Jurnal Minfo Polgan
Volume 13, Nomor 1, 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i1.13490 p-ISSN : 2089-9424

Terbit : 13 Februari 2024

The Significant Rise In Cybercrime Can Be Attributed To Vulnerabilities In Cybersecurity

[1] Ellanda Purwawijaya, [2] Dinur Syahputra, [3]Aripin Rambe, [4] Junerdi Nababan
[1, 2,3]Universitas Battuta, [4]Universitas Mahkota Tricom Unggul

[1]ellanda.purwa.wijaya@gmail.com, [2]dinsyahui12@gmail.com, [3]arambe1903@gmail.com,
[4]junerdin@gmail.com

ABSTRAK

In today's world, our dependence on computers extends to even the most basic daily tasks. As users, we consistently engage with computers for activities such as communication, data sharing, information retrieval, social interactions, and more, all conducted over networks. It is evident that the network connecting various devices globally, including servers, computers, laptops, mobile phones, etc., serves as the fundamental technology facilitating these tasks. However, this interconnected system poses a significant threat in the form of cybercrime. Despite the implementation of cybersecurity measures throughout the network, there exist flaws and obstacles that compromise security, leading to the occurrence of these crimes. One can envision the relationship between cybercrime and cybersecurity as a ratio, with cybercrime holding the higher value. This variable is steadily increasing at a greater rate than cybersecurity, indicating a growing imbalance between the two.

Keyword: Cybercrime, Cyber security, Phishing, Malware.

INTRODUCTION

Data is transferred in various forms, including audio, video, emails, and textual formats. However, consideration is rarely given to whether the data involved is secure or if it is traveling through a protected pathway. In this context, individuals or users utilizing these network services may or may not possess awareness of this interconnected aspect. Currently, a significant proportion of transactions occurs on the network, with approximately 60% to 80% of the population consistently being online.(Marcum & Higgins, 2019)

Given all these situations and conditions, there is a necessity for enhanced security, specifically the implementation of cybersecurity, to address the vulnerabilities that may lead to the occurrence of cybercrime. With technology advancing daily, encompassing fields such as Data Analytics, data science, AI, cloud computing, electronic commerce, etc., it involves highly crucial information that necessitates a high level of cybersecurity. (Huber & Huber, 2019)

However, with the rise in the information and technology sector, there is a corresponding increase in cybercrimes. Pinpointing the precise cause of these cybercrimes is nearly impossible. Therefore, there is a necessity for a straightforward and comprehensive paradigm or technique to mitigate the occurrence of such unfavorable scenarios, which adversely impact various fields, organizations, institutions, and industries involved. (Ehimen & Bola, 2010)

LITERATURE REVIEW

Cybercrime constitutes a deliberate effort involving computers, networks, or electronic devices, with the intention to disrupt or harm the progress, reputation, economy, physical well-being, or mental state of an individual or a group. Individuals engaging in these unlawful activities are referred to as cybercriminals or cyber offenders. Security measures are evaluated based on how data is stored, encoded, transmitted, encrypted, and deleted. Numerous statistics indicate that companies prioritize the security of individual data with great importance. (Thakur et al., 2015)

Cybercrime, synonymous with computer crime, encompasses various illicit activities.

Examples of cybercrime include stealing information, committing e-commerce fraud, engaging in illegal transactions—both monetary and non-monetary—hacking, copyright infringement, information leakage, and numerous other offenses. Cybercrime can be categorized in two primary ways: 1. Crimes originating from the computer system itself. 2. Utilization of computers in the evolution of existing crimes. Crimes stemming from the computer system include disruptions to network systems, unauthorized invasions, or recordings. (Kaur & Ramkumar, 2022)

The evolution of existing crimes using computers encompasses activities such as personal information theft, cyber threats, child abuse, impersonation, and stalking. The widespread integration of technology into people's lives has significantly escalated cybercrime. Consequently, preventive measures must be implemented to address these cybercrimes, leading to the concept of cybersecurity.(Gunduz & Das, 2020)

RESEARCH METHODS

Primary cybercrimes or cyberattacks

1. Compromised business emails involve unauthorized access to a trusted business person's email account, enabling the perpetrator to assume their identity and carry out fraudulent activities such as requesting payments. (Sarker et al., 2020)
2. Phishing disguises itself as a legitimate source but is actually fraudulent. It deceives individuals into providing their personal information either through form submissions or by enticing them to click on a link.
3. Malware refers to malicious software that infiltrates your system through infected links or by clicking on images in emails or web applications. Once installed, this software operates discreetly in the background, causing harm to your system without your knowledge of its presence or activities.
4. Social engineering involves the exploitation of social websites where users interact with systems or other individuals. However, some of these social platforms are utilized for manipulation, aiming to obtain or access personal information, contact details, data, and even monetary assets, among other things.
5. Frauds involving credit and debit cards have seen a significant increase in recent years, with millions of credit card details being stolen and subsequently used by unauthorized individuals.
6. Hacking enables a hacker to gain full access to the targeted computer system. It has been proven to be one of the most dangerous situations for an organization.

Cyber Security

Measures are implemented to enhance cybersecurity and diminish illegal activities conducted over networks using computer systems or electronic devices with communication capabilities. These measures are the sole reason for the internet's survival to date. Every organization, regardless of its size, operating on the internet necessitates some form of security against various threats such as fraud, theft, invasion, and more. Cybersecurity can be viewed as a precautionary measure adopted by institutions subsequent to their encounter with any newly emerging cybercrime or attack. (Safitra et al., 2023)

We can assert that the implementation of cybersecurity serves as a precautionary measure employed by technical societies or organizations. It is imperative for organizations to implement cybersecurity in a highly effective manner. This is because cybersecurity acts as a protective shield against various cyberattacks and cybercrimes. Cybersecurity implementation can be viewed as a precautionary measure adopted by technical societies or organizations. It is essential for organizations to execute cybersecurity measures with utmost excellence. This is because cybersecurity serves as a protective barrier against various cyberattacks and cybercrimes. (Hasan et al., 2023)

Cyber Security

Cybersecurity can be implemented in two ways, namely: 1. Individually, on a small scale.
2. By organizations, on a larger scale. At an individual level, whether using applications offline or online, it is essential to create a unique authentication user ID and password that are not easily

decrypted. One must be mindful of how and from where network services are accessed. Additionally, it is important to log out from the system once the task is completed. At the organizational level, as a larger entity, it is crucial for organizations to thoroughly examine all aspects of cyber attacks or cybercrimes during the implementation of cybersecurity measures. Moreover, organizations must fortify their systems to effectively combat future cyber threats that may arise at any moment.(Lallie et al., 2021)

Organizations Ways To Approach Cyber Security

As the organization stores information digitally, ensuring data privacy and security is their priority. Through the implementation of cybersecurity measures, the organization aims to establish a secure workspace that is also user-friendly, enabling tasks to be performed securely and efficiently. Nearly every company and organization is prioritizing the enhancement, management, and updating of cybersecurity alongside their other responsibilities, including resource allocation and service expansion. Neglecting to assess the current situations and scenarios regarding data before implementing cybersecurity measures is deemed imprudent. (Wayahdi et al., 2021)

The techniques utilized for cybersecurity include the following:

1. Password Security and Access Control

This involves employing unique user identification and passwords to safeguard against unauthorized access, serving as the primary line of defense for cybersecurity.

2. Antivirus Software

These software systems are designed to monitor computer systems, detecting and preventing computer viruses and malicious software programs. Additionally, they offer protection against worms, Trojans, and various other cyber threats.

3. Firewall

A firewall, whether software-based or hardware-based, is designed to serve as a security barrier between your computer system and the network. It aims to safeguard your system from breaches, hackers, viruses, worms, and prevents unauthorized entities from gaining access to your system.

4. Malware Scanners

Malware scanners are employed to search for malware by scanning all forms of data, including documents and files, to identify any potential security threats posed by malware.

5. Data Authentication

Data transferred and received must undergo verification to ensure it originates from a trusted and authorized source that is reliable. Additionally, during data transmission, measures must be taken to prevent manipulation or alteration. This authentication process can be facilitated by tools such as antivirus software.

RESULTS AND DISCUSSION

Results:

In the advancing digital era, cybercrime has emerged as a serious threat to individuals, businesses, and even governments worldwide. The significant increase in cybercrime can directly be attributed to vulnerabilities in cybersecurity. These vulnerabilities provide opportunities for cybercriminals to infiltrate, sabotage, or steal sensitive data online.

1. Increasing Reliance on Technology: Modern society is becoming increasingly dependent on technology for various activities, from financial transactions to communication. This makes us more vulnerable to cyber attacks due to the growing amount of data stored and accessed online.

2. Evolving Methods of Attack: Cybercriminals continue to develop methods and tools to breach security systems. With increasingly sophisticated technology, they can easily find loopholes in cybersecurity and exploit them for personal gain or other malicious purposes.

3. Lack of Security Awareness: Many individuals and organizations lack awareness of the importance of cybersecurity and fail to take adequate measures to protect themselves. This lack of awareness provides opportunities for cybercriminals to succeed in their attacks more easily.

4. Complexity of IT Infrastructure: The increasing complexity of information technology (IT) infrastructure makes it vulnerable to cyber attacks. With numerous devices and networks

interconnected, security vulnerabilities can arise at various points, providing opportunities for cybercriminals to strike.

5. Gap in Defense: Despite many organizations investing in cybersecurity, there is still a gap between the attacks carried out by cybercriminals and the defensive capabilities of these organizations. This results in successful attacks even on companies with robust cybersecurity systems.

Discussion:

The significant increase in cybercrime and vulnerabilities in cybersecurity indicate the need for more serious steps to protect ourselves from cyber attacks. Some steps that can be taken include increasing awareness of cybersecurity at all levels, investing more resources in developing strong security systems, and enhancing cooperation between the public and private sectors to combat cybercrime. With these collective efforts, we can reduce the risk of cyber attacks and create a safer and more reliable online environment for everyone.

CONCLUSION

Data integrity involves safeguarding information from unauthorized modification by third parties. Information holds value only when it remains accurate; tampered data can incur significant costs for both the sender and the recipient. Cybercrime often outpaces cybersecurity, even with the implementation of top-tier security measures. Instances of cybercrime can lead to substantial destruction, sometimes resembling cyber warfare.

Both technology users and providers should never assume that their security systems are sufficient to defend against all types of cyberattacks. Cybercriminals continually devise new methods to exploit vulnerabilities in established security systems. In our experience, no technology exists without any loopholes to date.

As individuals and organizations, we must be ready to face any threats and attacks over the internet that could result in losses across various aspects including physical, emotional, social, mental, and economic dimensions.

The significant increase in cybercrime is directly linked to vulnerabilities in cybersecurity. This phenomenon becomes more pronounced with the rapid advancement of technology and our increasing reliance on digital infrastructure. Vulnerabilities in cybersecurity create opportunities for cybercriminals to launch attacks, steal sensitive data, and disrupt vital online services. Factors such as lack of awareness of cybersecurity, inadequate investment in defense systems, and the gap between cyberattacks and existing defenses further exacerbate this situation. Therefore, there is a need for more serious and collaborative efforts from various parties, including individuals, businesses, and governments, to address vulnerabilities in cybersecurity and protect themselves from cybercrime threats. With the right and coordinated actions, we can create a safer and more reliable digital environment for everyone.

REFERENSI

Ehimen, O. R., & Bola, A. (2010). Cybercrime in Nigeria. *Business Intelligence Journal*, *3*(1), 93–98.

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

Hasan, M. K., Habib, A. K. M. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network and Computer Applications*, *209*, 103540.

Huber, E., & Huber, E. (2019). *Cybercrime*. Springer.

Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766–5781.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers \& Security*, *105*, 102248.

Marcum, C. D., & Higgins, G. E. (2019). *Cybercrime*. Springer.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369.

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, *7*, 1–29.

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015). An investigation on cyber security threats and security models. *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, 307–311.

Wayahdi, M. R., Ginting, S. H. N., & Syahputra, D. (2021). Greedy, A-Star, and Dijkstra's Algorithms in Finding Shortest Path. *International Journal of Advances in Data and Information Systems*, *2*(1), 45–52. https://doi.org/10.25008/ijadis.v2i1.1206