CYBERSECURITY: FROM PAST THREATS TO PRESENT SOLUTIONS

Pavel CIUMACENCO[*], Denis PLEȘCA, Ștefan ISTRATI

Department of Software Engineering and Automation, group FAF-232, Faculty of Computers, Informatics and Microelectronics, Technical University of Moldova, Chișinău, Republic of Moldova

*Corresponding author: Pavel Ciumacenco, pavel.ciumacenco@isa.utm.md

Abstract. *The development of cyber security has been prominent in the last couple of decades, it has met multiple obstacles and managed to detect new paths to overcome them. This article aims to provide research on the history and current innovations concerning cybersecurity topics, as nowadays it affects not only organizations but every person who has an electronic device. We achieve this by researching already existing articles and extracting ideas and information that would align with the main objective of our paper. By doing this, we managed to outline the historical progression of cyber security starting from the early computer viruses to the sophisticated intrusion systems. Also, we went through and gathered the most impactful and innovative creations in the cybersecurity field that combat a multitude of modern cyber threats. From what was said above, we conclude that this article highlights how cyber security evolved and adapted over years of existence, it underscores the importance of resilience in countering new threats and protecting digital assets.*

Keywords: *cyber-threat, database, internet, intrusion prevention system, technologies;*

Introduction

In today's world, the cyber world has become a popular and inevitable source of information, sharing not only personal activities but also professional ones including business, shopping, bank transactions, advertisements, services, etc. This exponential increase in the use of cyberspace has resulted in an exponential increase in cybercriminal schemes. Therefore, cybersecurity is one of the most important defenses against the constant flow of online threats in today's digital world, which is always growing. This article is meant to explore the development of Cybersecurity, tracing its evolution from the weaknesses of the past to modern solutions and security algorithms.

A Particular Examination of Cybersecurity

In a general condition, Cybersecurity is considered to be a subset of IT security. Cybersecurity aims to protect computer systems, networks, data, and digital infrastructure from cyber threats and attacks. To effectively achieve those, nowadays, the implementation of security measures such as access controls, encryption, and firewalls. In this section, we will attempt to give an inside view of how exactly Cybersecurity works. Brenner [1] points out that modern technologies change the way frauds are conducted, with them being far more difficult for law enforcement officers to detect, giving those offenders the possibility to commit crimes on a far broader scale than their real-world equivalents.

Cybersecurity operates on multiple fronts, combining various technical, procedural, and user-oriented strategies to reduce risks and protect digital assets. One of its main goals is to establish a robust defense mechanism against a wide range of cyber threats such as malware, phishing attacks, ransomware, and insider threats. In addition, Cybersecurity involves proactively identifying vulnerabilities in systems and networks, followed by implementing solutions and updates to fix these issues. The versatile nature of Cybersecurity seamlessly counters the various cyber threats, that is its main purpose and strength.

In his book, "Cybersecurity and Cyberwar: What Everyone Needs to Know" [2], Singer highlights the ever-evolving identity of cyber threats and the increasing complexity of tactics used by cybercriminals. A clear example of this process is the evolution of Ransomware attacks. Their essence was in encrypting files, demanding money for the decryption keys. Later this strategy adopted a blackmail aspect, exfiltrating sensitive data and threatening to release it publicly unless the ransom is paid. The author emphasizes the importance of understanding the strategic implications of Cybersecurity within the national security and changing geopolitical dynamics.

A well-known practice that we want to accentuate is the encryption of information, as it is nowadays one of the most essential means of Cybersecurity. The same opinion was shared by Schneier, a well-known security expert and author of "Secrets and Lies: Digital Security in a Networked World", emphasizing the critical importance of encryption in protecting sensitive information from unauthorized access. He argues that encryption is a pillar of Cybersecurity, “On another level, cryptography is a core technology of cyberspace” [3] facilitating secure communication and transmission of data over digital networks.

In his book [4], Joseph Steinberg provides practical advice on Cybersecurity best practices for individuals and organizations. The author emphasizes the importance of constant monitoring, sharing threat intelligence, and developing an incident response plan to effectively counter cyber threats in today's interconnected world. The trade-off of information security investments and sharing cyber information between companies results in spending less money on security systems but helps to reach the same level of protection attained by companies that do not share.

Indeed, Cybersecurity operates on a multitude of fronts Cybersecurity, reflecting the evolving nature of digital threats. Over time, cybercriminals have grown increasingly sophisticated, employing advanced tactics to exploit vulnerabilities and carry out malicious activities on a global scale. Concurrently, individuals have become increasingly aware of the importance of Cybersecurity as the vulnerabilities that may result in the leakage of their data, heightening concerns surrounding Cybersecurity. This dual progression underscores the need for comprehensive, preventive measures to mitigate risks and protect against cyber threats in an interconnected world.

Comprehensive Timeline Analysis of Cybersecurity

As the first computers were starting to scale their manufacturing, to satisfy different human needs, appeared the first cyber threats in the name of “Virus”. These represent a direct attack on those standalone computers during the late 1980s. This situation motivated the creation of the first antivirus system in 1987 by the German Computer Security Expert, Bernd Robert. This system was capable of countering the virus called Vienna that infected files of type *.com on DOC-based systems. The method used was by detecting the fingerprint of the file and then comparing it with the virus fingerprints in the database, in this manner were identified the files that have been affected by the virus.

The next wave of cyber threats was happening in the Internet space in the form of cyber attacks. The first worm named Morris Worm, created by Robert Tappan Morris had a big impact as it put an end to the first Internet small community. To solve this issue, firewalls were introduced. A firewall in a computer network setting represents a machine or a collection of machines that allows the safe transfer between two networks. Still, “No firewall provides perfect security” [5], that is because it is considered that any traffic passing through the firewall is a potential network attack on the computer. For example, the majority of firewalls have some email provision, however, email is one of the most known methods of attack. Another thing to consider is that the security inside of a firewall tends to decrease with time if the internal machines are not constantly updated. Firewalls have left a significant mark on Cybersecurity as nowadays almost every organization connected to the Internet has implemented a form of a firewall that will ensure a level of protection against threats from the outside.

The 3rd generation of Cybersecurity is a major evolution that laid the foundation of today’s Cybersecurity. This is noted by the large-scale implementation of an intrusion prevention system (IPS). This period has seen an increasing exploitation of vulnerabilities in application software.

As technology advances rapidly, applications become more and more complex. This complexity has opened up new horizons for hackers, with attacks becoming more complex and therefore harder to detect and harder to prevent. During this period there was a significant increase in such attacks, which overturned the security system of this period and a large part of the information from the private environment reached the public environment. In response to these types of attacks, new types of IPS have been developed. These systems are based on detecting and countering malicious activities in real time. This new system differed from the intrusion detection system (IDS) in that the latter only passively analyzes and monitors the traffic environment, while the IPS system identifies potential threats and takes action to block or deprive the source of the threats. For this reason, the IPS system marked the beginning of a new era in Cybersecurity.

The fourth generation in the realm of Cybersecurity represented the moment when cyberattacks escalated to a new level, transferring from randomly targeting individuals to strategically going after larger corporations that have substantial finances. The ransom demands have commonly been the equivalent of just a few hundred pounds for an individual PC. Until recently, most ransomware attacks were simply opportunistic and mostly affected the computers of individual users or small businesses. Even though the second and third generations of internet security focused on access control and monitoring all traffic, they failed to verify the actual end-user content found in emails, file downloads, and similar sources. At the same time, it became easier for more people to launch these attacks. All of these accentuated the need for anti-bot and sandboxing tools to detect and neutralize new forms of cyber threats. Anti-bot tools represent systems that are designed in such a way as to find and block the access of the bots to websites and web services. Well-known anti-bot tools are CAPTCHA and IP-blocking. Sandboxing is a security technique that creates a specific environment, named sandbox, and isolates it from the main architecture, preventing malware programs from inside from influencing the main system.

Currently, Cybersecurity plays an important role in the life of the entire planet because large-scale attacks with multiple vectors of actions characterize the newest generation of cyber threats. The complexity of a cyber attack today is much greater than 10-15 years ago. This complexity is due to several factors such as the sophistication of techniques and technologies used by hackers. One of the cyber threats that is common today is "Ransomware" attacks "With more than 10 terabytes of data stolen monthly, ransomware is one of the biggest cyber threats in the EU, with phishing now identified as the most common initial vector of such attacks" [6]. It represents a type of software that threatens a victim by destroying or blocking their data access to certain systems until the victim pays a ransom". The annual cost of cybercrime to the global economy is estimated to have reached €5,5 trillion at the end of 2020, double the figure of 2015 "[6]. Today's cyber threats can come from a variety of actors: from hackers acting individually to groups of hackers acting together to orchestrating larger-scale attacks. Cyber attacks can also come from certain states against other states or from other groups that are secretly funded by the state to obtain information. For this reason, some forms of Cybersecurity implemented to prevent older attacks, have been outdated and are no longer effective against the newest attacks. Thus, Cybersecurity is still evolving to adapt to new types of attacks, to make the online environments as safe as possible.

Progressive Cybersecurity Innovations of the Modern-Day

As the landscape of Cybersecurity is constantly evolving, even more, innovations are being created to fight several cyber threats and cyber attackers. To keep the security efficient against those factors multiple innovations had to come into play. One of the most prominent examples is the Zero Trust Architecture. Speaking generally, it can be described as a never-trusting concept that always rejects network requests eliminating any trust in them. The ZTA is presented as a new alternative for VPN services that have become too expensive and insecure. "ZTA is a multi-layered approach to an organization's network security with the idea of never trusting and always verifying every access to a resource" [7], knowing that, it is only logical to assume that the majority of current organizations would consider switching from VPN services to the ZTA, however in reality, this turned out to be not the anticipated scenario. Despite all the benefits of the ZTA it still is not popular as the organizations lack information on its benefits and drawbacks. This state of things is not beneficial to the development of Cybersecurity as it blocks the potential of a newer and more cost-effective architecture for protecting networks.

The next innovation we want to bring to the discussion is the Endpoint Detection and Report mechanism, also known as the Endpoint Threat Detection and Response. It was created by A. Chuvakin in 2013. EDR follows a specific chain of actions to provide a report concerning potential cyber threats. It starts by collecting data from endpoints and sending it for storage and processing in a centralized database where it is thoroughly correlated to try and detect suspicious activity from hosts. In case of a serious cyber threat, both the user and the emergency response teams are provided a report on the situation of an emerging danger. In recent years EDRs have been heavily tied with AI methods and machine learning as they appear to be rule-based, helping in finding new patterns and correlations of threatening behavior. From all that was said above we can conclude that EDR show antivirus capabilities as an EDR will trigger an alert once it detects irregular behavior. The most critical asset of the EDR is that it may detect unknown threats and prevent them before they escalate and become harmful due to the behavior and signs. Even if behavioral patterns could sound ideal for detecting malicious acts, this also implies the existence of many false alerts, meaning that ordinary unharmful user actions are considered malicious, as EDRs prioritize precision over other things. Although EDRs bring a valuable boost to security, the overall security of the organization highly depends on the human factor, which is its biggest negative factor.

Another proven effective weapon against cyber threats is Cyber Threat Intelligence (CTI) as it has appeared as an important solution for businesses to address security events' increasing quantity and complexity. CTI can be defined as the active identification and precise analysis of cyber threats, to achieve this goal it uses a Threat Intelligence-Sharing Platform (TISP) that may access threatening data and turn it into refined and precise intelligence that can be further integrated into technologies that are aimed to produce an incident response. Firms that center themselves on informational security offer TISP solutions that can be classified into two categories: content aggregation (which provides feeds that contain threat data), and threat intelligence management (that uses the results of data to generate economic). Now going back to the CTI it is considered to be a process of gathering, analyzing, and distributing information contributing to identifying, monitoring, and anticipating cyber threats. That is how exactly CTI can help businesses to become more involved and attracted to Cybersecurity development, as it directly contributes to identifying vulnerabilities before the attackers get to exploit them. CTI also plays an essential role in detecting attacks by using intrusion detection systems. These are rooted in practices of cyber criminals or types of attacks, located by processing gathered intelligence data. Another thing is that CTI provides specific security plans specifically created towards retaliating against the patterns used by cyber threat actors, making it a key tool for organizations that are interested in preventing, detecting, and responding effectively against potential cyber-attacks. As for the actual use of this method, it has been proven to be quite a beneficial security solution all because of the benefits it provides, it managed to successfully attract the attention of most organizations. The big takeaway from CTI is that it managed to produce a significant impact on how nowadays organizations process and take action regarding various issues in their security systems.

The next technology we will talk about is deception technology. This is one of the most developed areas of Cybersecurity. This technology is based on the fact that it lures hackers or people with bad intentions into certain traps so that the latter can become more visible and easier to detect. This technique is quite effective because it has revolutionized threat detection, moving from a reactive to a preventive defense mechanism. This technology is dynamic as it adapts to evolving threats throughout the contamination. For this reason in practice, this technology is always one step ahead of the attacker. Also, to evolve and improve itself, this technology uses artificial intelligence and machine learning technologies, which increase its effectiveness. Unlike traditional Cybersecurity measures and technologies, Deception technology not only detects the source of damage but also prevents this source from expanding and causing more damage. This technology has an important role in Cybersecurity which has put many obstacles to hackers.

A component that is also used in Cybersecurity is Identity and Access Management (IAM). This technology has also become a revolutionary one for Cybersecurity by creating a well-organized structure to manage and secure some data and access rights to some data. IAM uses several technologies that are new to Cybersecurity. Two of these new technologies implemented are multi-factor authentication and biometric verification. With the help of these technologies, access rights to certain data are granted to use depending on the type of authority they hold. Thanks to these technologies, unauthorized access to some more personal data such as bank details has been limited. IAM is continuously evolving by interacting with advanced analytics and threat intelligence to detect and prevent specific attacks in real time.

Also, as a very important part of modern Cybersecurity is worth mentioning Cloud Security. Taking into consideration that most organizations and even particular individuals moving their data, applications, and particular information onto the cloud ensuring their security is a very important task nowadays. For those purposes, encryption, IAM, network security controls, and continuous monitoring are used. As cloud adoption keeps growing, organizations need to keep their security up-to-date, to prevent any information leaks.

Conclusions

Cybersecurity is undoubtedly a shared responsibility, essential for maintaining integrity and privacy in the online environment. Starting with the most primitive attacks and evolving to today's complex attacks, cybersecurity has also developed through multiple generations of innovations in order to find new ways to combat online criminals and to protect user data online. In fact, knowing that cybersecurity is an ongoing process, over the years its involvement in the regular person's life has become more prominent, to a point where every person that owns an electronic device connected to the internet needs a way to protect its data. Today, cybersecurity has reached phenomenal results, such as encryption and firewalls, to minimize the risk of the virtual environment. This is thanks to the increasing interest of companies and media in the address of the cyber security field. The cyber threats have started to affect companies and populations in more aggravated ways, which caused cyberspace to search for new ways to protect the users and their data, but also to react and combat the cyber criminals in their attempts to access sensitive data by constructing a multi-layered defense system.

References

[1] S. W. Brenner, "Cybercrime Metrics: Old Wine, New Bottles?", VIRGINIA JOURNAL OF LAW & TECHNOLOGY, vol. 9, no. 13, p. 53, January 2004.

[2] P. W. Singer and A. Friedman, "Cybersecurity and Cyberwar: What Everyone Needs to Know", Oxford University Press, January 3, 2014.

[3] B. Schneier, "Secrets and Lies: Digital Security in a Networked World", Wiley, 2015, p. 450.

[4] J. Steinberg, "Cybersecurity For Dummies", Wiley, 2019.

[5] K. Ingham and S. Forrest, "A History and Survey of Network Firewalls", University of New Mexico, p. 42, 2002

[6] "Top cyber threats in the EU" [Online]. Available: https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/

[7] Z. Adahman, A. W. Malik, Z. Anwar, "An analysis of zero-trust architecture and its cost-effectiveness for organizational security", September 2022, https://doi.org/10.1016/j.cose.2022.10291.