UNIVERSITY "POLITEHNICA" of BUCHAREST

DOCTORAL SCHOOL ETTI-B

Decision 531 **of** 28.07.2020

SUMMARY
OF PhD THESIS

CYBER SECURITY: THE VULNERABILITIES OF FUTURE INFORMATION SYSTEMS

SECURITATE CIBERNETICĂ: VULNERABILITĂȚILE SISTEMELOR INFORMATICE ALE VIITORULUI

PhD Candidate: **Ionuț-Daniel BARBU**

DOCTORAL COMMITTEE

Chair of the committee	**Prof. Gheorghe BREZEANU, PhD**	from	**University POLITEHNICA of Bucharest**
Supervisor	**Prof. Ioan BACIVAROV, PhD**	from	**University POLITEHNICA of Bucharest**
Examiner	**Prof. Mircea POPA, PhD**	from	**Politehnica University Timisoara**
Examiner	**Prof. Gheorghe ȘERBAN, PhD**	from	**University of Pitesti**
Examiner	**Assoc. Prof. Marian VLĂDESCU, PhD**	from	**University POLITEHNICA of Bucharest**

BUCHAREST 2020

Table of Contents

Acknowledgements

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU/159/1.5/S/132397.

Chapter 1. Introduction

Over the last decade, technology in general and, in particular, information technology have profoundly transformed the global business environment, with continuous advances in all areas, from teamwork, cloud data storage and blockchain to Artificial Intelligence (AI) and IoT (Internet of Things). As digital technologies evolve and change traditional business models, cybersecurity risks appear to be evolving even faster. Cyber risk has moved to a higher level, beyond the already "classic" security breaches and sensitive data leaks, reaching sophisticated schemes that can disrupt an entire company or industry, managing a supply chain or even, at government level, may affect the functioning of a state. The damage amounts to billions of euros and affects companies in any sector of activity and, also, national economies.

1.1. Presentation of the field and opportunity of the doctoral thesis

The field of information technology is constantly changing, new hardware technologies are appearing, software is improving, and business processes are being optimized. The history of information systems consists of a constant flow of technological advances. Mainframe computers were followed by minicomputers, which in turn were followed by personal computers and then mobile devices. Software development has followed a similar trajectory, with an evolution from batch-oriented applications, specific to mainframe systems, moving from client-server models to distributed service architectures and Web applications. Business processes have changed, and data processing has expanded beyond the level of back-office systems geared toward core operations, to widely adopted collaboration and productivity applications.

The "*2019 Global Cyber Risk Perception Survey*", conducted by Marsh and Microsoft, investigates perceptions of cyber risk and risk management in organizations around the world, especially in the context of a rapidly evolving business technology environment [1]. The conclusions of this study, briefly presented below, highlight the current state of cyber risk in organizations.

1. Awareness of cyber risks has increased. Motivated by the frequency and severity of recent incidents with a major impact on data security, organizations' priorities regarding security risks and threats increased significantly in 2019 compared to 2017 among organizations.

2. The risks associated with cyber-attacks or threats far outweighed all other risks. In 2019, most respondents ranked cyber risk as a top concern, while economic uncertainty came in second position of these concerns.

3. Most organizations are considering or already using several new technologies. Businesses borrow technological innovation, and most do not see cyber risk as a barrier. At least 70% of respondents to the 2019 survey mentioned at least one innovative operational technology - including cloud computing, own digital products and connected IoT devices - that they have adopted or are considering.

In this context, the opportunity of the chosen topic is given by the actuality and impact of cybersecurity, considered as the most important technologically aspect in the Global Risks Report 2020 of the World Economic Forum [2]. Introduced in 2015 by Klaus Schwab, the Founder and Executive Chairman of the World Economic Forum, in the article "*The Fourth Industrial Revolution. What It Means and How to Respond*" [3], the term "*Fourth Industrial Revolution*" refers to technologies that combine the fields of hardware, software and biology (cyber-physical systems), based on advances in telecommunications and connectivity. Thus, it is estimated that the 4IR (Fourth Industrial Revolution) era will be marked by discoveries in emerging technologies in fields such as robotics, artificial intelligence, nanotechnology, quantum computing, biotechnology, IoT, IIoT (Industrial IoT), decentralized consensus technologies (blockchain), wireless technologies and 5G mobile networks, 3D printing and fully autonomous vehicles. This wave of 4IR technologies will dramatically reshape economies and societies: precision medicine, autonomous vehicles and drones are expected to grow rapidly, while artificial intelligence is expected to boost global growth by 14% by 2030 [4].

1.2. The purpose of the doctoral thesis

The work "*Cyber Security: The Vulnerabilities of Future Information Systems*" examines the global context of current cyber security, presents the author's considerations regarding the prospects for the evolution of cyber threats and vulnerabilities, and proposes several security solutions, applicable to both current and future systems that will govern our activity in the near future.

All involved entities (from individual users to small organizations, large companies or entire nations) must accept a unanimously accepted axiom, currently valid and from which we started the research in this doctoral thesis. Cyber vulnerabilities exist, cyber threats can be proactively addressed, the impact of attacks can be mitigated, information loss can be minimized, disaster recovery policies can be applied at the organizational level. In this context, *cybersecurity risk can be managed / minimized, but it cannot be eliminated*.

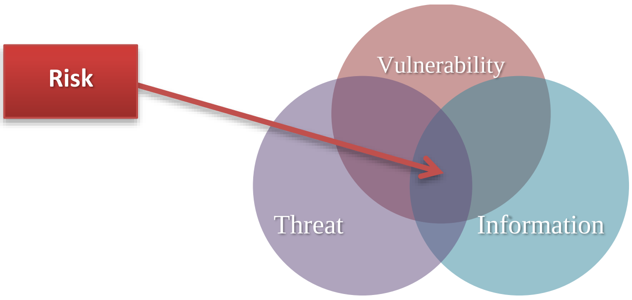


Fig. 1.5 Cybersecurity risk

The topic of this doctoral thesis was approached from two points of view which, only implemented complementary, will have an impact on the organization. Given my dual professional training, I analyzed the current situation both from a managerial perspective, by proposing a model for implementing an information security program adapted to the industry and the ever-changing challenges, and from a technical point of view, applying an in-depth security analysis model. Thus, analyzing the impact of vulnerabilities on information systems, networks and IoT devices, we observed the less mature areas of security systems and developed scalable technical solutions to address security issues and reduce the attack area once implemented.

The chapters of the work provide an overview on the awareness of the implications of cybersecurity in honeypots systems and in smart cities to cover a diverse range of applicability. The research was carried out by a test session conducted in a development environment designed to build small IoT projects to study the limitations of hardware and software in data packet analysis.

The results presented in the paper also led to the acquisition of cyber intelligence on the actors who conduct cyber-attacks on local computers, LANs and e-learning platforms. Because we want to promote access to education at very low costs, the hardware used in the study involved low prices, and the type of software was open source or educational.

The main purpose of this doctoral thesis is to draw attention to the need for security implementations and compliance standards for risk mitigation in areas of applicability, given the types of vulnerabilities and threats specific to currently used technologies, in a physical, mental, technical and organizational / managerial totally modified by the COVID-19 pandemic that humanity is currently facing.

1.3. Organization by chapters and the content of the thesis

The PhD thesis was structured in 5 chapters and a final section consisting of 3 annexes

Chapter 1 introduces the topic of this thesis, presenting the field of cyber security, the context in which the work was developed and the opportunity to choose this topic, current and especially by perspective, even in the immediate future.

Chapter 2 addresses general aspects on information security: this concept is framed within a more complex term (dependability of systems) and standards and regulations in this area are presented (including aspects related to IoT and personal data protection). A special subchapter is dedicated to security risk analysis and management. At the end of the chapter are presented methodologies and strategies for developing security policies at organizations level. There is also a comparative analysis of SOC vs. SIC cybersecurity centers and a profile of the cybersecurity analyst.

Chapter 3 presents cyber security threats to systems. We exposed aspects related to the types of cyber-attacks, the profiles and motivations of cyber-attackers and the current vulnerabilities of applications. In another subchapter we analyzed in detail two types of current threats (APT - Advanced Persistent Threats - and ransomware), with prospects for increasing complexity and impact in the near future, and we performed two types of analysis (static and dynamic detection) for malware applications. Also, in this chapter we implemented a system for analyzing cyber-attacks and attackers, which consisted of several honeypots (Moodle e-learning platforms) distributed worldwide in a honeynet in order to obtain cyber intelligence.

Chapter 4 begins with 3 categories of theoretical models used for the analysis and implementation of information systems security. Based on the Defense in Depth model, we proposed solutions for securing the 7 levels considered at the organizational level. To secure the local network, we have developed an intrusion detection application based on a preliminary analysis of available hardware and software resources. A Raspberry Pi architecture was initially used as hardware support, and as software support, following a critical study on the dependability of cloud computing platforms, we chose DigitalOcean Public Cloud services.

Chapter 5 presents the conclusions of the researches and the results obtained after the doctoral studies. The published scientific papers and the research activity carried out are indicated, including the participating within the programme POSDRU/159/1.5/S/132397. Finally, several directions for developing contributions and readjustment the whole society to the new global context generated by the coronavirus pandemic are analyzed.

Chapter 2. Information security

In the second chapter of the paper we presented aspects related to the concept of information security that aims to protect data and information systems against illegal access and violation of principles regarding their confidentiality, integrity or availability.

The chapter began with a theoretical introduction of some basic concepts regarding dependability of information systems. A fundamental component of this concept is the reliability of a system, i.e. the probability of its proper functioning over time. For the reliability analysis, the most used methods were briefly listed, among which we could mention RBD (Reliability Block Diagram) in the category of methods based on the state of operation of the system, respectively FTA (Fault Tree Analysis) in the category of methods based on system failure.

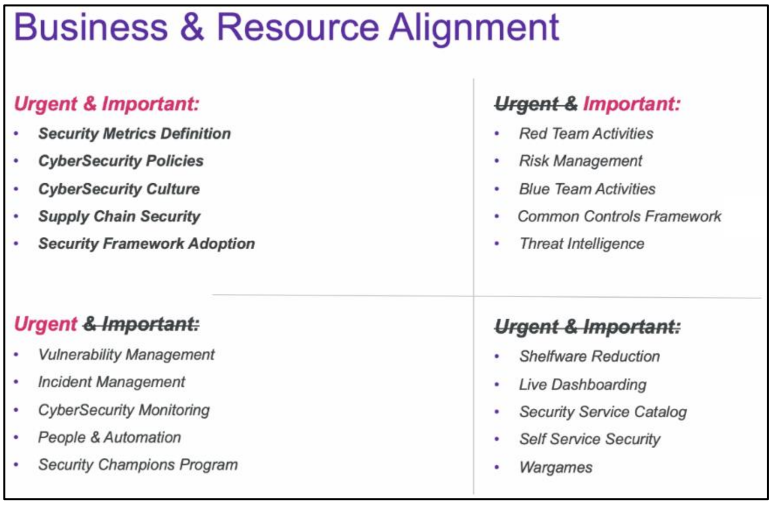
ISO/IEC 27001:2013 addresses information security through the following three components of dependability: confidentiality, integrity and availability, aspects presented in detail in subchapter 2.1.2. Confidentiality is defined by ISO 27001:2013 as “the property that information is not made available or disclosed to unauthorized persons, entities or processes” [24], integrity refers to the protection of accuracy and active information, and the availability is the probability that a system be operational at the current time.

In subchapter 2.2 we have synthesized relevant standards and regulations in the field of information security. For the ISO/IEC 27001:2013 standard "*Information technology - Security techniques - Information security management systems - Requirements*" we presented the structure and changes compared to a previous version, 27001:2005. The NIST Cyber Security Framework, presented below, is a collection of guidelines in the field of information systems security, used at the organizational level to assess and improve the capacity to prevent, detect and respond to cyber-attacks.

Regarding the issue of personal data protection, two relevant regulations were mentioned: GDPR (General Data Protection Regulation (EU) 2016/679) valid in the European Union and the EEA (European Economic Area), respectively the California Consumer Privacy Act (CCPA). The comparative study of the two regulation shows several similarities, but we can emphasize in particular the differences in the scope and, obviously, in the geographical area to which those provisions apply. It is important to note that there is an improved understanding of the importance of data value. In addition to global approaches, such as the adoption of the two legislative decisions, which aim to protect sensitive data at the level of the individual (consumer), an important role is played by the fact that users know and are aware that there may be important information in any system, which can compromise the entire infrastructure.

The last part of this subchapter presents regulations intended for the standardization of the IoT domain. This standardization is necessary for the coherent, compatible and secure development of IoT specific applications. Among the organizations that address such standardizations are ISO and IEC with the standard "*ISO/IEC CD 27030 - Information technology - Security techniques - Guidelines for security and privacy in the Internet of Things (IoT)*", under development at the time of writing this work.

Subchapter 2.3 presented analysis and management of security risk. The purpose of such an assessment is to increase the level of security in the design and implementation of a project. A critical initiative for the defense of networks is the "zero-trust" concept. Zero trust refers to a set of network security paradigms that restrict defenses from wide perimeters of the network to individuals or small groups of resources. Its focus on protecting resources rather than network segments is a response to trends that include remote users and cloud-based assets, which are not located within a company-owned network. In this subchapter, special attention was paid to time management issues through the Eisenhower decision matrix method. A personal contribution was the design of a customized matrix to improve the activity of a company, in which tasks were organized based on 2 criteria: urgency and importance (Eisenhower method) [39].



Business & Resource Alignment

Urgent & Important:
- Security Metrics Definition
- CyberSecurity Policies
- CyberSecurity Culture
- Supply Chain Security
- Security Framework Adoption

~~Urgent &~~ Important:
- Red Team Activities
- Risk Management
- Blue Team Activities
- Common Controls Framework
- Threat Intelligence

Urgent ~~& Important:~~
- Vulnerability Management
- Incident Management
- CyberSecurity Monitoring
- People & Automation
- Security Champions Program

~~Urgent & Important:~~
- Shelfware Reduction
- Live Dashboarding
- Security Service Catalog
- Self Service Security
- Wargames

Fig. 2.7 Proposing an Eisenhower matrix to improve the activity of a company

Another personal contribution can be found in the subchapter 2.4.2, where we completed a questionnaire whose purpose was to determine the degree of awareness of information security within organizations. The questionnaire (presented in full in Annex A.1) consists of 20 questions with two or more possible answers, and each answer was assigned a risk factor between 1 (minimum security risk) and 10 (maximum security risk). The results of completing this questionnaire (calculating the level of risk to the human component of an organization) can be used in employee information, awareness and training programs or in security policies required in the organization.

In subchapter 2.4.3 we performed a comparative analysis of SOC vs. SIC and we have highlighted the benefits of the transition from classic Security Operations Centers (SOCs) to an advanced model (SIC - Security Intelligence Center) that uses intelligence to understand and anticipate threats to an organization [48]. A comparison between the two models can be based on the approach to cyber security, reactive vs. proactive. SIC focuses on the ability to anticipate threats before they become incidents and on the disadvantages of traditional SOC, including posture and reactive security monitoring. The impact of such a transition on processes, but also on users and organizations, is beneficial. It is worth mentioning the aspect of migration automation that allows human resources to be separated from routine activities, allowing them to focus on the information gathered. As the tools of the various business-oriented vendors are designed to work for everyone, but are not particularly optimized for anyone, the importance of implementing customized tools, supported by engineering teams with advanced knowledge in the field, was emphasized.

In today's IT field, automation is what drives any business. Undoubtedly, a SIC should base its operations on automation. Applying automation to daily activities allows analysts to see, identify, track, and more importantly, respond to threats before they affect systems. In this global analysis of automation, it is essential to approach honeypots as one of the most successful tools used to collect information about threats.

The advantage of an intelligence-based defense solution is particularly important in dynamic environments where the flow of information is fast, and anomalies need to be identified quickly. In today's landscape of cyber threats, there must be a deep understanding of past and present events in order to try to defend against future attacks. Therefore, a SIC analyst needs to focus on SOC and SIC comparisons and to develop the capacity to obtain a complete vision [49]. Given that all "CxO" roles (CIO, CISO, etc.) aim at an evolved security stance, monitoring team managers must prepare for the transition of their teams' approach to an active threat detection. Although there is no predefined standard recipe for migrating from a security operations center to a smart security center, it is recommended to move as soon as possible given the Advanced Persistent Threats as a certainty of the present and especially the future.

In subchapter 2.4.4 we have made a profile of the cybersecurity analyst [51], a challenging job which, although at first it may seem difficult and demanding, is supported, in addition to the constant exchange of knowledge between employees of this professional category, by tools monitoring of security systems mapped at all levels of the Defense in Depth strategy. This analyst must be constantly up to date with security news, concepts, threats and trends and has the support of other specialists in related security fields, such as vulnerabilities assessment, forensics, data loss prevention, penetration testing or network security.

Chapter 3. Cyber security threats

Chapter 3 addressed the topic of cyber security threats, and the components analyzed were: cyber-attacks, cyber attackers, current computers vulnerabilities and estimates of current threats and the prospect of immediate evolution.

At the beginning of the chapter we classified cyber-attacks according to a series of criteria and we detailed the main categories of malicious applications, including malware, phishing, SQL injection, XSS (Cross-Site Scripting), DoS (Denial of Service). Next, we analyzed the top 15 of cyber security breaches in recent history and their impact on organizations.

The contribution made in subchapter 3.1.3 addresses security risks due to ARP (Address Resolution Protocol) spoofing attacks [69]. Low-cost hardware was used, combined with existing software capabilities for packet analysis and intrusions detection. The proposed solution, consisting of the monitoring device together with the created application and Python scripts, was developed as a concept that can be used by security analysts in testing, the ultimate purpose being for network equipment manufacturers to adopt similar solutions to provide malicious attacks detection capabilities for devices that are part of the Small Office Home Office (SOHO) market segment.

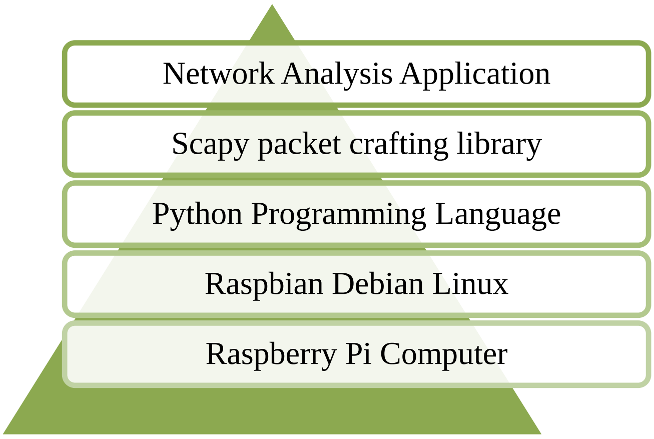

Network Analysis Application
Scapy packet crafting library
Python Programming Language
Raspbian Debian Linux
Raspberry Pi Computer

Fig. 3.5 The software and hardware stack of the monitoring solution [69]

Cyber attackers were analyzed in subchapter 3.2. We made a classification of them and described the characteristic profile, the main attributes and the specifics of their targets. Next, for a better understanding of the behavior and tools used by attackers and to study the complexity of the techniques, tactics and procedures used in cyber-attacks, we designed and implemented a honeynet. After analyzing several industries and assessing the risks in each of them, we turned our attention to the e-learning environment.

Universities are the birthplace of research and development, but they are also high-value targets for malicious actors.

In subchapter 3.3 we conducted a research [78] on collecting information on actors launching attacks against e-learning platforms, in order to complete the profiles of these attackers. A honeypot is a system (computer or network) that aims to detect and divert attackers by attracting them to the network. The importance of deploying honeypot points to understand the attackers of e-learning platforms was studied by implementing honeypots in a public cloud environment. Thus, we have developed a honeynet infrastructure based on 3 geographical regions: North America, Europe and Asia, consisting of low-interaction and high-interaction research honeypots to understand the tactics of attackers. After analyzing the data collected, the conclusions are that this type of research is extremely relevant to understand the current and future state of cybersecurity in the e-learning environment.

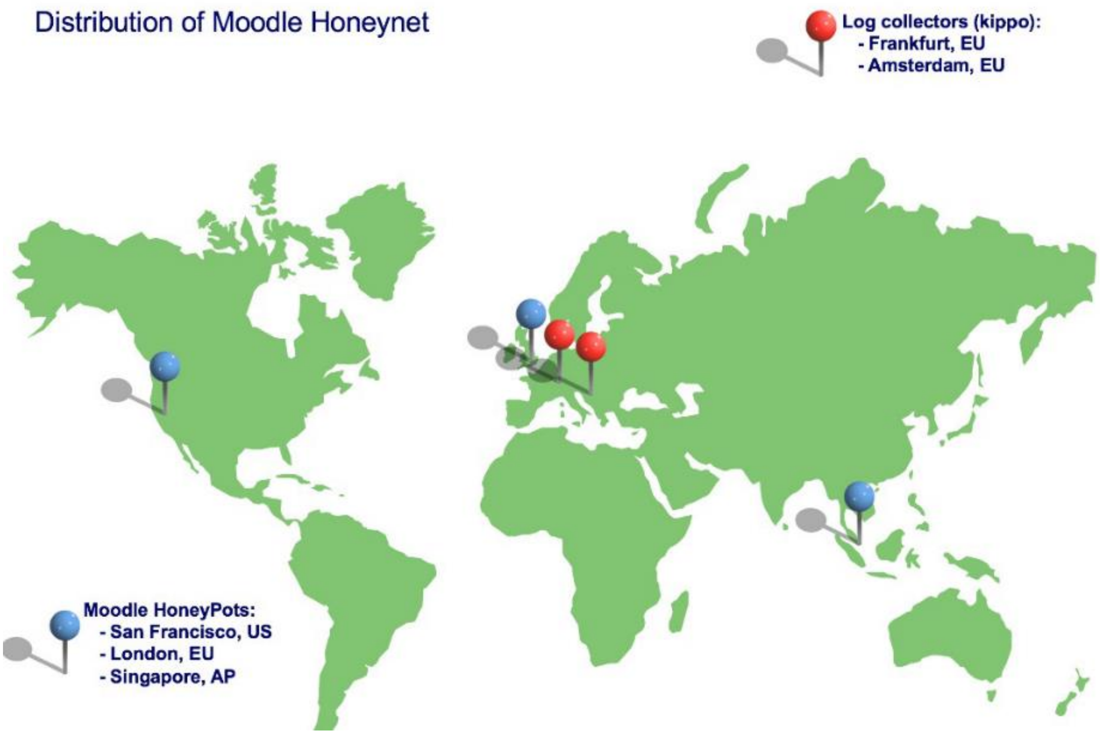
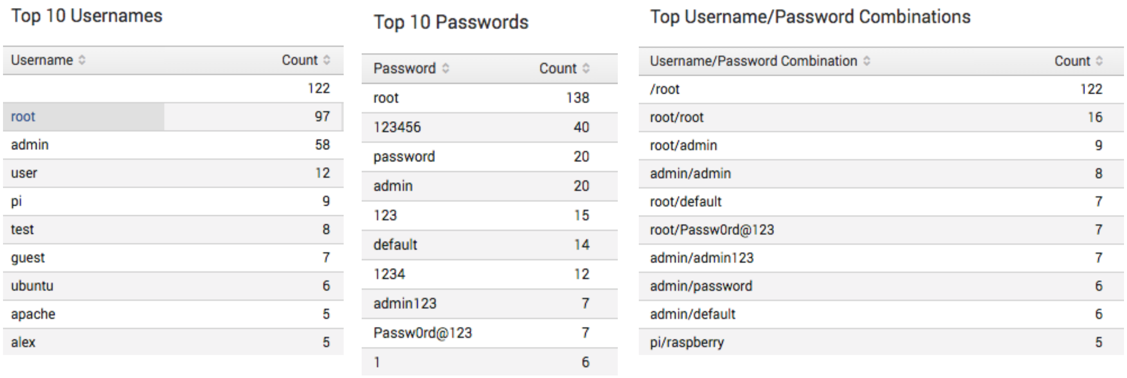


Fig. 3.8 Honeypot map [78]



Top 10 Usernames

Username ⇕	Count ⇕
	122
root	97
admin	58
user	12
pi	9
test	8
guest	7
ubuntu	6
apache	5
alex	5

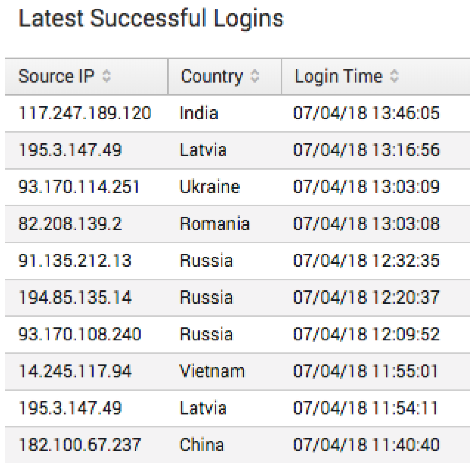
Top 10 Passwords

Password ⇕	Count ⇕
root	138
123456	40
password	20
admin	20
123	15
default	14
1234	12
admin123	7
Passw0rd@123	7
1	6

Top Username/Password Combinations

Username/Password Combination ⇕	Count ⇕
/root	122
root/root	16
root/admin	9
admin/admin	8
root/default	7
root/Passw0rd@123	7
admin/admin123	7
admin/password	6
admin/default	6
pi/raspberry	5

Fig. 3.10 Information on usernames and passwords used by attackers [78]



Latest Successful Logins

Source IP	Country	Login Time
117.247.189.120	India	07/04/18 13:46:05
195.3.147.49	Latvia	07/04/18 13:16:56
93.170.114.251	Ukraine	07/04/18 13:03:09
82.208.139.2	Romania	07/04/18 13:03:08
91.135.212.13	Russia	07/04/18 12:32:35
194.85.135.14	Russia	07/04/18 12:20:37
93.170.108.240	Russia	07/04/18 12:09:52
14.245.117.94	Vietnam	07/04/18 11:55:01
195.3.147.49	Latvia	07/04/18 11:54:11
182.100.67.237	China	07/04/18 11:40:40

Fig. 3.11 Database for logins monitoring [78]

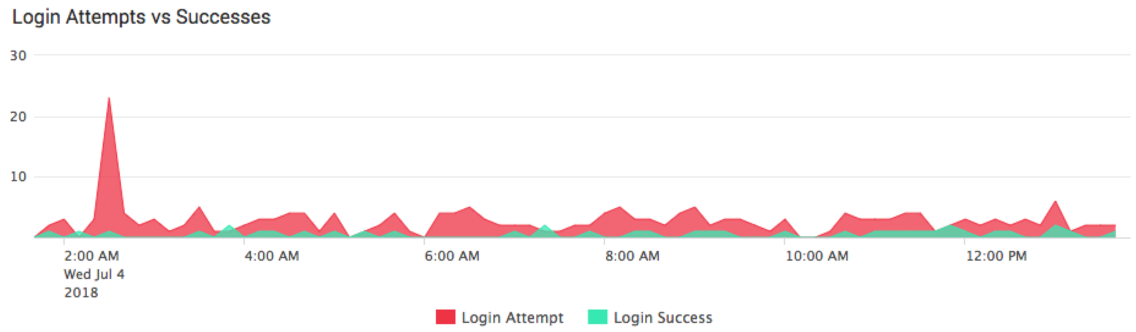


Fig. 3.12 Information on successful / unsuccessful connections of attackers [78]

Vulnerabilities of information systems, discussed in subchapter 3.4, is a wide topic that can be talked about a lot and what is even more interesting is that there will always be something new that will test the attackers, but also the security staff. Studies regarding the future of information systems vulnerabilities refer to mobile devices that are growing in use. Even if mobile devices are perceived as the number one threat for the current period, the devices themselves are not a risk, but important data that they can store or how to use them as a ramp to launch new attacks.

After a classification of vulnerabilities and the presentation of the 6 steps in their management, we studied in detail and made two contributions regarding vulnerabilities such as Buffer Overflow and Heartbleed. For the first case, we presented a Buffer Overflow attack on a vulnerable application - FreeFloat FTP Server. "The attacker used basic concepts from programming and networking to gain access to the target machine. From the point of view of offensive security, we analyzed the attack on an FTP server, which led to obtaining rights over the target system using free software tools, to which anyone can access. It is obvious that attacks on computer systems can be very complex, but, as we have shown, such attack can be carried out without much effort, which shows that an attacker does not necessarily have to be highly trained, and the support he needs is minimal" [84].

Subchapter 3.4.2 addressed the issue of Heartbleed computer vulnerability, a bug that left many private keys and other sensitive information available on the Internet.

Considering the long exposure, the ease of operation and the attacks that leave no trace, this vulnerability must be considered extremely dangerous. As a case study of this vulnerability, we simulated a Heartbleed attack on a machine (a Linux image for the ARM architecture installed on a Raspberry Pi device). The attack was launched from a virtual machine running Kali Linux using the NMAP network scanner and other scripts written in Python programming language. Due to encrypted requests, the difference between legitimate use and an attack cannot be based on their content, but by comparing the size of the request with the size of the response. This implies that an IDS / IPS can be programmed to detect the attack, but to block it is necessary to completely block the verification. The Heartbleed vulnerability patch is just a first step in securing systems and applications. In practice, after applying the patches, it is necessary to generate a new pair of public / private keys.

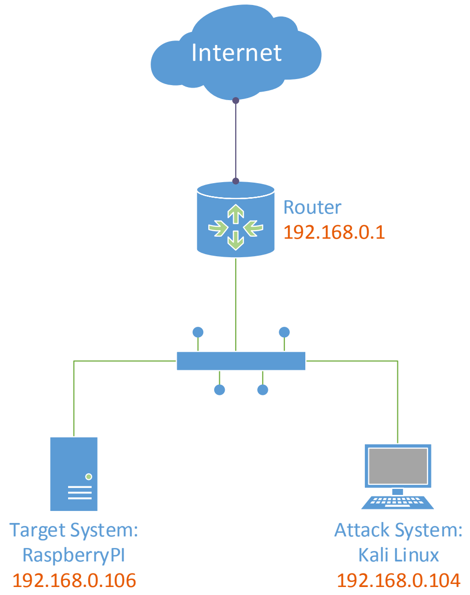


Fig. 3.21 Proposed configuration for implementing a Heartbleed attack [95]

At the end of the chapter we made a series of assessments regarding two types of current threats, with certain prospects of increasing complexity and which are announced to have new devastating effects: Advanced Persistent Threats (APT) and ransomware [102] [111]. APT, with a complex level of action and sophisticated techniques, attacks especially large organizations or state institutions, requiring intelligence-based cyber defense, collecting threat information combined with the correct interpretation of IoC indicators on system compromise. The danger of attacks launched by ransomware applications is currently on an upward trend, using advanced encryption algorithms and keys of increasing lengths.

The original contributions explained at the end of chapter consisted of proposing two useful solutions in preventing attacks launched by ransomware applications. The first solution is the static detection of these applications, uses a Python script and is based on a low-cost hardware infrastructure running standardized open-source technologies, with the main advantages of fast execution and a wide range of potential users.

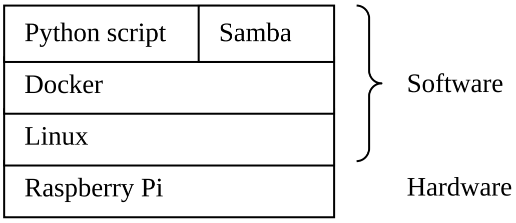


Fig. 3.27 Technology stack proposed to ransomware detection [112]

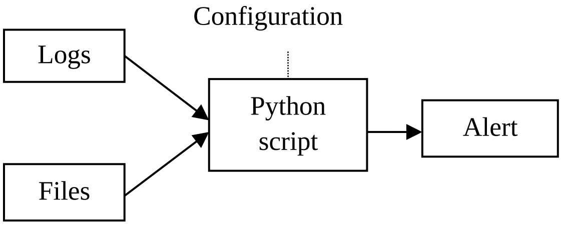


Fig. 3.28 Logic diagram for Python detection module [112]

Later, we developed the architecture of a dynamic solution for detecting and analyzing ransomware applications based on behavioral analysis of malware.

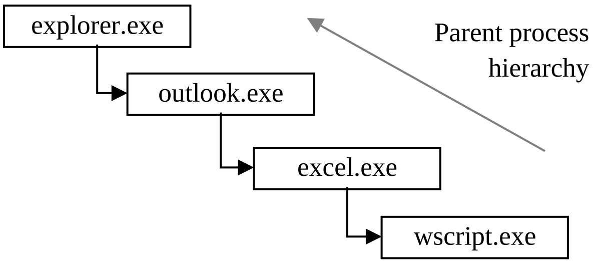


Fig. 3.33 Process hierarchy [103]

One of the ways to use the intelligent system presented in the subchapter 3.5.4 would be as a basic component of an antivirus solution, which could be integrated to monitor newly created processes and to provide data to the other major components of the antivirus. Another way to use the application would be during the malware analysis process. If Sysmon is installed on a computer or there is an image of the volatile memory of the computer, they can be used as inputs to the application and analyzed based on safe / malware patterns. For large computing networks, the intelligent system can be run simultaneously on multiple computers; in this case a global management console is required so that the results can be centralized and analyzed. The result should provide a perspective on the safe, suspicious or malicious behavior of the whole group of computers by monitoring trends in process execution.

Chapter 4. Cyber security strategies

Chapter 4, entitled "Cyber security strategies", analyzes theoretical models and makes practical contributions in the field of techniques that improve the security of complex systems approached from several points of view, both physically and logically.

The first part of the chapter is dedicated to theoretical models for implementing and analyzing the security of information systems. The analysis of multi-level models involved the breakdown of the concept of security into physical and logical levels and their individual description. These two levels are key elements and an effective security involves ensuring both levels: physical security (unauthorized access to equipment) and logical security (operating system access, security of services, etc.).

The purpose of an IT security audit of information systems is to fully identify the vulnerabilities, to assess its needs, to know the risk to which it is subject and to provide a solution to eliminate the vulnerabilities. One of the practical policies to reduce risks is to limit or eliminate unnecessary user rights, while keeping the minimum privileges for an access account (least privileged user account).

Further is presented Cyber Kill Chain model, a traditional security model that describes a classic scenario - an outside attacker who follows a few well-defined steps to break into a network and steal data - breaking down the attack steps to help organizations to prepare. Cyber Kill Chain describes in a remarkable way the vectors of threat and the attacks that current organizations are facing.

Developed by Lockheed Martin's CSIRT (Computer Security Incident Response Team), the purpose of the Cyber Kill Chain model is to better understand the stages by which an attacker develops an attack and to help security teams stop this attack in any of the identified stages. Subchapter 4.2 describes the three main stages of the model (pre-compromise, compromise and post-compromise) and details the component stages (phases) of each. The attacker performs reconnaissance, intrusion into the security perimeter, exploitation of vulnerabilities, obtaining and escalating privileges, lateral movement to gain access to more valuable targets, tries to provide activity and, finally, extract data from the organization.

Application of the principle of layered security (Defense in Depth) presented in subchapter 4.3 has as main purpose the achievement of multilevel data protection, both at rest and in transit [128]. The purpose of this technique is not necessarily to prevent security breaches, but rather to delay the actions of an attacker, so that the victim (usually an organization) gains time to identify and respond to a cyber-attack. A computer network cannot be protected by a single security measure. Cyber-attacks have evolved dramatically in the last two decades. Social engineering, threats from inside of organizations and cloud technology have changed the way we define the security perimeter and, according to some opinions, have made its definition irrelevant. A firewall protects the network from outside attacks but is not effective when attacks come from inside. The implementation of security policies and connections control procedures will also be ignored by an attack from outside the network.

In this context, one of the key concepts in ensuring information security is the principle of Defense in Depth, i.e. the establishment of a multilayer defense system using independent methods (ensuring multi-level security) that can:

- prevent the exploits;
- detect and intercept the attack;
- find out the threat agents and the consequences of an attack.

A successful approach involves the introduction of several security barriers to ensure protection against various types of threats. Thus, in this subchapter we have illustrated an overview of this defense in depth technique applied according to the risk analysis performed in Chapter 2 to ensure data security. We detailed examples of "layers" of protection and presented, by categories, the measures to be taken at the level of a company for an effective and solid defense in depth. The basic elements for applying defense in depth within an organization are human resources (employees), technology (hardware and software) and the level of operation (periodic monitoring / updating activities, but also incident recovery).

Ensuring the security of information systems consists not only in the acquisition of powerful hardware or modern software. At the organizational level, a strong and coherent policy is needed to control access to data and implement strategies that ensure data security, regardless of the technology used. At the level of the employee's individual consciousness, reflexes must be formed to minimize security breaches and ensure data security and confidentiality: carefully accessing links, ignoring programs or applications from uncertain sources, complex and different passwords. A personal contribution in this chapter was the development of a program for extracting insecure passwords using the crypt() function and a dictionary brute-force type attack.

In subchapter 4.5 we developed a system for detecting intruders in a LAN. First, we presented the hardware and software environment in which this application was implemented. The hardware support consisted of a recent generation Raspberry Pi model, chosen due to its low costs and high performance, suitable for the specifics of the application and the required computing power. The Python programming language was chosen because of its advantages (open-source, versatile, easy to use and with many libraries included).

In subchapter 4.5.2 we compared the solutions offered by the cloud computing environment and we presented specific aspects to the Top 3 leaders on the online cloud services market: Amazon Web Services, Microsoft Azure and Google Cloud. Each vendor comes with advantages and disadvantages, so the optimal solution must be chosen according to the specifics of each organization, service needs, and the price correlated with the need for hardware and software resources offered. Several aspects need to be considered when determining the cloud deployment model for a organization. The criteria addressed may be the need to comply with the organization's regulations, financial resources, preferred spending pattern, geographical locations of users or predictability of demand. Not all cloud models can address these requirements equally, and the criteria analyzed are an initial guide for determining whether a private, public, hybrid, or community cloud is best for the organization in question.

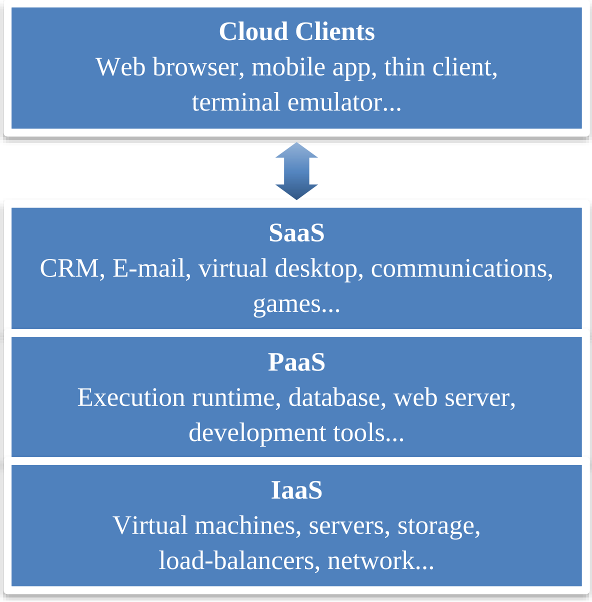

Cloud Clients
Web browser, mobile app, thin client, terminal emulator...
SaaS
CRM, E-mail, virtual desktop, communications, games...
PaaS
Execution runtime, database, web server, development tools...
IaaS
Virtual machines, servers, storage, load-balancers, network...

Fig. 4.7 Cloud computing service models [149]

Intrusion detection solutions, currently available on the market, aim to protect large networks and are highly priced. The open source solution for small LANs, designed in the subchapter 4.5.3, has the capabilities to detect intrusion into the local network by analyzing IP addresses [159]. Configured to work manually or automatically, this software builds a basic reference list and constantly compares its elements with the existing IPs in the network. When an anomaly occurs, it alerts the administrator and provides also the ability to determine the open ports and vulnerabilities of that equipment. The proposed solution ("*Network Mapper*") is based on free and open source technologies. The purpose of designing a solution with very low computing resource requirements is that the software layer can be ported to consumer networking equipment, such as routers designed for home and small offices, providing ransomware detection capabilities that complement the antivirus solution.

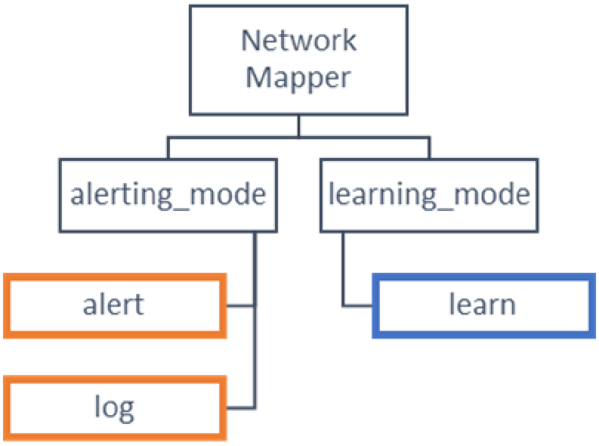


Fig. 4.8 Network Mapper - working modes [159]

Chapter 5. Final conclusions

The last chapter contains the synthesis of the aspects presented in this work and the list of original contributions, respectively of the papers published during the doctoral programme. I indicated the activities that I carried out during the doctoral programme and identified some further directions in which the contributions could be developed. At the end of the chapter we made an analysis of the complex context generated by the current coronavirus pandemic and we estimated both the attack vectors specific to the next period and the priorities to which organizations will have to pay maximum attention in order to resume and adapt activities to a "new normal".

5.1. Main aspects presented in the thesis

The original results obtained during this doctoral studies can be considered both from an engineering point of view, through a series of technical contributions in the scientific field of the topic, and from a managerial perspective, by proposing and implementing a cyber security program for optimizing the activity of a large multinational organization.

The main objective of the doctoral thesis was to develop a series of compatible and eligible products for the cyber security of the future by studying cyber-attacks and their evolution to understand the impact of a proactive approach compared to a reactive approach. The secondary objectives were the elaboration of theoretical, comparative analyzes, and the design of hardware configurations and software applications aimed to minimize the impact of cyber-attacks and optimize costs within some organizations.

Chapter 2 of the paper addresses the issue of information security presented at the theoretical level of the concepts involved, standards and regulations on information security, security risk management and security policies within organizations. At the beginning of the chapter we described the general concepts of system and dependability of a system, the latter representing the characteristic of a system through which it provides with confidence the service for which it was designed, avoiding more frequent or severe failures than an acceptable considered level. We have detailed the basic components of dependability, focusing on three of them - confidentiality, integrity and availability, which are essential in ensuring information security.

Next, in subchapter 2.2 we have analyzed some relevant standards and regulations in the field of information security:

- ISO/IEC 27001:2013, a standard specifying "the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature." [24];
- NIST Cybersecurity Framework, a framework that "integrates industry standards and best practices to help organizations manage their cybersecurity

risks. It provides a common language that allows staff at all levels within an organization - and at all points in a supply chain - to develop a shared understanding of their cybersecurity risks." [29];

- two regulations for the protection of users' personal data: GDPR (for the European Union and the European Economic Area) and CCPA for the State of California (United States), comparatively studied and highlighting the measures taken to protect the confidential data of the individual (consumer), his rights and obligations, but also those of companies, in the relations of mutual interaction;
- IoT standardization activities (in different stages of work) initiated by several international organizations in order to ensure a common language for addressing the challenges in the field of cyber security targeting IoT devices.

From the point of view of approaching risk management from several perspectives, considered throughout the doctoral programme, we studied the evolution of cyber-attacks, developed and applied a framework for defining and analyzing cyber security risk at the organizational level. Thus, we defined and implemented a cyber security management department and a program within some companies and especially within a merger of two global companies by applying the method of layered defense (Defense in Depth). We particularly studied the implications and vulnerabilities that such a merger - between a PCI DSS (Payment Card Industry Data Security Standard) and SOX (Sarbanes-Oxley Act) certified company and a company that only adheres to a few cyber security implementation practices - has for the resulting organization. We thus identified several risk points and, following the technical assessments, developed a methodology and created an analysis matrix based on the Eisenhower method of concentrating efforts, presented in the subchapter 2.3.1. We concluded that a proactive scenario-based approach and event anticipation had a higher success rate in reducing the attack area and the costs of cyber incidents.

From a technical point of view, we aimed to design, develop and implement solutions to go through the process of converting data to wisdom. One method of extracting the necessary data was to conduct a cybersecurity awareness questionnaire within some organizations, in order to obtain information and knowledge on the main risk areas in terms of staff employed. In Annex A.1 we presented in extenso this questionnaire consisting of 20 questions, and each possible answer was assigned an original risk coefficient with values between 1 (minimum security risk) and 10 (maximum security risk). Using the explanations and the procedure for calculating the general score indicated in subchapter 2.4.2, an organization can determine the level of awareness of information security at the level of the human component - employees - and can improve its value through information, awareness and training programs for employees, by developing good practice guidelines or within internal security policies.

From an organizational point of view, in subchapter 2.4.3 we conducted a comparative study on the impact and results of SOC and SIC security centers and, based on this analysis, redefined the sub-departments within the security department of an organization. Also, in subchapter 2.4.4, developing the professional profile of the cybersecurity analyst, we determined the needs in terms of human resources and defined the levels of professional development for employees.

Chapter 3 presents the main categories of cyber security threats, and for each of them we highlighted the relevant aspects and made original contributions at a theoretical and / or practical level (hardware / software). Cyber-attacks were classified according to several basic criteria: type of threat, mode of action, intent, origin or target. Also relevant are the tools used in carrying out an attack and the level of access obtained from a successful attack. The main categories of threats (malware, phishing, SQL injection, XSS, DoS, Session Hijacking, Man-in-the-Middle or reuse of credentials) were presented in detail, after which we performed an analysis of the most important cyber security breaches in recent history, noting that not only the number of these incidents has increased, but in particular the value of the impact on both organizations and users affected by confidential data leaks.

A type of attack I insisted on in subchapter 3.1.3 was the ARP spoofing. After a technical presentation of this attack, we proposed a solution for detecting ARP spoofing attacks using a hardware platform based on Raspberry Pi and Linux operating system as a monitoring device that will be connected to a SPAN port of a smart switch via which all network traffic will be copied and sent for analysis. The script, written in Python, detects scanning activities (by querying IP addresses on a local network), being effective for small LANs (SOHOs), but limited due to the network interface at 100 Mb/s. The presented solution acts at the level of the Reconnaissance stage within the Cyber Kill Chain model (later developed in Chapter 4) because the network scan is equivalent to the activity in which the attacker gathers information about existing devices in the network.

In subchapter 3.2 we analyzed the profiles, attributes and motivations of cyber attackers. According to statistics for the first part of 2020, cybercrime remained in first place (86.6%) in the top of the motivations behind the attacks, which led to the conclusion that cyber attackers who have mainly economic (financial) or destructive purposes are the most active in this market. Such attackers possess advanced attributes, such as a high level of knowledge, and rely on increased aggression and fine techniques (e.g. social engineering) to achieve their goal.

The realization of the portrait of cyber attackers based on the criteria set out above is complemented by the original contribution found in the subchapter 3.3. In order to collect and centralize data on cyber-attacks targeting e-learning systems (Moodle platforms), we designed a honeynet network architecture initially implemented in local systems (Raspberry Pi), then using a cloud infrastructure, and few research honeypots strategically placed in 3 geographic regions: North America, Europe and Asia. We also developed an application that collected and aggregated attacker data (IP addresses, passwords and usernames used in attacks) related to the versions and vulnerabilities of the e-learning platforms used. From the analysis of these data we obtained information, knowledge and intelligence about attackers in order to understand their ways of attack and the objectives pursued. The results of this study can be used as IoC rules in intrusion detection and prevention systems.

A very important category of cyber security threats are vulnerabilities, which are those weaknesses (hardware or software) in an information system that attackers can exploit in order to violate established security policies and conduct operations without had the necessary access rights. Thus, in subchapter 3.4 we have detailed and tested two types of software vulnerabilities: Buffer Overflow (for which we simulated an attack that used this vulnerability, presented in Annex A.2) and Heartbleed (together with the proposal of a hardware configuration used to implement an attack that exploited this bug). Following the study of the technical aspects of these vulnerabilities and attack simulations - performed locally (within the laboratory's LAN) and based on virtual machines and open source applications, chosen due to their costs and scalability - knowledge was obtained, with which we assessed the consequences of these types of exploits.

Subchapter 3.5 of this work presents two of the current types of cyber threats with the most dangerous effects: APT and ransomware malware. From the point of view of information security, APT is the most important factor of the current information technology environment due to the use of extremely sophisticated techniques that allow them to act for a long time without being detected. On the other hand, one of the current challenges in cybersecurity is ransomware, which encrypts files on the system's hard drive and requires a ransom. Next, we proposed two solutions for detecting malware attacks aimed at obtaining financial benefits: a static detection, by developing an original Python script on a low-cost hardware infrastructure running standardized open source technologies (in subchapter 3.5.3), respectively a dynamic solution based on the behavioral analysis of the malware (in subchapter 3.5.4). The intelligent system could serve as a component of an antivirus application, it can be integrated to monitor newly created processes and provides data to other components of the antivirus. However, the dynamic solution is in an early stage of development, requiring further research and study of several proposed ideas (these further developments are indicated in subchapter 5.4).

Chapter 4 begins with theoretical approaches on implementation models, analysis and information security. We have presented in detail two models: Cyber Kill Chain and Defense in Depth. The Cyber Kill Chain model is a traditional security model structured in 3 stages (pre-compromise, effective compromise and post-compromise), which in turn consists of a total of 7 stages. The role of such a model is to break down the steps of an attack (cyber-attack in the case of this analysis) and help organizations defend themselves against threat vectors.

The main purpose of the Defense in Depth model is not necessarily to prevent security breaches, but rather to delay the actions of an attacker, so that the victim organization gains time to identify and respond to a cyber-attack. Layered security introduces several security barriers to ensure protection against various types of threats. One of these layers of protection can be represented by authentication techniques (passwords, tokens or biometric data). Using the results of the questionnaire in Annex A.1 regarding the used passwords (complexity, safety measures, degree of reuse, etc.) we made in subchapter 4.3.2 an application used to verify the level of security provided by passwords. This application exploits vulnerabilities in the encryption process by simulating a dictionary brute-force type attack.

Another protection layer in the Defense in Depth model is the detection of activities that would lead to security breaches, and such an intrusion detection system has been developed in the subchapter 4.5. First, we analyzed the opportunities offered by the implementation of a software solution designed and developed on ARM hardware architectures based on a Raspberry Pi system (subchapter 4.5.1). Next, the software solution was implemented in a cloud computing infrastructure, analyzing and comparing the advantages and limitations of such approaches compared to developments on low-cost hardware configurations (Raspberry Pi systems, SOHO local networks). In order to implement the online solutions, we made in subchapter 4.5.2 a critical study on the dependability of cloud computing platforms with a special emphasis on the cost / benefit ratio from the perspective of fundamental concepts in information security: confidentiality, integrity, availability. Finally, the proposed system for detecting intrusions within small LANs (conceptually presented in subchapter 4.5.3 and extended in Annex A.3) is intended to mitigate Man-in-the-middle attacks. The advantages of this solution are the use of free and open source technologies, very low computing resources and, finally, it is portable on other network equipment.

5.2. Original contributions

Below I briefly present the list of original contributions in the PhD thesis. These, together with the prospects for further development, are a foundation for reducing the cyber security risk due the vulnerabilities of present and future information systems. In addition to information systems, the adaptation and realignment of a cyber security risk management program is critical in the context in which the work environment and infrastructure are being redefined as a result of the COVID-19 pandemic. I appreciate that these measures will have to be considered from now on, for a proactive attitude in addressing current and future cyber security risks and ensuring business continuity.

1. We have developed and applied a framework for defining and analyzing cybersecurity risk within a global company that develops and licenses technology and intellectual property in areas such as ICT (Information and Communication Technology), artificial intelligence, audio / video, integrated circuits and automotive industry.

2. We defined and implemented a cybersecurity program and a management department within a merger of two global companies by applying the layered defense method. We organized over 100 one on one interviews and team meetings with colleagues from a wide range of roles and responsibilities, from engineers involved in product design and development, infrastructure and systems architects, as well as and leaders of testing, development, human resources and finance departments. Following both the technical and organizational evaluation, we proposed a matrix based on the Eisenhower method of risk reduction, an annual budget for technological integration, investments in technologies and personnel, and we took over a team within the CFO-led department.

3. We designed a questionnaire on cybersecurity awareness within an organization to determine the main areas of risk from the point of view of employees, knowing that the most vulnerable area of attack within organizations is the human component. The results obtained from the dissemination of this questionnaire contributed to the improvement of the security program within the considered organization and the development of good practice guides for other similar organizations operating in the ICT industry.

4. We conducted a comparative study on the impact and results of cyber security centers such as SOC (Security Operations Center) and SIC (Security Intelligence Center). This study resulted in redefining the sub-departments within the security department as we concluded that an implementation based on the analysis of measurements and intelligence collected by various methods has a higher success rate in reducing the attack area and the cost generated by incidents. This is due to the proactive scenario-based approach and anticipation of cybersecurity events versus the reactive approach based on waiting and responding to information security incidents [B1] [C5].

5. We developed a professional profile of the cybersecurity analyst to determine the human resources needs within the security department and defined career development stages for employees [B4].

6. We developed an cyber-attack and attackers analysis system based on a network of honeypots implemented both in local systems (such as Raspberry Pi) and in various geographical areas by using computational capacity of the cloud computing as a step in the application of the Cyber Kill Chain model [A2].

7. We conducted a study on the technical aspects and impact of the Heartbleed vulnerability, in which we assessed the consequences of its exploitation, as well as the response of global companies to reduce exposure to this vulnerability by testing using laboratory LAN and by monitoring the resources available online containing information about the responses to this event [B3].

8. We studied the implications and vulnerabilities that a merger between a PCI DSS and SOX certified company and a company that only adheres to a few cyber security implementation practices has for the resulting organization. We thus identified several risk zones and designed and implemented a management program to reduce the attack area.

9. We developed the architecture of a dynamic solution for detecting and analyzing ransomware by implementing the knowledge gained after graduating from the Machine Learning course (at the University of Washington) [A4].

10. We developed a system for detecting intruders and intrusions as a layer in the Defense in Depth model to determine the necessary in terms of monitoring and response to security events. This program was the most important step in understanding the ecosystem to be protected [A1] [B2] [C4].

11. We developed a static detection solution following the analysis of the impact of malware applications aimed at obtaining financial benefits [B5] [B6]. The solution consists of an original Python script [A6] and uses a low-cost hardware infrastructure that runs standardized open source technologies, making it both fast and accessible to the general public.

12. We conducted a critical study on the dependability of cloud computing platforms [C3] and placed a special emphasis on the analysis of cost / benefit options in terms of the main concepts of IT security: confidentiality, integrity and availability of data.

13. We developed a program and an architecture for collecting and centralizing data on cyber-attacks using honeypot endpoints built as a basis for Moodle e-learning platforms [A2] [A3]. Thus, a honeynet was defined and implemented using a cloud infrastructure and the data of the attackers (IP addresses, passwords and usernames used in the attacks) were analyzed correlated with the versions and vulnerabilities of the e-learning platforms used.

14. We applied "Cyber Kill Chain" method of analyzing cyber-attacks and proposed a solution to counter ARP spoofing attacks [B7].

15. Using a suite of open source applications, chosen due to their costs and scalability, we studied the impact of the Buffer Overflow cyber-attack by simulating it in the laboratory infrastructure [C1].

16. We designed and developed a Python script that check the security level of passwords, which exploits vulnerabilities in the encryption process by simulating a dictionary brute-force attack type [C2].

17. We implemented software solutions designed and developed on ARM hardware architectures using Raspberry Pi platforms and a cloud computing infrastructure, analyzing and comparatively presenting the advantages and limitations of such approaches.

5.3. Activity during the doctoral programme

The following is a summary of my work during my doctoral programme: the papers published within scientific conferences or journals, the results obtained after participating in the programme POSDRU/159/1.5/S/132397 "*Excellence in research through doctoral and postdoctoral scholarship*" (ExcelDOC) and other relevant activities in the field of doctoral thesis.

These were key elements that allowed me not only to complete my PhD dissertation and the entire internship, but also made an essential contribution to improving my personal expertise in cybersec and my professional development as a specialist in the field, both technically as well as managerially.

5.3.1. List of published papers

A. Scientific papers in publications indexed ISI / IEEE Xplore

A1. I.D. Barbu, C. Pascariu, I.C. Bacivarov, S.D. Axinte, M. Firoiu, *Intruder monitoring system for local networks using Python*, 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Jun 29 - Jul 01, 2017, eISBN 978-1-5090-6458-8, doi: 10.1109/ECAI.2017.8166457, WOS: 000425865900073

A2. I.D. Barbu, G. Petrică, S.D. Axinte, I. Bacivarov, *Analyzing cyber threat actors of e-learning platforms by the use of a honeynet cloud based infrastructure*, Proc. of the 13th International Scientific Conference "eLearning and Software for Education", Bucharest, 2017, Vol. 3, pp. 352-357, doi: 10.12753/2066-026X-17-226

A3. G. Petrică, **I.D. Barbu**, S.D. Axinte, I. Bacivarov, I.C. Mihai, *E-learning platforms identity using digital certificates*, Proc. of the 13th International Scientific Conference "eLearning and Software for Education" Bucharest, 2017, Vol. 3, pp. 366-373, doi: 10.12753/2066-026X-17-228

A4. C. Pascariu, **I.D. Barbu**, *Dynamic analysis of malware using artificial neural networks. Applying Machine Learning to identify malicious behavior based on parent process hierarchy*, 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Jun 29 - Jul 01, 2017, eISBN 978-1-5090-6458-8, doi: 10.1109/ECAI.2017.8166505, WOS: 000425865900121

A5. G. Petrică, **I.D. Barbu**, S.D. Axinte, C. Pascariu, *Reliability analysis of a web server by FTA method*, The 10th International Symposium on Advanced Topics in Electrical Engineering (ATEE), Bucharest, 2017, pp. 683-686, doi: 10.1109/ATEE.2017.7905101, WOS: 000403399400133

A6. C. Pascariu, **I.D. Barbu**, *Ransomware honeypot. Honeypot solution designed to detect a ransomware infection identify the ransomware family*, 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, June 27-29, 2019, eISBN 978-1-7281-1624-2, doi: 10.1109/ECAI46879.2019.9042158

B. Scientific papers in publications indexed in international databases

B1. I.D. Barbu, C. Pascariu, I.C. Bacivarov, *Migration of a SOC to SIC. Security Operations Center vs. Security Intelligence Center. The use of honeypots for threat intelligence*, Proc. of the 15th International Conference on Quality and Dependability Sinaia, Romania, September 14th-16th, 2016, pp. 150-155, ISSN 1842-3566

B2. I.D. Barbu, G. Petrică, *Defense in Depth principle to ensure information security*, IJISC - International Journal of Information Security and Cybercrime, Vol. 4, No. 1, 2015, pp. 41-46, doi: 10.19107/IJISC.2015.01.06
B3. I.D. Barbu, I.C. Bacivarov, *The Heartbleed bug - a vulnerability in the OpenSSL cryptographic library*, Proc. of the 14th International Conference on Quality and Dependability Sinaia, Romania, September 17th-19th, 2014, pp. 100-109, ISSN 1842-3566
B4. I.D. Barbu, C. Pascariu, *Information security analyst profile*, IJISC - International Journal of Information Security and Cybercrime, Vol. 3, No. 1, 2014, pp. 29-36, doi: 10.19107/IJISC.2014.01.03
B5. C. Pascariu, **I.D. Barbu**, I.C. Bacivarov, *WannaCry ransomware analysis. 1 day, 150 countries, >57k infected computers*, Asigurarea Calității - Quality Assurance, Anul XXIII, Numărul 90, Aprilie-Iunie 2017, pag. 4-7, ISSN 1224-5410
B6. C. Pascariu, **I.D. Barbu**, *Ransomware - an emerging threat*, IJISC - International Journal of Information Security and Cybercrime, Vol. 4, No. 2, 2015, pp. 27-32, doi: 10.19107/IJISC.2015.02.03
B7. C. Pascariu, **I.D. Barbu**, I.C. Bacivarov, *Network security monitoring with embedded platforms*, Proc. of the 16th International Conference on Quality and Dependability Sinaia, Romania, September 26th-28th, 2018, pp. 243-246, ISSN 1842-3566

C. Scientific reports during doctoral programme

C1. Scientific report 1, June 2014: *Buffer Overflow vulnerability exploitation using open-source tools*
C2. Scientific report 2, December 2014: *Studiul metodelor de programare utilizând Python în vederea dezvoltării unui program de verificare a parolelor*
C3. Scientific report 3, June 2015: *Studiul programelor de tip OpenStack în vederea implementării în sistemul de securitate dezvoltat. Studiu comparativ între securitatea informațiilor on premise sau în cloud*
C4. Scientific report 4, December 2015: *Intruder monitoring system for local networks using Python*
C5. Scientific report 5, June 2016: *Studiu comparativ între implementarea unui centru de securitate cibernetică de tip SOC (Security Operations Center) și SIC (Security Intelligence Center)*

5.3.2. POSDRU/159/1.5/S/132397 programme

Between April 2014 and December 2015, I participated in the programme POSDRU/159/1.5/S/132397 "*Excellence in research through doctoral and postdoctoral scholarship*" (ExcelDOC). The general objective of this programme was to "increase the competitiveness and professional performance of future PhDs and researchers who have obtained a PhD in science, through participation and active involvement in doctoral and postdoctoral programs, contributing to the development of a body of expert researchers able to take an interdisciplinary approach in the field of research, development and innovation" [160].

5.3.3. Other activities in the field of doctoral thesis

Participation in events

1. I have participated in international scientific conferences "International Symposium on Advanced Topics in Electrical Engineering" (2017), "eLearning and Software for Education Conference" (2017), "Electronics, Computers and Artificial Intelligence" (2017, 2019), "Quality and Dependability" (2014, 2016, 2018).
2. I attended Annual Symposium of Doctoral School of Electronics, Telecommunications and Information Technology, 1st edition (2018).
3. I have been actively involved in the field of cybersecurity by:
- creating teams and communities;
- supporting education and training at national / international level;
- organizing events for the general public (BSidesBucharest, OWASP Romania conferences, several hackathons and workshops), academic field and business environment (presentations of products, services, technologies).

Other published papers

1. In IJISC - International Journal of Information Security and Cybercrime - reviews of cybersecurity events I attended as a speaker or guest (Black Hat USA, Defcamp, OWASP, BSides, SPARKS).
2. I have made an active contribution to improving the cybersecurity culture by developing studies and analyzes on cybersecurity, disseminated through personal website or published on specialized websites (magazines, blogs, forums and technical communities).

References (selection)

[1] Marsh & Microsoft, 2019 Global Cyber Risk Perception Survey, Marsh LLC, 2019, https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf.

[2] World Economic Forum, The Global Risks Report 2020, http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

[3] K. Schwab, The Fourth Industrial Revolution. What It Means and How to Respond, Foreign Affairs, 2015, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.

[4] World Economic Forum, Wild Wide Web. Consequences of Digital Fragmentation, 2020, https://reports.weforum.org/global-risks-report-2020/wild-wide-web/.

[24] International Standard ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements, 2nd edition, 2013.

[29] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[39] B. McKay, K. McKay, The Eisenhower Decision Matrix: How to Distinguish Between Urgent and Important Tasks and Make Real Progress in Your Life, 2013, https://www.artofmanliness.com/articles/eisenhower-decision-matrix/.

[48] I.D. Barbu, C. Pascariu, I.C. Bacivarov, Migration of a SOC to SIC Security Operations Center vs. Security Intelligence Center. The use of honeypots for threat intelligence, Proceedings of the 15th International Conference on Quality and Dependability Sinaia, Romania, September 14th-16th, 2016, pp. 150-155, ISSN 1842-3566.

[49] I.D. Barbu, Studiu comparativ între implementarea unui centru de securitate cibernetică de tip SOC (Security Operations Center) şi SIC (Security Intelligence Center), Raportul ştiinţific nr. 5, iunie 2016.

[51] I.D. Barbu, C. Pascariu, Information Security Analyst Profile, IJISC - International Journal of Information Security and Cybercrime, Vol. 3, No. 1, 2014, pp. 29-36, doi: 10.19107/IJISC.2014.01.03.

[69] C. Pascariu, I.D. Barbu, I.C. Bacivarov, Network security monitoring with embedded platforms, Proceedings of the 16th International Conference on Quality and Dependability Sinaia, Romania, September 26th-28th, 2018, pp. 243-246, ISSN 1842-3566.

[78] I.D. Barbu, G. Petrică, S.D. Axinte, I. Bacivarov, Analyzing cyber threat actors of e-learning platforms by the use of a honeynet cloud based infrastructure, Proc. of the 13th International Scientific Conference „eLearning and Software for Education", Bucharest, 2017, Vol. 3, pp. 352-357, doi: 10.12753/2066-026X-17-226.

[84] I.D. Barbu, Buffer Overflow vulnerability exploitation using open-source tools, IJISC - International Journal of Information Security and Cybercrime, Vol. 2, No. 2, 2013, pp. 43-54, doi: 10.19107/IJISC.2013.02.05.

[95] I.D. Barbu, I.C. Bacivarov, The Heartbleed bug - a vulnerability in the OpenSSL cryptographic library, Proceedings of the 14th International Conference on Quality and Dependability Sinaia, Romania, September 17th-19th, 2014, pp. 100-109, ISSN 1842-3566.

[102] C. Pascariu, I.D. Barbu, I.C. Bacivarov, WannaCry Ransomware Analysis. 1 day, 150 countries, > 57k infected computers, Asigurarea Calităţii - Quality Assurance, Anul XXIII, Numărul 90, Aprilie-Iunie 2017, pag. 4-7, ISSN 1224-5410.

[103] C. Pascariu, I.D. Barbu, Dynamic analysis of malware using artificial neural networks Applying Machine Learning to identify malicious behavior based on parent process hierarchy, 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Jun 29 - Jul 01, 2017.

[111] C. Pascariu, I.D. Barbu, Ransomware - an emerging threat, IJISC - International Journal of Information Security and Cybercrime, Vol. 4, No. 2, 2015, pp. 27-32, doi: 10.19107/IJISC.2015.02.03

[112] C. Pascariu, I.D. Barbu, Ransomware honeypot. Honeypot solution designed to detect a ransomware infection identify the ransomware family, 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, June 27-29, 2019, eISBN 978-1-7281-1624-2, doi: 10.1109/ECAI46879.2019.9042158.

[128] I.D. Barbu, G. Petrică, Defense in Depth Principle to Ensure Information Security, IJISC - International Journal of Information Security and Cybercrime, Vol. 4, No. 1, 2015, pp. 41-46, doi: 10.19107/IJISC.2015.01.06.

[149] E. Gorelik, Cloud Computing Models, Working Paper CISL# 2013-01, MIT, 2013.

[159] I.D. Barbu, C. Pascariu, I.C. Bacivarov, S.D. Axinte, M. Firoiu, Intruder monitoring system for local networks using Python, 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Jun 29 - Jul 01, 2017.

[160] Proiectul POSDRU/159/1.5/S/132397 (ExcelDoc), http://cempdi.pub.ro/exceldoc/.