The role of cyber security in facing the challenges of cyber warfare and cyber-attacks

KARIMAN RAMZY El HELOW
Higher Institute of Computer, King Mariout, Alexandria, King Mariout Academy, Alexandria, EGYPT

Abstract. Cybersecurity has become a growing problem plaguing the entire world, where software systems have been subjected to constant attacks by malicious entities, which led to serious consequences that affected most institutions and individuals. To address this problem, we must focus on how to develop secure systems by educating software developers. Therefore, there should be an urgent need to develop safe software and use it to build software applications. And the application of security aspects at every stage of the software development life cycle in order to add significant protection to the programs.

This paper presents the possibility of using cybersecurity to counter the spread of cyber warfare and cyber-attacks, and to identify the different patterns of these attacks.

Key-Words. Cybersecurity; Cyber-Attacks, software engineering; Software Development Life Cycle (SDLC)

1 Introduction

With the advent of the Internet, the world has become a small village, and with the rapid growth of security, the world of hacking has also grown faster. Looking at the issue of cybersecurity is due to the fact that companies providing cloud computing do so, which is why these companies must be well secured using the latest advanced encryption techniques [1, 2]. So-called cyber terrorism has emerged, which is the use of innovative information technology by terrorist groups to advance their political agenda [3, 4]. Cyber warfare, which is called the fifth Domain of warfare, has become the latest trend of cyber terrorism, which is the use of information technology by nation states to pass through the networks of another country to cause damage, deterioration of communications, interruption of commerce, or endangerment of data, or weakening of infrastructure services. This is done by hackers trained in how to take advantage of computer networks' details, and under the auspices and support of nation-states [5- 6]. While some countries have resorted to what is known as cyber espionage, which is the use of information technology to obtain confidential information without the knowledge or permission of its owners with the aim of gaining strategic, military and economic advantage, by using malware [7, 8].

The aim of this paper is to use cyber security to confront the spread of cyber warfare and cyber-attacks, plan early actions to prevent these attacks from occurring, and to develop and test programs and devices to provide appropriate security. This paper discusses the role of cybersecurity in preventing these attacks and presenting an appropriate solution.

The rest of the paper is organized as follows: Section 2 Global Reports of Cyber Attacks, Section 3 The Potential Role of Cybersecurity in Combating These Cyber Attacks, Section 4 presents the findings and discusses a brief overview of the different types of cyber-attacks, and discusses the implications of using Cybersecurity in analyzing and predicting attacks. The final section concludes the paper and explains future work.

2 Global Reports of Cyber Attacks

2.1 Costs of Cybercrime

Statistics show that Cybersecurity will cost companies around the world an estimated $ 10.5 trillion annually by 2025, as the rising from $ 3 trillion in 2015 as shown in Figure1[9]. With a growth rate of 15% annually–Figure 2 shows the global damage costs of cybercrime, which is considered the most influencing factor in the transfer of economic wealth [10].

Fig 1, growth of Cybercrime Costs

Fig 2, Global Cybercrime Damage Costs

2.1.1 Cybercrime for Medium and Small (Businesses) companies (SMEs)

Ccenture's Cost of Cybercrime Study indicates that About 43% of cyber-attacks target small businesses, but only 14% of these companies struggle to defend themselves. According to the Ponemon Institute Report on the State of Cybersecurity, the most common types of cyber-attacks on SMEs include: Hacked/Stolen Devices: 33%, Credential Theft: 30%, Phishing/Social Engineering: 57% [11- 15].

2.1.1.1 2021 Cyber Attacks Timeline

Cybercrime always tops the motives chart with 88.3%, as it was 84.1% in March 2021. While Malware accounts for nearly 50% of attacks. Reports indicated that in January 2021, 160 cyber-attack incidents were collected, in February 2021, 240 incidents were collected, in March 2021, 276 incidents were collected, in April 2021, 240 incidents were collected. And in May 1-15, 2021, 89 incidents were collected, with an average of 5.9 events per day, while in the latter half of May, 85 events were collected, with an average rate of 5.32 events per day, as shown in figure 3 [16 - 18].

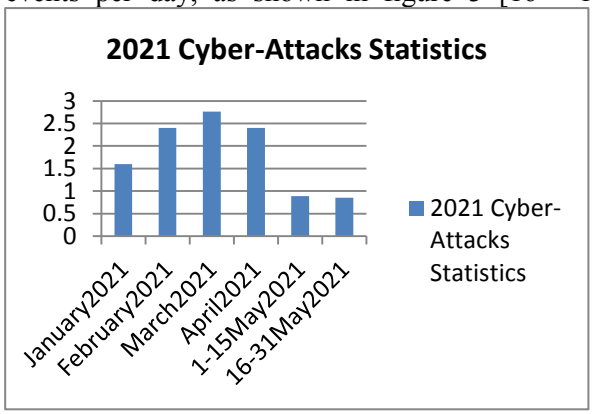

Fig 3, 2021 Cyber-Attacks Statistics

2.2 CheckPoint's 2021 Cyber Security Report

This Report shows how criminals and hackers exploited Corona (COVID-19) pandemic in 2020 to target all business sectors and cloud exploits to phishing and ransomware [19], this resulting in a new institution falling victim to ransomware every 10 seconds around the world. in the end of 2020, cyberattacks on hospitals have increased by 45% worldwide [20].

2.2.1 Datto's Global State of the Channel Ransomware Report 2020

The report shows that ransom cases are on the rise, rising from 24% in 2019 to 90% in 2020, as shown in figure 4 [21]:

Fig 4, Datto's Global State of Ransomware Report 2020

2.2.1.1 Verizon's report on the responsible for data breaches

The Verizon's report notes that most cyberattacks are launched by organized crime groups, internal bad actors, affiliated groups, company partners and outsiders as shown in figure 5 [22].

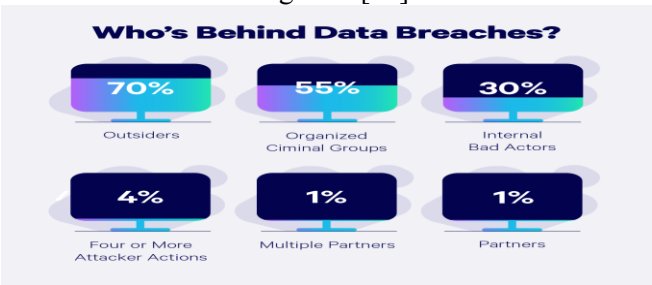

Fig 5, Verizon's report on who's Behind Data Breaches

3 The Potential Role of Cybersecurity in Combating the Cyber Attacks

In the past, governments and organizations have used individual security techniques to secure their networks and the valuable data within them. But with the increase in the violations, organizations are thinking about launching the issue of cybersecurity to provide protection in the data center, across environments, on the network, and in public and private clouds. By focusing on prevention, organizations can prevent threats from affecting the network, and reducing cybersecurity risks to a manageable degree. Whereas, cybersecurity is a set of tools, security concepts, guidelines, procedures, training, risk management methods and techniques that can be used to protect the cyber environment, user assets and the organization [23].

Cyber security always strives to achieve and maintain the security characteristics of user and organization assets against security risks that threaten systems in the cyber environment. Using cybersecurity can also help manage risks, prevent

attacks, data breaches or them theft, and identity theft. Cybersecurity operations can be a challenge, in organizations and government networks, where cyber threats target the secret and military assets of a country or its people [24]. Here, the organization must have an effective incident response plan that is able to prevent attacks and their severity, Such as protecting information from being stolen or lost while checking computers, also conducting additional studies using software engineering and cybersecurity environment, and focusing on the application of the security aspect from the beginning of the software development life cycle [25, 26].

4 Results and Discussion

4.1 A brief overview of the different types of cyber attacks

The use of security trends, (new technologies) and smart threats has become a challenging task. However, assets and information must be protected from cyber threats, which take many forms, such as:

a- cybercriminals are those who obtain unauthorized access to computer systems; they are categorized into three groups: the first type is amateurs, politically motivated hackers and terrorist organizations, the second type is financially motivated hackers or state-sponsored hacking, and the third type is ex-employees who seek revenge.

b- Ransomware is a type of malware that an attacker blocks a victim's computer system files through encrypting and requiring a payment to decrypt them.

c- Malware is any program or file that an attacker uses it to harm a computer user, such as viruses, Trojans, worms, and spyware.

d- Social engineering is attacks that rely on deceiving users to breach security measures to obtain protected sensitive information.

e- Phishing is a type of fraud in which the attacker (the fraudster) sends fraudulent emails with the intent to steal sensitive data, such as login information or credit card.

f- End-user is the person who accidentally downloads malware to a device.

g- Cyber terrorism: is the launch attack by terrorist groups on communications infrastructure, computer systems and networks to advance their political agenda.

h - Cyber war: is the passage of nation-states through the networks of another country to cause damage by trained hackers, under the auspices of the nation-states.

i- Cyber espionage: it is obtaining confidential information without the knowledge of its owners, to gain strategic, military and economic advantage, by using malware.

4.1.1 using Cybersecurity in analyzing and predicting attacks

Based on the damage caused by the cyber-attacks to the organization's systems and networks, the use of cyber security to analyze and predict these attacks is essential. Here, comes the effective role of information security analysts to protect the organization's systems and networks, through appropriate planning and implementation of the necessary security measures. And create solutions to prevent critical information from being stolen, hacked, or destroyed; this can only be done through systematic development. So the application of software engineering techniques is an important step, and also the software engineers must be aware of the risks and security issues associated with the design, development and secure the computer network.

Here, successful security must begin at each stage of the software development lifecycle which is the analysis, design, implementation, testing and maintenance stages. In the analysis stage, the requirements of stakeholders and users are determined. The software design phase involves creating a blueprint from the software, outlining the guidelines for system design. The implementation phase includes the coding activities required to create the software, according to the customer requirements. In the Test phase the system is tested to remove errors. Finally, the maintenance phase, improvements, bug fixes. With an emphasis on incorporating security concerns into each stage of the software development lifecycle, developers can also getting the code they wrote, being reviewed by threat advisors, and improving code security by specifying a security code, as well as operational security. User education is vital to the security of any organization, where any user can accidentally introduce a virus into the system and destroy it. Validating the identity of users is essential by using genetic algorithms for identification in software or computer forensics, from fingerprints, face or voice scans, to identify an individual's purported identity based on their physiological or behavioral characteristics.

4.1.1.1 Disaster recovery and business continuity

it means determining how the organization responds to cyber security incidents. Also, how the organization will restore its programs and information to return to the same operational capacity that it was in before the event while ensuring the continuity of work. Since cyber security protocols focus on real-time malware

detection, heuristic analysis should be used to monitor the behavior of programs and their code to defend against viruses, worms, or Trojan horses. Also, employees must be educated about how to use end-user security software. And must be updated the software and operating system in the organization, Use strong passwords, Avoid using unsecure WiFi networks in public places, use anti-virus software, do not open email attachments from unknown individuals and do not open unfamiliar websites. For the security of web databases the security impact on all web data management functions must be examined. It includes transaction management, index and storage management, metadata management, and query processing.

5 Conclusions and Future Work

Disruptive incidents in the future will continue to fuel, and with it concerns about the potential for strategic cyber-war. Planning for worst-case scenarios and optimally managing risks is a national security task. But it is also important to use cybersecurity against malicious incidents to know how to identify and fix vulnerabilities to help ensure the security of enterprise systems. And work on improvement, evaluation of efficiency and training of engineering cadres, planning to implement methods that secure software, hardware, and networks, developing tools and techniques to prevent attacks, and implementing security requirements at every stage of the software development lifecycle, with a focus on testing and maintenance given their importance, and conducting risk analysis at every step to build a strong secure program. In addition to conducting additional studies using software engineering and programming a cyber-learning environment and the country's businesses must be using the AI to defend themselves. In future smart systems, there are two requirements for cybersecurity, namely "security engineering" and "security by design". This will require the systems to have automatic detection of malware, threats and attacks without installation, and also to track, identify and analyze cybersecurity threats to combat viruses, hackers, terrorists, espionage or any terrorist activities.

References

[1] Kevin Curran, Sean Carlin, Mervyn Adams, Security Issues in Cloud Computing, Research Gate, 2012.

[2] Seemma P.S, Nandhini S., and Sowmiya M., Overview of Cyber Security, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 7, Issue 11, November 2018.

[3] Jordan J. Plotnek, Jill Slay, What is Cyber Terrorism: Discussion of Definition and Taxonomy, Research Gate, October 2019.

[4] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity", Journal of Computer and System Sciences, vol. 80, no. 5, pp. 973-993, 2014.

[5] Petr Hruza, Jiri Cerny, CYBERWARFARE, International conference KNOWLEDGE-BASED ORGANIZATION 23(1), Vol. XXIII, No. 1, 2017.

[6] Researchgate.net, "Computer Security and Mobile Security Challenges", 12 October 2016.

[7] David Freet, Rajeev Agrawal, cyber espionage, Encyclopedia of Big Data, 2017.

[8] Millman, Renee, "New polymorphic malware evades three quarters of AV scanners". SC Magazine UK., December 15, 2017.

[9] Steve Morgan, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cybercrime Magazine, Sausalito, Calif. – Nov. 13, 2020.

[10] McAfee report, Economic Impact of Cybercrime - No Slowing Down, December 2020.

[11] Jack M. Germain, The Cybersecurity Outlook for 2021 and Beyond, Tech News World, Jun 4, 2021.

[12] Abdulmajeed Alahmari, Bob Duncan, Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence, International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020.

[13] Catrina Doxsee, Jake Harrington, Significant Cyber Incidents, CSIS Center for Strategic International Studies, June 17, 2021.

[14] ROB SOBERS 134 Cybersecurity Statistics and Trends for 2021, Varonis.com, Mar. 2021.

[15] Statistas Statistics Reports, Global number of cyber security incidents in 2020, sorted by victim industry and organization size, 2021.

[16] Symantec Corporaton, "Internet Security Threat Report", Vol. 21, Mountain View, Calif., April 2016. Last Accessed: June 26, 2018, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[17] HACKMAGEDDON, 1-15 May 2021 Cyber Attacks Timeline, 19 May 2021.

[18] HACKMAGEDDON, 16-31 May 2021 Cyber Attacks Timeline, 3 June 2021.

[19] INTERPOL, INTERPOL report shows alarming rate of cyberattacks during COVID-19, 4 August 2020.

[20] Check Point Software Technologies LTD, Check Point's 2021 Cyber Security Report, 2021.

[21] Datto, Datto's Global State of the Channel Ransomware Report 2020, November 2020.
[22] Verizon, Verizon's report on who is the responsible for data breaches?, 2021.
[23] Daniel, Schatz; Julie, Wall, "Towards a More Representative Definition of Cyber Security", Journal of Digital Forensics, Security and Law. 12 (2), ISSN 1558-7215., 28 December 2017.
[24] MSSP Alert, "Multi-Vector Attacks Demand Multi-Vector Protection", July 24, 2018.
[25] Chris Johnson, CyberSafety: CyberSecurity and Safety-Critical Software Engineering, Chapter In book: Achieving Systems Safety, pp.85-95, December 2012.
[26] R. Jones and A. Rastogi, "Secure Coding: Building Security into the Software Development Life Cycle", Information Systems Security, vol. 13, no. 5, pp. 29-39, 2004.