Jurnal Informasi dan Teknologi

https://jidt.org/jidt

2024 Vol. 6 No. 2 Hal: 204-208 e-ISSN: 2714-9730

Analysis of Cyber Attacks on Network Security

Fauzan Prasetyo Eka Putra✉, Ubaidi, Senah Anggreni Amba Sugi, Khafifatul Mufidah, ,Yayu Rahma Febriani

Department of Informatics, Faculty of Engineering, Universitas Madura

prasetyo@unira.ac.id

Abstract

Network security is a crucial issue in today's digital era, with increasing cyber attacks targeting infrastructure and sensitive data. Analysis of cyber attacks on network security is an important aspect of efforts to protect information systems from ever-evolving digital threats. This research investigates various types of cyberattacks that can threaten network security, including phishing attacks, malware, denial of service (DoS), and brute force attacks. We also analyze defense methods that can be used to reduce the risk of cyberattacks, including firewalls, data encryption, real-time security monitoring, and security training for users. This research provides a deeper understanding of the current cyberattack landscape and effective strategies for reducing network vulnerabilities to such attacks. Thus, the results of this analysis can make an important contribution to improving network security in various sectors, from companies to government.

Keywords: DOS, Cyberattack , Computer Networks, Phishing, Malware

1. Introduction

In this modern era, society cannot be separated from the internet and gadgets[1]. The world of technology is experiencing massive and rapid developments in human life [2]. Globalization is developing very rapidly in many fields, including aspects of information technology related to cyber security and data sovereignty [3]. It is not surprising that information technology brings great benefits to countries in the world, helping them to prosper, progress, and improve human civilization, electronic commerce, electronic learning, internet banking, etc., but at the same time, it is an illegal activity [4].

Cyber-security a priority for every country in the world, Information technology communications are used in many aspects of life, including society, economy, law, organization, health, education, culture, government, security, and defense, etc.[5]. Therefore, it is very important to consider and anticipate cybersecurity threats [6].

Concerns about these attacks are driving governments and electronic systems providers) to improve their system protection and respond to cyberattacks [7].

According to Kominfo, Indonesia is a country that is the target of cyber attacks, with the National Cyber Code Bureau (BSSN) releasing the 2021 Cyber Security Annual Monitoring Report [8].

The threat of cybercrime is a form of modern or non-military warfare threat that is motivated by the interests of certain individuals or groups and can cause the collapse of a nation [9]. Many cyber security attacks are carried out by criminal groups with financial motivations [10].

Computer crime is the dark side of technological progress, which has a broad impact on every aspect of modern life [11]. In the real world, someone can break into someone else's house and take valuables from that person's house [12], but in the virtual world, someone can access another person's computer or computer network and steal data. worth that person [13]. The scope of cyber security includes security tools, policies, and concepts that can be used to protect all company resources and users [14].

Cybercrime or cybercrime poses a serious challenge to society and is dangerous for the individuals and organizations affected [15]. Increasing public awareness of the potential for cybercrime must be a concern in every activity in the digital space, especially cyberspace [16].

2. Research Methods

The method used is a literature study. Literature study is a method of collecting data or sources related to the topic being discussed in research [17].

a. Cyber Attack

Increasing public awareness of the potential for cybercrime must be a concern in every activity in the digital space, especially cyberspace [18]. This is because each service stores sensitive usage information[19]. The disadvantage of this cyber threat is that the perpetrator can freely take over the victim's account, the account could be a credit card, online transaction tools such as Dana, OVO, mobile banking, etc. [20].

Receipt: 30-11-2023 | Revision: 26-06-2024 | Publish: 04-07-2024 | doi: 10.60083/jidt.v6i2.569

A cyber attack is an attempt by an unauthorized person to gain access to a computer system or network and damage or steal information [21]. These attacks can include a variety of techniques, including malware, phishing, passwords, ransomware, and denial of service (DoS)[22].

Apart from these attacks, there are many other types of cybercrime attacks such as spoofing attacks, man-in-the-middle attacks, and many more[23].

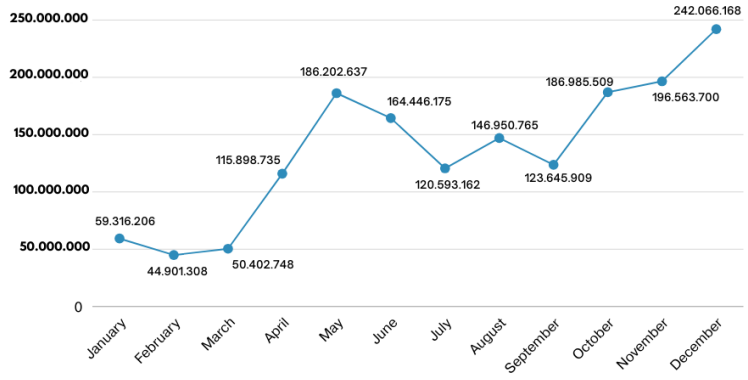

Figure 1. 2021 Cyber Attack Graph

Based on the National Cyber Security Index (NCSI) report, Indonesia's Cyber Security Index score in 2022 is 38.96 out of 100. This value places Indonesia in the third lowest position among the G20 countries. Indonesia is currently ranked 83rd in the world out of 160 countries listed in the report[24].

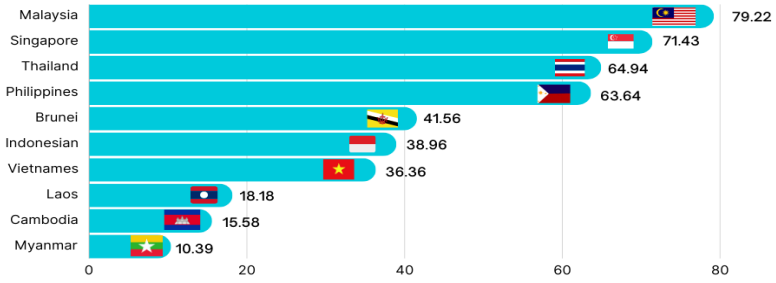

Figure 2. Cyber Rankings in Countries

The number of social media hacking attacks has increased significantly in recent years, reaching more than 10 million attacks in 2022, according to data from a cybersecurity company[25].

b. Cyber Security

Cybersecurity is a set of tools, guidelines, security principles, safeguards, recommendations, opportunity management strategies, movement, training, first-class applications, assurance, and Information that includes technical knowledge [26].

Cybersecurity also includes all processes carried out to maintain and reduce data protection, integrity, and availability of existing data. This process requires protecting each information system from various physical and cyber attacks.

Cyber-security is an effort to protect information from cyber-attacks. Below are some of the main elements of cyber security:

1. Information infrastructure, namely intermediaries supports the continuity of the information manipulation process, including hardware and software. These---include routers, switches, servers, operating systems, and databases.
2. Perimeter defense is a useful intermediary for defending information infrastructure components such as IDS, IPS, and firewalls [26].

c. Computer network

A computer network is a relationship between two or more computers connected via cable or wireless transmission media [27].

Public Internet and worldwide computer networks are inherently insecure. When data is sent from one computer to another over the Internet, it is sent to many other computers, allowing other Internet users to intercept or modify the data[28].

3. Result & Discussion

With technological advances, the global security dimension that developed in the horizontal era of the 21st century also extends to the cyber dimension [29].
The National Cyber Security Strategy study found that the threat of cybercrime includes endangering the confidentiality, integrity, and availability of systems and information [30]. Cybercrime activities include denial of service/DOS attacks, hacking, virus/Trojan distribution, cyber terrorism, and fraud, identity theft/phishing[31]. The challenges involved in navigating cyberspace include the rapidly evolving complexity of cybersecurity, ethical dilemmas, and the strategies required to manage these changes [32].
Computer networks need to be secured to avoid cyber attacks. Regularly update the Operating System (OS) to avoid cyber attacks. An old version of the Operating System can be an opening for hackers to enter and manipulate computer networks. There are various types of cyber attacks, namely:

1. Denial of Service Attack / DOS Attack
   A denial of service attack is an attack that floods a server with traffic or requests for large amounts of data to the server, to bring down the web network system so that the server is unable to provide service and crash attacks carried out by hackers [33]. DoS is an attack that can cause severe damage to a system [34].
2. Phishing
   Phishing is a way of obtaining information about someone's data by using phishing techniques [35]. The most common forms of phishing are email phishing, SMS, phone calls, web phishing, and pop-ups on unsecured websites [36]. This data is an "easy" target for cybercriminals when escalating phishing crimes [37].
3. Malware
   Malware or Malicious Software is a program that damages a system to carry out various activities that are detrimental to its owner [38]. These losses slow down your system and damage and destroy important stored data [39].

Above are several types of cyber attacks. Developing a strong security system is key to combating increasingly complex and evolving threats [40].

4. Conclusion

The world technology is experiencing massive and rapid development in human life. Globalization is developing very rapidly in many fields, including aspects information technology related to cyber-security and data sovereignty. Network cyber security in cyber attacks is very necessary. Attacks have several types, namely: phishing, malware, Denial of Service Attack / DOS Attack, etc. This can be minimized by sharing knowledge with the public about cyber attacks.

References

[1] S. Media, K. Siswa, S. Smk, and P. Bangsa, "Praxis : Jurnal Pengabdian Kepada Masyarakat," vol. 4, no. 1, pp. 8–12, 2024.
[2] A. B. Prasetyo, T. Andrian, and Khoirunnisya, "Pelatihan Kriptografi Dasar Dan Edukasi Keamanan Siber Di SMK Puspita Bangsa Ciputat," vol. 4, no. 1, pp. 35–39, 2024.
[3] M. P. Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]," *J. Polit. Din. Masal. Polit. Dalam Negeri dan Hub. Int.*, vol. 13, no. 2, pp. 222–238, 2023, doi: 10.22212/jp.v13i2.3299.
[4] V. S. Ginting, E. Benna, P. Manurung, C. Crime, and C. Crime, "Penerapan Kebijakan Digital Dalam Rangka," pp. 249–253, 2016.
[5] Y. Ginanjar, "Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara," *J. Din. Glob.*, vol. 7, no. 02, pp. 291–312, 2022, doi: 10.36859/jdg.v7i02.1187.
[6] U. B. Darma, "MENDESAIN CYBER SECURITY UNTUK KEAMANAN WEBSITE MENGGUNAKAN WEB APLICATION FIREWALL PADA KANTOR BKPSDM This work is licensed under a Creative Commons Attribution-," vol. 2, no. 4, pp. 386–395, 2024.
[7] M. S. Abdullah and I. H. Ikasari, "Perkembangan Terbaru Dalam Keamanan Siber, Ancaman Yang Diidentifikasi Dan Upaya Pencegahan," *JRIIN J. Ris. Inform. dan Inov.*, vol. 1, no. 1, pp. 96–98, 2023.
[8] M. Y. Samad and Pratama Dahlian Persadha, "Memahami Perang Siber dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman di Siber," *J. IPTEKKOM J. Ilmu Pengetah. Teknol. Inf.*, vol. 24, no. 2, pp. 135–146, 2022, doi: 10.17933/iptekkom.24.2.2022.135-146.
[9] S. Ariyaningsih, A. A. Andrianto, A. surya Kusuma, and Rezi, "Korelasi Kejahatan Siber Dengan

PercepatanDigitalisasi Di Indonesia," *J. Ilmu Huk. Univ. Pas.*, vol. 1, pp. 1–12, 2023.
[10] P. Hukum, T. Tindak, and P. Siber, "Submitted: 16 December 2023 Accepted: 25 December 2023," vol. 1, pp. 8–20, 2023.
[11] A. Umbara and D. A. Setiawan, "Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19," *J. Ris. Ilmu Huk.*, pp. 81–88, 2022, doi: 10.29313/jrih.v2i2.1324.
[12] T. Yusnanto, "Training And Recognition of The Importance of Cybersecurity For Umkm In Entering The Digital Market," *Teumulong J. Community Serv.*, vol. 1, no. 2, pp. 66–73, 2023, doi: 10.62568/jocs.v1i2.11.
[13] R. Syah, "Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber," *J. Impresi Indones.*, vol. 2, no. 9, pp. 864–870, 2023, doi: 10.58344/jii.v2i9.3594.
[14] C. Vania, M. Markoni, H. Saragih, and J. Widarto, "Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber," *J. Multidisiplin Indones.*, vol. 2, no. 3, pp. 654–666, 2023, doi: 10.58344/jmi.v2i3.157.
[15] R. Butarbutar, "Kejahatan Siber Terhadap Individu: Jenis, Analisis, DanPerkembangannya," *Technol. Econ. Law J.*, vol. 2, no. 2, pp. 299–317, 2023.
[16] K. K. Yustisia, A. D. Winarsih, M. Lailiyah, A. N. Yudhawardhana, A. S. Binatoro, and Q. Arifah, "Edukasi Literasi Digital Siswa Sekolah Dasar Tentang Strategi Keamanan dan Manajemen Siber," *GERVASI J. Pengabdi. Kpd. Masy.*, vol. 7, no. 1, pp. 135–147, 2023, doi: 10.31571/gervasi.v7i1.4472.
[17] D. Parinata and N. D. Puspaningtyas, "Studi Literatur: Kemampuan Komunikasi Metematis Mahasiswa Pada Materi Integral," *J. Ilm. Mat. Realis. (JI-MR*, vol. 3, no. 2, p. 94, 2022.
[18] Achmad Mukhlis, Baiq Laila Alfila, and Aliya Zhafira Wastuyana, "Ancaman dan Langkah Pengamanan Sistem Informasi Menggunakan Metode Systematic Literature Review," *J. Ilm. Sist. Inf. dan Ilmu Komput.*, vol. 3, no. 2, pp. 143–152, 2023, doi: 10.55606/juisik.v3i2.496.
[19] T. Tan and B. Soewito, "Menggunakan Framework Nist Cybersecurity Di Universitas Zxc," vol. 6, no. 2, pp. 411–422, 2022, doi: 10.52362/jisamar.v6i2.781.
[20] A. Solikhawati and A. Samsuri, "Evaluasi Bank Syariah Indonesia Pasca Serangan Siber: Pergerakan Saham dan Kinerja," *J. Ilm. Ekon. Islam*, vol. 9, no. 3, p. 4201, 2023, doi: 10.29040/jiei.v9i3.10309.
[21] D. Septasari, "The Cyber Security and The Challenge of Society 5.0 Era in Indonesia," *Aisyah J. Informatics Electr. Eng.*, vol. 5, no. 2, pp. 227–233, 2023, doi: 10.30604/jti.v5i2.231.
[22] K. Dan and R. Terbaru, "Jurnal+Dienda+Causa," vol. 1, no. 5, 2023.
[23] T. G. Laksana and S. Mulyani, "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan," *J. Ilm. Multidisiplin*, vol. 3, no. 01, pp. 109–122, 2024, doi: 10.56127/jukim.v3i01.1143.
[24] Y. Daeng, J. Levin, M. Razzaq Prayudha, N. Putri Ramadhani, S. Imanuel, and A. Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia Yusuf Daeng, "Analisis Penerapan Sistem Keamanan Siber TerhadapKejahatan Siber Di Indonesia," *J. Soc. Sci. Res.*, vol. 3, no. 6, pp. 1135–1145, 2023.
[25] R. Aldiansyah, T. Informatika, U. Pamulang, and T. Selatan, "Mengukur Rentan : Evaluasi Kerentanan Terhadap Serangan Hacking di Ekosistem Media Sosial ISSN 3025-7409 (Media Online)," *JURIHUM J. Inov. dan Hum.*, vol. 1, no. 4, pp. 397–402, 2023.
[26] F. Indah and A. Q. Sidabutar, "Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)," *J. Bid. Penelit. Inform.*, vol. 1, no. 1, p. 2, 2022.
[27] C. Novira, "Program Studi D-3 Teknik Informatika Fakultas Vokasi," no. January, 2023.
[28] S. Nurul, Shynta Anggrainy, and Siska Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim)," *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, pp. 564–573, 2022, doi: 10.31933/jemsi.v3i5.992.
[29] R. Hafidz, F. D. Setiawan, and F. Sinlae, "Keamanan Cybersecurity: Strategi Geometri Politik dan Pembangunan Global Terkhusus Asia Tenggara," *Nusant. J. Multidiscip. Sci.*, vol. 1, no. 2, pp. 208–215, 2024.
[30] M. A. R. Tamhidah, "Pengaruh Media Sosial Terhadap Penyebaran Informasi Palsu Dan Kejahatan Siber," *Innov. J. Soc. Sci. Res.*, vol. 3, no. 6, pp. 9133–9147, 2023.
[31] F. Surahman, "Tantangan Dalam Menjaga Keamanan Data Official Statistics dari Serangan Cybercrime," *J. Ilm. Multidisiplin*, vol. 1, no. 11, pp. 904–907, 2023.
[32] Y. Dianti, "**済無**No Title No Title No Title," *Angew. Chemie Int. Ed. 6(11), 951–952.*, pp. 5–24, 2017, [Online]. Available: http://repo.iain-tulungagung.ac.id/5510/5/BAB 2.pdf
[33] U. Ubaidillah, T. Taryo, and A. Hindasyah, "Analisis dan Implementasi Honeypot Honeyd Sebagai Low Interaction Terhadap Serangan Distributed Denial Of Service (DDOS) dan Malware," *JTIM J. Teknol. Inf. dan Multimed.*, vol. 5, no. 3, pp. 208–217, 2023, doi: 10.35746/jtim.v5i3.405.
[34] H. Ramli and M. Y. Alifsyah, "Analisis Keamanan Komputer Terhadap Serangan Distributed Denial of Service (DDOS)," *J. Renew. Energy Smart Device*, vol. 1, no. 1, pp. 25–30, 2023, doi: 10.61220/joresd.v1i1.235.
[35] Wahyu Hidayat M *et al.*, "Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar," *Vokatek J. Pengabdi. Masy.*, vol. 1, no. 1, pp. 28–33, 2023, doi: 10.61255/vokatekjpm.v1i1.29.
[36] F. P. Eka Putra, A. Baidawi, A. A. Mubarok, and Frediyanto, "Merancang Jaringan Sensor Nirkabel dan IoT untuk Kota Pintar Pamekasan," *J. Inf. dan Teknol.*, vol. 5, no. 2, pp. 138–145, 2023, doi: 10.37034/jidt.v5i2.331.
[37] A. Zulfikri, F. P. E. Putra, M. A. Huda, H. Hasbullah, M. Mahendra, and M. Surur, "Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Filtering Firewall Dengan Port Blocking," *Digit. Transform. Technol.*, vol. 3, no. 2, pp. 857–863, 2023, doi: 10.47709/digitech.v3i2.3379.
[38] F. Prasetyo and E. Putra, *Jaringan Komputer Untuk Pemula*, no. March. 2024.

[39] F. P. Eka Putra, M. N. Arifin, K. Zulfana Imam, E. Saputra, and Sofiyullah, "Pengembangan Sistem Informasi Laboratorium Terintegerasi Sistem Akademik Menggunakan Agile Scrum," *J. Inf. dan Teknol.*, vol. 5, no. 2, pp. 109–119, 2023, doi: 10.37034/jidt.v5i2.367.

[40] F. Prasetyo, M. N. Arifin, and A. Irmawan, "Optimization of Mobile Ad Hoc Network DSDV and OLSR Using Evolutionary Algorithm for Elearning induction mode," *J. Disruptive Learn. Innov.*, vol. 2, no. 1, p. 1, 2020, doi: 10.17977/um072v2i12020p1-8.