https://doi.org/10.24867/FUTURE-BME-2024-120 Original scientific paper

CYBERSECURITY ISSUES OF COMPUTING SYSTEMS

Stevan Stankovski[1] [0000-0002-4311-1507], *Gordana Ostojić*[2] [0000-0002-5558-677X]

Abstract

In an era where digital transformation is integral to societal infrastructure, the imperative of robust cybersecurity measures in computing systems has never been more critical. This paper addresses the multifaceted cybersecurity issues confronting contemporary computing systems, encompassing hardware, software, and network vulnerabilities. We explore the evolving threat landscape characterized by sophisticated cyber-attacks, including advanced persistent threats, ransomware, and zero-day exploits. A comprehensive analysis is provided on the latest cybersecurity frameworks and protocols designed to mitigate these risks, with a particular focus on machine learning and artificial intelligence (AI) applications in threat detection and response. Additionally, we examine the role of emerging technologies, such as blockchain and quantum computing, in enhancing cybersecurity defenses. Case studies of recent high-profile cyber incidents are presented to underscore the practical implications of theoretical vulnerabilities and the effectiveness of contemporary security solutions. Furthermore, this paper discusses the regulatory and ethical considerations in cybersecurity, emphasizing the need for a balanced approach that safeguards privacy while ensuring robust protection against cyber threats. By synthesizing current research findings and industry practices, we propose a set of best practices and strategic recommendations for fortifying the cybersecurity posture of computing systems. We aim to provide a comprehensive understanding of the current challenges and future directions in cybersecurity, ultimately contributing to the development of more resilient and secure computing environments.

Key words: *cyber-attacks, ransomware, Blockchain.*

1. Introduction

In the 21st century, digital transformation has become an integral component of infrastructure, reshaping industries, economies, education, and daily life. From micro to macro environment, personal communications to national infrastructure,

[1] University of Novi Sad, Faculty of Technical Sciences, Serbia, stevan@uns.ac.rs

[2] University of Novi Sad, Faculty of Technical Sciences, Serbia, goca@uns.ac.rs

computing systems are embedded in nearly every aspect of modern existence. They enable the seamless operation of production systems, financial markets, healthcare systems, transportation networks, and government services. This integration has significantly enhanced efficiency, connectivity, and accessibility, driving innovation and economic growth. However, the pervasive adoption of digital technologies also introduces significant cybersecurity challenges that must be addressed to safeguard these advancements (Verma, 2024).

Cybersecurity, the practice of protecting systems, networks, and data from digital attacks, has emerged as a critical priority for individuals, businesses, and governments. The consequences of cyber-attacks can be severe, including financial loss, operational disruptions, data breaches, and reputational damage. As cyber threats become more sophisticated and widespread, the need for robust cybersecurity measures has never been more pressing (Olson, et al., 2011). This paper aims to provide a comprehensive analysis of the multifaceted cybersecurity issues confronting modern computing systems, exploring the threat landscape, inherent vulnerabilities, and the latest defense mechanisms.

2. Cybersecurity Threats

Different kinds of cybersecurity threats can occur in computing system networks, but three types can often be singled out as the most frequently occurring forms of threats: advanced persistent threats (APT), ransomware and zero-day exploits.

APT are among the most significant and insidious cyber threats. These attacks are characterized by their prolonged and targeted nature, often orchestrated by highly skilled and well-resourced adversaries, such as nation-states or organized cybercrime groups. APTs aim to establish a long-term presence within a target network to steal sensitive information or disrupt operations. Unlike typical cyber-attacks, which may be quick and opportunistic, APTs involve extensive reconnaissance, sophisticated infiltration techniques, and stealthy persistence, making them particularly challenging to detect and mitigate. A diagram of the APT lifecycle with crucial steps and actions is represented in Figure 1 (Buckbee, 2023).

Ransomware has emerged as a prominent threat, affecting individuals, businesses, and critical infrastructure. This type of malware encrypts victims' data, rendering it inaccessible until a ransom is paid to the attackers, typically in cryptocurrency. The impact of ransomware can be devastating, leading to significant financial losses, operational disruptions, and, in some cases, permanent data loss. High-profile incidents, such as the WannaCry and NotPetya outbreaks, have underscored the potential scale and severity of ransomware attacks.

Zero-day exploits leverage previously unknown vulnerabilities in software or hardware, allowing attackers to bypass traditional security defenses. These exploits are particularly dangerous because they can be used to launch attacks before developers have a chance to create and distribute patches. The discovery and exploitation of zero-day vulnerabilities often occur within a highly competitive black market, where such vulnerabilities can be sold for substantial sums. The challenge of defending against zero-day exploits underscores the importance of proactive security measures and advanced threat detection capabilities.

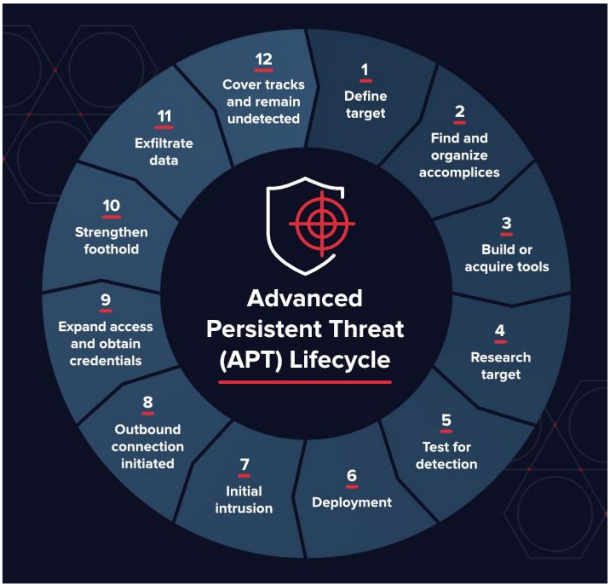
12 Cover tracks and remain undetected
1 Define target
2 Find and organize accomplices
3 Build or acquire tools
4 Research target
5 Test for detection
6 Deployment
7 Initial intrusion
8 Outbound connection initiated
9 Expand access and obtain credentials
10 Strengthen foothold
11 Exfiltrate data
Advanced Persistent Threat (APT) Lifecycle

Figure 1: APT Lifecycle (Buckbee, 2023)

3. Cybersecurity Frameworks and Protocols

Cybersecurity issues have led to the definition of cybersecurity frameworks and protocols designed to mitigate risks, with the implementation of machine learning and artificial intelligence (AI) applications in threat detection and response.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a comprehensive approach to managing and reducing cybersecurity risk. It consists of five core functions: Identify, Protect, Detect, Respond, and Recover (Liu, et al., 2024). These functions guide organizations in understanding and managing their cybersecurity risks in a structured and systematic manner. The framework also emphasizes the importance of risk assessment, continuous monitoring, and incident response planning.

The ISO/IEC 27001 standard is an internationally recognized framework for information security management. It provides a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability. The standard outlines requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). Adopting ISO/IEC 27001 helps organizations demonstrate their commitment to security and compliance with regulatory requirements (Podrecca, et al., 2024).

Machine learning (ML) has revolutionized threat detection by enabling the analysis of vast amounts of data to identify patterns and anomalies indicative of cyber threats. Traditional security systems often rely on signature-based detection, which can be ineffective against new and unknown threats. ML algorithms, on the other hand, can detect previously unseen threats by learning from historical data and identifying deviations from normal behavior. Techniques such as anomaly detection, clustering, and classification are commonly used in ML-based security systems to enhance threat detection capabilities.

Artificial intelligence (AI) enhances incident response by automating the detection and mitigation of cyber threats. AI-powered systems can analyze and correlate data from multiple sources in real-time, enabling faster and more accurate identification of incidents (Zhang, et al., 2022). Automated response actions, such as isolating compromised systems, blocking malicious traffic, and deploying patches, help mitigate the impact of cyber-attacks and reduce the response time. AI also plays a critical role in threat hunting, allowing security teams to proactively search for signs of compromise within their networks.

Blockchain technology offers a decentralized and tamper-evident ledger system that can enhance data integrity and transparency. Each block in a blockchain contains a cryptographic hash of the previous block, a timestamp, and transaction data, making it nearly impossible to alter the information without detection. Blockchain's applications in cybersecurity include securing transactions, ensuring the authenticity of digital records, and providing transparent and immutable audit trails (Saleh, 2024). By leveraging blockchain, organizations can enhance trust and accountability in their digital interactions.

Quantum computing represents a paradigm shift in computational power, with the potential to solve complex problems that are currently infeasible for classical computers. While quantum computing poses a threat to existing cryptographic methods, it also offers opportunities for developing new, more secure cryptographic techniques (Chawla & Mehra, 2023). Quantum-resistant algorithms are being researched to withstand the capabilities of quantum computers. Understanding the implications of quantum computing is crucial for future-proofing cybersecurity strategies and ensuring long-term protection of sensitive information.

4. Case Studies and Practical Implications

Many large firms all over the world, have been hit by a breach that may have disclosed highly sensitive information about its customers. Besides that, ransomware attacks happen every day not only to legal entities but also to individual users. Governments and regulatory bodies worldwide are establishing standards and regulations to enhance cybersecurity and protect privacy. Notable examples include the General Data Protection Regulation (GDPR) in Europe and the Cybersecurity Information Sharing Act (CISA) in the United States. Ethical considerations play a crucial role in cybersecurity, as organizations must balance the need for robust security with the protection of individual privacy rights, so their cybersecurity practices adhere to ethical principles, such as transparency, accountability, and respect for privacy.

In Deloitte case, hackers gained access to Deloitte's email system via an inadequately secured administrative account. This email system was hosted on Microsoft's Azure cloud service and was first successfully attacked in October or November 2016. This meant the attackers had access to emails, potentially containing highly sensitive communications between Deloitte and its clients, as well as between Deloitte employees, for nearly a year. The admin account used just a simple password for authentication (Data breaches, 2017).

The Equifax data breach, which occurred in 2017, exposed the personal information of approximately 147 million people. The breach resulted from a vulnerability in the Apache Struts web application framework, which Equifax failed to patch in a timely manner. Attackers exploited this vulnerability to gain access to sensitive data, including names, Social Security numbers, birth dates, addresses, and driver's license numbers. The incident highlighted the importance of timely patch management, robust vulnerability scanning, and proactive threat monitoring (Data breaches, 2017).

The WannaCry ransomware attack, which spread globally in 2017, affected hundreds of thousands of computers across various industries, including healthcare, finance, and government. WannaCry exploited a vulnerability in the Windows operating system, leveraging the EternalBlue exploit to propagate rapidly. The attack encrypted data on infected systems, demanding ransom payments in Bitcoin for decryption. The widespread impact of WannaCry underscored the necessity of regular software updates, robust backup solutions, and effective incident response planning (Akbanov, et al., 2019).

5. Best Practices and Strategic Recommendations

There are different methods that can be used to minimize cybersecurity issues but several can be distinguished: risk assessment and management, secure software development lifecycle (SDLC), multi-factor authentication (MFA) and continuous monitoring and incident response.

Cybersecurity actions begin with a thorough risk assessment with the purpose of identifying potential threats and vulnerabilities. Organizations should periodically conduct risk assessments to evaluate the probability and impact of different threats. This process involves identifying critical assets, assessing the effectiveness of existing security measures, and ranking risks based on their potential impact. In this way, organizations can allocate resources effectively and implement adequate security measures.

Implementing an SDLC is essential for minimizing vulnerabilities in software products. The SDLC integrates security practices throughout the software development process, from design to deployment. Key practices include threat modeling, secure coding standards, code reviews, and vulnerability testing. By incorporating security early and continuously, organizations can reduce the risk of introducing vulnerabilities and ensure the development of secure software.

MFA enhances security by requiring multiple forms of verification for user authentication. MFA typically combines something the user knows (e.g., a password), something the user has (e.g., a mobile device), and something the user is (e.g., a fingerprint) (Almadani, et al., 2023). Implementing MFA significantly reduces the risk of unauthorized access, even if one factor is compromised. Organizations should adopt MFA for all critical systems and encourage its use across their user base.

Continuous monitoring involves the ongoing collection and analysis of security data to detect and respond to threats in real-time. Security Information and Event Management (SIEM) systems play a crucial role in continuous monitoring by aggregating and analyzing logs from various sources. Incident response planning is also critical for minimizing the impact of security incidents. Organizations should develop and regularly update their incident response plans, conduct simulated exercises, and ensure that their security teams are well-trained and prepared to respond to incidents.

6. Conclusion

The trend of industry digital transformation besides benefits like: higher levels of efficiency and productivity, enhanced data collection, quality improvements to products and services, etc. has brought system weaknesses in the form of sophisticated cyber-attacks such as APTs, ransomware, and zero-day exploits, which implicates the need for robust cybersecurity measures. Inherent vulnerabilities in computing architectures, including insecure coding practices, inadequate encryption standards, and flawed authentication mechanisms, further aggravate these challenges.

Advancements in artificial intelligence can be implemented for threat detection and incident response, enabling more proactive and adaptive security measures. Emerging technologies, like blockchain and quantum computing, offer both opportunities and challenges for cybersecurity. By synthesizing current research findings and industry practices, this paper proposes best practices and strategic recommendations for fortifying the cybersecurity posture of computing systems.

By analyzing challenges and future directions in cybersecurity, we aim to contribute to the development of more resilient and secure computing environments. This paper provides a comprehensive guide for enhancing cybersecurity in the digital world.

Acknowledgments

The research in this work was funded by the project entitled "Continuous Improvement of DIIM Teaching Processes Through the Implementation of the Results of Scientific Research Work in the Field of Industrial Engineering and Management".

REFERENCES

[1] Akbanov, A., Vassilakis, V. G., & Logothetis, M. D. (2019). Ransomware detection and mitigation using software-defined networking: The case of WannaCry. *Computers & Electrical Engineering*, *76*, 111–121. https://doi.org/10.1016/j.compeleceng.2019.03.012.

[2] Almadani, M.S., Alotaibi, S., Alsobhi,H., Hussain, O.K., Hussain, F.K. (2023). Blockchain-based multi-factor authentication: A systematic literature review. *Internet of Things*, *23*(100844). https://doi.org/10.1016/j.iot.2023.100844.

[3] Buckbee, M. (2023). *What is an Advanced Persistent Threat (APT)?* https://www.varonis.com/blog/advanced-persistent-threat

[4] Chawla, D., & Mehra, P. S. (2023). A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions. *Internet of Things*, *24*(100950). https://doi.org/10.1016/j.iot.2023.100950.

[5] Data breaches: Deloitte suffers serious hit while more details emerge about Equifax and Yahoo, (2017). *Computer Fraud & Security*, *2017*(10), 1–3. https://doi.org/10.1016/S1361-3723(17)30086-6.

[6] https://doi.org/10.1016/j.compind.2022.103744.

[7] Liu, L., Sajid, Z., Kravaris, C., & Khan, F. (2024). Detection and analysis of cybersecurity challenges for processing systems. *Process Safety and Environmental Protection*, *185*, 1061–1071. https://doi.org/10.1016/j.psep.2024.03.088.

[8] Olson, R., Ligh, M., Sinclair, G., Hartstein, B., Sudusinghe, S., Gary, J., Falcone, R., De Mata, A., Smith, R., & Lawrence, A. (2011). *Cyber Security Essentials*. Taylor & Francis Group, LLC.

[9] Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001, *Computers in Industry*, *142*(103744).

[10] Saleh, A. S. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. *Blockchain: Research and Applications*, 100193. https://doi.org/10.1016/j.bcra.2024.100193

[11] Verma, R. (2024). Cybersecurity Challenges in the Era of Digital Transformation, In *Transdisciplinary Threads Crafting The Future Through Multidisciplinary Research Volume – 1* (pp. 178–186). Infinity Publication PVT. LTD.

[12] Zhang, Z., Ning, H., Shi, F. Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.C. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, *55*, 1029–1053. https://doi.org/10.1007/s10462-021-09976-0.