vulnerability

by David Maina

Submission date: 26-Feb-2024 12:54PM (UTC+0530)
Submission ID: 2302417072
File name: Significant_of_Cyber_Security_Vulnerabilities.docx (24.91K)
Word count: 2322
Character count: 14018

Significant of Cyber Security Vulnerabilities

Name of the Student

Institution

Course

Instructor

Date

Abstract

This essay investigates the criticality of cybersecurity vulnerabilities and the necessity of the preemptive solution measures. Studying different kinds of vulnerabilities, including software, hardware and human factors, we examine the outcomes, i.e., data breaches, financial losses and national security threats. Surrounded by recent relevant research, the essay also provides mitigation techniques such as patch management, security awareness training, and defense-in-depth implementations. The adoption of such approaches also reinforces the value of proactively addressing vulnerabilities, ensuring not vulnerable assets are compromised and avoiding unnecessary escalation of cyber threats. This essay highlights a key requisite of continuous evaluation, adaptation, and enhancement of cybersecurity policies to effectively foresee emerging risks and protect people, organizations, and states from cybersecurity hazards.

Significant of Cyber Security Vulnerabilities

Introduction

Cybersecurity weaknesses are the security system's underlying security flaws that potentially present a target for malicious actors to abuse. These vulnerabilities can result in unauthorized access, alteration, or disruption of data systems, leading to the compromise of the confidentiality, integrity, and availability of information and therefore exposing individuals, organizations and even nations to significant risks. In the modern scenery when majority of our personal and sensitive data is getting stored and transmitted digitally, the role of cybersecurity cannot be underestimated. Data security has become fundamental in the current era where assets are vulnerable to cyber attacks and interactions are not safe digitally. The mapping of system (Humayun et al. 2020) has revealed a dominant pattern of cyber security vulnerabilities. It shows that many studies prioritise common threats such as phishing, DDoS attacks and malware. As clearly shown, Aslan et al. (2023) underline cyber threat evolution and necessity of innovative solutions. This essay provides through an overview of vulnerabilities in cybersecurity, explains common threats, trends, and mitigation strategies.

Types of Cybersecurity Vulnerabilities

Software vulnerabilities remain to a great extent one of the often used and frequently exploited s of cybersecurity. These weaknesses are a consequence of either software code or design faults thus providing the attackers with access points to compromise the integrity of a system and gain unautouarized access to sensitive information (Alsharif et al., 2022). Frequent examples are buffer overflown, SQL injection, and cross-site scripting (XSS). Buffer leak occurs when a program tries to fill a memory block with more data than the allocated size, which in turn

allows an attacker to take arbitrary actions or modify a program's normal behavior (Vander–Pallen et al., 2022). Symmetrically, SQL injection attacks target web application backends by inserting illicit SQL sentences inside input fields. These attacks are capable of manipulating the database and retrieving confidential data (Razaque et al., 2019). In Cross- Site Scripting , malicious codes are injected as scripts into the web pages observed by other users. This leads to the unauthorized access or data theft (Ghelani et al., 2022). These software vulnerabilities highlight the necessity for reliable software development processes and continual security testing procedures to find out any probable defects.

Vulnerabilities in hardware components are the other critical threat that cybersecurity faces, for these are weaknesses in the chips, memory, and firmware of computers that make them vulnerable. Spectre and Meltdown vulnerabilities, which are hardware faults found in modern CPUs, show the danger level of these types of hardware flaws (Hasanova et al., 2019). This vulnerabilities are exploiting speculative execution mechanism in processors that are supposed to prevent access of the attacker to the memory, which is a vital data. Spectre and Meltdown being of the most complex vulnerabilities, the solution is taunting, as it requires redesign of the hardware and patches of the software to mitigate (Razaque et al., 2019). Other than this, when firmware vulnerabilities are there, such as shown in embedded systems and peripheral devices, attackers can gain full time access on compromised systems (Ghelani et al., 2022). This particularity, should be considered, when drawing up a holistic security approach.

Human factors are another fundamental dimension of cybersecurity threats that may arise out of the actions or the behavior of the people in an organization. The deficiency of awareness and training about typical human fallibilities may lead to serious threats to cybersecurity, for instance, phishing, weak passwords and social engineering(Alsharif et al.,2022). One type of

attacks that use phishing are those that are conducted via emails or messages with a deceptive content aimed at misleading users to disclose their sensitive information or click malicious links. Insecure password practices, such as the use of simple passwords or password sharing, are the source of vulnerabilities for hackers to gain access to users' accounts (Razaque et al., 2019). Through social engineering techniques that misuse human psychology, individuals are tricked to expose confidential information or to execute actions that undermine security (Hasanova et.al, 2019). This emphasizes the need for security awareness training and the inherent education programs.

Significance of Cybersecurity Vulnerabilities

Cybersecurity threats are emphasized due to their clear ability to give rise to many different catastrophes, from data leaks to national security crises. Among the consequences of exploits, data breaches should be mentioned for instance; these very often lead to the exposure of confidential data and may have a severe impact either on the individuals or on the organizations in particular (Vander–Pallen et al., 2022). Take the example of the Equifax data breach of 2017 that was conducted by hackers who took advantage of the vulnerable systems, and as a result, personal information of 147 million people was compromised (Ruposky, 2022). Such breaches not only erode trust in the targeted organization but also is not restricted to the affected individuals only but also may lead to identity theft, financial frauds and reputational damages.

Economic effects also represent another devastating effect of cybersecurity incidents, with the organizations bearing the costs of both direct and indirect effects including mitigating the breaches and what comes thereafter. To respond to the attacks and to conduct forensic inquiries would require a lot of finance to foot such expenses (Gunduz & Das, 2020). Besides the fact that these regulatory fines are imposed for non-compliance with laws aimed at data

protection like the General Data Protection Regulation in the European Union, their escalation can further weigh down financially on organizations found wanting in data security (Krause et al., 2021). Beyond the immediate financial costs of cyber incidents, there are also other intangible costs (e.g., reputational harm and loss of customer trust) which may have deeper and longer lasting implications, on the survivability and competitiveness of the organization.

The incapacitation or disturbance of key services is an extreme effect of cybersecurity vulnerabilities, as cyberattacks can cause destruction against critical infrastructure and systems rendered nonfunctional. Cyber adversaries aiming to disrupt the energy supply and create widespread mayhem highlight power grids as the target for a cyber attack (Krause, Wein, Amoroso, & Rosoff, 2021). In 2015, Ukraine had a critical power failure caused by a computer virus that attacked its power system. It demonstrated clearly that cyber threats can take down vital infrastructure and services which are fundamental for the society (Rees & Rees, 2023). Similarly, cyber security attacks on health care systems, transportation networks, and financial institutions can cause societal disorder, insecurity and instability.

As cybersecurity threats such as vulnerabilities can compromise government systems, critical infrastructure and military operations this way posing a serious national security risk (Patel & Chudasama, 2021). The state-funded cyber espionage staged by different actors seeks to steal sensitive information, disrupt ongoing operations, or impair strategic capabilities (Yarovenko, 2020). The Stuxnet (an alleged state-sponsored) worm represents how cybersecurity vulnerabilities and national security converge, mainly because it was designed to illegally access Iran's nuclear facilities with the objective of making its centrifuges stop (Marmol, 2020). Succesful incidents of this type help to uncover the need for the protection of national interests

and the protection of cyberspace from those who exploit vulnerabilities to obtain geopolitical benefits.

Mitigation Strategies

Addressing cybersecurity vulnerabilities is crucial to reinforce prevention of likely threats and protect vital resources. A few solutions have turned out to be successful in removing the vulnerabilities and making the cyber adversaries harder to achieve their goals. Patching becomes a key element in cybersecurity defense, whereby the system administrators apply security patches and updates as soon as possible for software and systems. Patching patching performs well in fixing existing security gaps and improving the degree of resistance to attacks to malicious intruders (Dissanayake et al., 2022). Similarly, the WannaCry ransomware attack in 2017 which leveraged a vulnerability in the older versions of Microsoft Windows was provide medical care for and contained its spread through the use of security patches.

Education of users in security awareness training is the key to the reduction of human-based vulnerabilities since it introduces cybersecurity best practices, and thus the security culture is nurtured inside the organization. Through training employees to identify and avoid common threats such as phishing attacks, weak passwords, and social engineering techniques, organizations can build a security culture in which employees take responsibility for their own data security (Hart et al., 2020). Technical learning tools such as interactive training modules or serious game Riskio can be utilized to boost team engagement and learning rate of key security concepts (Dash & Ansari, 2022).

Defense-in-depth is a multi-layered approach that involves installation of redundant controls to provide duplicative security protection against intrusion. This approach seeks to

establish a robust security architecture by reducing the threats through preventive, detective, and reactionary measures (Rass et al., 2020). As an example, putting various firewalls, intrusion detection systems (IDS), and encryption methods at the different network layers can serve the purpose of trying to detect and stop unauthorized access attempts. Furthermore, these security tools (segmentation and access controls) prevent the attackers from moving sideways within a network, hence minimizing the possibility of huge damages resulting from potential breaches (Papakonstantinou et al., 2020). It is paramount to acknowledge that cybersecurity is an activity that should be done continuously; it requires constantly monitoring, adaptation, and renovation in order to keep in pace with newly arising threats and new technologies.

Conclusion

The importance of cybersecurity vulnerabilities and mitigation techniques have been discussed in this essay. It looked at the various kinds of vulnerabilities; hardware, software, and human factors and emphasized the possible outcomes, data breaches, monetary losses, interruptions to services, and dangers to national security. Defense-in-depth techniques, patch management, security awareness training, and other mitigation tactics were highlighted, with an emphasis on how they strengthen defenses and lower risks. Proactively addressing cybersecurity vulnerabilities is essential to safeguarding important assets and reducing the effect of any assaults. Organizations can reduce vulnerabilities and strengthen their defenses against cyberattacks by remaining watchful, putting strong security measures in place, and encouraging a culture of security awareness. Furthermore, in an increasingly linked digital world, cybersecurity measures must be continuously assessed, adjusted, and improved in order to remain ahead of emerging threats. In the end, taking preventative action is essential to protecting people, businesses, and countries from the constant threats presented by cybersecurity flaws.

References

Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science & Engineering*, *40*(3).

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2022). Software security patch management-A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, *144*, 106771.

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints*.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, *169*, 107094.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, *95*, 101827.

Hasanova, H., Baek, U. J., Shin, M. G., Cho, K., & Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, *29*(2), e2060.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*, 3171-3189.

Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in power grids: Challenges and opportunities. *Sensors*, *21*(18), 6225.

Marmol, R. A. (2020). *Protecting Civilians from Cyber Operations in Cyber Warfare* (Doctoral dissertation, Utica College).

Papakonstantinou, N., Linnosmaa, J., Bashir, A. Z., Malm, T., & Van Bossuyt, D. L. (2020, January). Early combined safety-security Defense in Depth assessment of complex systems. In *2020 Annual Reliability and Maintainability Symposium (RAMS)* (pp. 1-7). IEEE.

Patel, K., & Chudasama, D. (2021). National security threats in cyberspace. *National Journal of Cyber Security Law*, *4*(1), 12-20p.

Rass, S., Schauer, S., König, S., Zhu, Q., Rass, S., Schauer, S., ... & Zhu, Q. (2020). Defense-in-Depth-Games. *Cyber-Security in Critical Infrastructures: A Game-Theoretic Approach*, 211-221.

Razaque, A., Amsaad, F., Khan, M. J., Hariri, S., Chen, S., Siting, C., & Ji, X. (2019). Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain. *IEEE Access*, *7*, 168774-168797.

Rees, J., & Rees, C. J. (2023). Cyber-Security and the Changing Landscape of Critical National Infrastructure: State and Non-state Cyber-Attacks on Organisations, Systems and

Services. In *Applications for Artificial Intelligence and Digital Forensics in National Security* (pp. 67-89). Cham: Springer Nature Switzerland.

Ruposky, T. J. (2022). The Exponential Rise of Cybercrime. *U. Cent. Fla. Dep't Legal Stud. LJ*, *5*, 137.

Vander–Pallen, M. A., Addai, P., Isteefanos, S., & Mohd, T. K. (2022, June). Survey on types of cyber attacks on operating system vulnerabilities since 2018 onwards. In *2022 IEEE World AI IoT Congress (AIIoT)* (pp. 01-07). IEEE.

Yarovenko, H. (2020). Evaluating the threat to national information security. *Problems and Perspectives in Management*, *18*(3), 195-210.

vulnerability

ORIGINALITY REPORT

1%	1%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to American Public University System Student Paper	<1%
2	Brendan Ooi Tze Wen, Najihah Syahriza, Nicholas Chan Wei Xian, Nicki Gan Wei et al. "chapter 2 Detecting Cyber Threats With a Graph-Based NIDPS", IGI Global, 2023 Publication	<1%
3	www.diva-portal.org Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

vulnerability

PAGE 1

PAGE 2

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 3

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word. Consider using the article **the**.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 4

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 5

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

Missing "," You may need to place a comma after this word.

PAGE 6

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 7

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to remove this article.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 8

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Article Error You may need to use an article before this word. Consider using the article **the**.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 9

PAGE 10

PAGE 11