order to gain trust. Among the most common attacks (performed through social engineering) are: fishing (with Smishing and Vishing varieties), Spear Fishing, Baiting, Tailgating.
- Phisical security – it is the process of protecting people, property and physical assets from events and scenarios that could result in damage or loss. Different cybersecurity teams must work together to secure an organization's digital and physical assets. This is necessary due to the fact that the complexity of physical security is increasing due to rapidly developing technologies such as Internet of Things (IoT) and Artificial Intelligence (AI)
- Career development – this is a fact that needs to be taken into account because the demand for experienced and qualified cyber security professionals has increased. Career development includes certification, conferences, peer groups, interest groups (such as LinkedIn), self-study, training, etc. In addition, there are various programs and topics (on multiple sites) such as information security, risk assessment, ethical hacking certification training, etc.
- Security Architecture – A security architecture is a unified security template for addressing the potential risks and requirements of a particular state or environment. The security architecture also defines where and when to apply security controls. Design principles and specifications for deep security controls are clearly documented in various documents and standards. The main attributes of the security architecture are:

- benefits:
- driving activities (Drivers):
  - benchmarks and good practices
  - financial
  - legal and regulatory
  - risk management
- forms
- relationships and dependencies

Architecture risk assessment, implementation, operations and monitoring, and security architecture and design are the key phases in the security architecture process.

4. Protection is a process, not a product - recommendations

Digital security involves creating a set of well-thought-out processes and practices. They include:

- Data backups – Important data should be stored in a secure location and it should be possible to quickly restore a good, tested copy of the data in the event of a problem with it.
- Good cyber habits – not to open (without checking) unexpected links or attachments received in email or text, even if they appear to be from a trustworthy sender.

- Keeping software up-to-date – operating systems such as Windows, MacOS, iOS or Android, as well as apps and browsers should be updated with the latest versions and fixes from the manufacturer.
- Use strong, unique passwords – good passwords should be at least 14 characters long, should not contain English words, and should not be reused across multiple accounts.
- Use multi-factor authentication – Whenever possible, both at home and at work, use multi-factor authentication.
- Lock devices – Make sure devices require a password, PIN, or biometric authentication, such as fingerprint or face recognition, to log in.

CONCLUSION

Cybersecurity is a broad topic, covering a large set of principles, tools, frameworks, and more. In an organization, to achieve an effective cyber security approach, people, processes, computers, networks and technology – all must be equally accountable and motivated. If all the components complement each other, it is very possible to successfully counter various cyber threats and attacks.

ACKNOWLEDGMENTS

This publication reflects research from the scientific project 23-FPNO-02 “Investigation of effective knowledge management mechanisms applied in software engineering when creating projects with Agile methodologies” - of the “Scientific Research” fund of Ruse University “Angel Kanchev”, 2023.

REFERENCES

1. Cybersecurity Act, State Gazette, Sofia, 2018.11.07 (Оригинално заглавие: Закон за киберсигурност, Държавен вестник, София, 7.11.2018г.)

2. What is mean the Cybersecurity (Какво представлява киберсигурността, 14.06.2023 - https://support.microsoft.com/bg-bg/topic/%D0%BA%D0%B0%D0%BA%D0%B2%D0%BE-%D0%BF%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B0%D0%B2%D0%BB%D1%8F%D0%B2%D0%B0-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%81%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82%D1%82%D0%B0-8b6efd59-41ff-4743-87c8-0850a352a390

3. https://www.consilium.europa.eu/bg/policies/cybersecurity/ - 20.06.2023

4. https://www.europarl.europa.eu/news/bg/headlines/society/20220120STO21428/kibersigh urnost-ghlavnite-i-novite-zaplakhi?at_campaign=20234-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=DSA&at_goal=TR_G&at_audience=&at_topic=Cybersecurity&gclid=EAIaIQobChMInPfYtc_1gQMVSIVoCR2CgQOYEAMYASAAEgLUw_D_BwE – 22.06.2023

5. https://www.knowledgehut.com/blog/security/cyber-security-domains - 05.08.2023

6. https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/

7. https://10pie.com/cybersecurity-domains/ - 10 Cybersecurity Domains and Difference Between Them, 12.08.2023

8. https://www.ncsc.gov.uk/ - The National Cyber Security Centre (NCSC) – UK, 15.08.2023

9. https://ccqm.ch/certification-process/iso-iec-27001-information-security-management-system/ - ISO/IEC 27001 ISMS (Information Security Management System), 17.08.2023