DIJEMSS: Dinasti International Journal of Education Management and Social Science
E-ISSN: 2686-6331
P-ISSN: 2686-6358
https://dinastipub.org/DIJEMSS dinasti.info@gmail.com +62 811 7404 455
DINASTI PUBLISHER
DOI: https://doi.org/10.38035/dijemss.v6i5

Security Challenges in Computer Networks and Modern Operating Systems

Gugum Gumelar[1], Weni Gurita Aedi[2]
[1]Information Technology, University of Pamulang, Tangerang City, Indonesia, gumelargugum105@gmail.com
[2]Information Technology, University of Pamulang, Tangerang City, Indonesia, dosen01906@unpam.ac.id

Corresponding Author: gumelargugum105@gmail.com[1]

Abstract: This study aims to identify and analyze the various security challenges faced in modern computer networks and operating systems. The research method used is descriptive qualitative, with data obtained from various sources, including journal articles related to computer networks and operating systems. Journal articles on network management, protocols, security, and performance, as well as research reports and case studies that address security challenges in modern computer networks and operating systems. The results show that the main challenge in maintaining the security of networks and operating systems is increasingly sophisticated and complex cyber attacks, which often go beyond the capabilities of existing security technologies. In addition, the low level of security awareness among users is a significant factor that aggravates the situation, as many users do not follow basic security practices. The study also found that effective implementation of security policies is still an unresolved issue in many organizations. Many existing policies are not implemented consistently or are not updated according to the development of new threats. By identifying these challenges, the study makes an important contribution to the development of better strategies and policies to improve the security of networks and operating systems in the future.

Keyword: Network Security, Operating Systems, Descriptive Qualitative Methods, Cyberattacks, Security Policies.

INTRODUCTION

In the hyper-connected digital age, security challenges are of paramount importance. Security in computer networks and modern operating systems has become an increasingly important issue in today's digital age. As more and more data is exchanged over networks and stored in operating systems, cybersecurity risks continue to increase. Security threats such as malware, phishing, ransomware, and Advanced Persistent Threats (APT) attacks target not only individuals but also organizations and critical infrastructure. This raises deep concerns about data protection and privacy (Aulia, Rizki, Prindiyana, & Surgana, 2023). In this period of rapid development of globalization and continued digitalization, computer network connections have become an essential element in various aspects of human life. Computer networks are nothing new almost all organizations, institutions, and digital companies utilize network connections to strengthen their operational management. (Putra, Adnyana, & Jasa 2021).

Computer networks and modern operating systems are an indispensable foundation in supporting business operations, government, and daily life in today's digital age. Ever-evolving information technology has brought greater connectivity, increased productivity and driven innovation in all aspects of life. However, along with its benefits, this progress also brings new challenges in terms of security. Increasingly complex security threats require serious attention from developers, system administrators and end users to understand and address the associated risks. In this context, protection of sensitive data, identification of system weaknesses, and implementation of stringent security practices are crucial to maintain the integrity and sustainability of existing systems. Thus, in-depth understanding and effective preventive measures are the main foundations in dealing with security challenges in this digital era (Aksenta, et al., 2023).

Cyberattacks are becoming more frequent and more complex, posing a major threat to information security. With the advancement of technology and the expansion of digitalization worldwide, there has been a significant increase in the number of ways attacks can be carried out, such as phishing, malware, and denial-of-service (DoS) attacks. This has led to more areas that are vulnerable to exploitation by attackers who take advantage of gaps in system security (Santoso, Madany, & Suryotrisongko, 2023). Even some criminal technologies are considered higher than the level of computer experts, so the security of networks and operating systems cannot be guaranteed. Because evidence in the process of computer crime is difficult to understand. There are important things that need to be done, namely doing a good job in preventing computer network security, to minimize the possibility of computer crime (Zen Munawar & Novianti Indah Putri, 2020). Like the hacker attack on Indonesia's National Data Center on June 17, 2024 highlights how vulnerable the current data security system is. The National Data Center, which stores sensitive and vital information for the continuity of government and society, is the main target for cyber criminals. This attack not only disrupted government operations but also posed a serious threat to national security and public trust. This incident shows that there are still loopholes that can be exploited by irresponsible parties (Rafli Al Ihsan & Binastya Anggara Sekti, 2024).

This increase emphasizes the need for proactive measures to secure digital infrastructure and sensitive data, including the use of strong encryption systems, continuous security monitoring, and user education to raise awareness of threats. In an era where our reliance on digital technology is deepening, mitigating risks and responding quickly to cyberattacks is crucial to maintaining global information stability and security.

METHOD

This study aims to identify the major security challenges faced in modern computer networks and operating systems as well as explore strategies that can be applied to address these challenges, providing a comprehensive and detailed overview of the phenomena under study. This study uses a descriptive qualitative approach by collecting or searching for sources of information on the internet (Assyakurrohim et al., 2022). The main focus of the study is on three main areas :

1. Understand how attack techniques evolve and their impact on network and operating system security.
2. Explore the level of user awareness about good security practices and the impact of user behavior on security.
3. Examine the effectiveness of existing security policies and obstacles to their implementation.

The source of data in this study comes from journal articles relevant to the topic of computer network security and operating systems. By identifying and analyzing these challenges, the study is expected to provide practical recommendations for improving security

in computer networks and modern operating systems. The results of this study are also expected to contribute to the development of better and more effective security strategies in the face of evolving threats. By using a qualitative descriptive approach this research will collect data through searching the latest academic literature such as Google Scholar, Media publications, and other relevant databases. Literature selection is based on inclusion criteria such as topic relevance, source credibility, and year of publication. After that the data obtained were analyzed by reading and studying in depth each literature that has been selected. The Data is then collected and analyzed for discussion and conclusions.

RESULTS AND DISCUSSION

This research identifies challenges in the security of modern computer networks and operating systems through a search of academic literature in the form of relevant journal articles. The data obtained from this analysis resulted in three main themes: increasingly sophisticated cyberattacks, low security awareness, and lack of effective security policy implementation.

Most journal articles noted a significant increase in the complexity and sophistication of cyberattacks. The most frequently mentioned attacks included:

- Phishing: This technique is becoming increasingly sophisticated with better use of social engineering to trick users into revealing personal information.
- Malware and Ransomware: Participants observed an increase in the use of malware that can infiltrate systems and ransomware that encrypts user data and demands a ransom.
- Advanced Persistent Threats (APT): Targeted and sustained APT attacks are becoming more common, especially against large organizations and critical infrastructure.

Technological advancements, such as artificial intelligence and machine learning, have been leveraged by attackers to develop more effective and difficult-to-detect attacks. Organizations need to adopt equivalent security technologies, such as AI-based intrusion detection systems, to detect and respond to these threats quickly.

This is in line with research conducted by Laksana and Mulyani explaining that artificial intelligence and machine learning have a significant role in maintaining cybersecurity. With their ability to detect, analyze and respond to attacks, security systems are becoming more effective in dealing with increasingly complex cyber threats. However, it is important to remember that artificial intelligence and machine learning are not a single solution. Collaboration between humans and technology is required to create an effective cybersecurity system that adapts quickly to new threats. Artificial Intelligence (AI) and Machine Learning (ML) enhance cybersecurity with their ability to detect, prevent and respond to attacks more efficiently (Laksana & Mulyani, 2024).

Security awareness among users remains a major challenge. Some key findings include:

1. Use of Weak Passwords: Many users still use passwords that are easy to guess or use the same password for multiple accounts.
2. Ignorance of Risks: Many users are unaware of the risks associated with their online behavior, such as clicking on suspicious links or downloading attachments from unknown emails.
3. Lack of Training and Education: Many organizations do not provide adequate security training to their employees.

Raising awareness and understanding of good security practices is key to reducing security risks. Ongoing education and training programs should be a priority for organizations. Using engaging and relevant approaches can help increase user participation and understanding.

According to the research, the socialization and education on data security and privacy in the digital era to increase public awareness and protection was carried out well and smoothly. This education equips people with the knowledge and skills to actively protect themselves. With a deeper understanding of safe practices in utilizing digital technology, individuals can reduce the risk of fraud, identity theft, and privacy intrusion that may occur. An educated public will be better prepared to face various threats in the digital world and be able to take appropriate steps to protect their data and privacy (Sihombing, Pandiangan, & Manurung, 2023).

While many organizations have security policies, their implementation is often ineffective. Some of the key issues identified are:

1. Lack of Resources: Many organizations, especially smaller ones, do not have enough resources to implement a comprehensive security policy.
2. Inadequate Training: Lack of training and professional development for IT security staff.
3. Resistance to Change: Most users and management show resistance to changes in new security policies and procedures.

To improve the effectiveness of security policies, organizations need to allocate sufficient resources and ensure that the policies are implemented consistently. Ongoing training and strong management support are also crucial. In addition, involving employees in the policy development process can help reduce resistance and improve compliance.

This is also in accordance with what Soesanto et al. revealed, that in addition to having a strong national defense, interrelated and influential legal support is also needed to deal with the threat of cybercrime (Santoso, Madany, & Suryotrisongko, 2023).

This research emphasizes the importance of a holistic approach to network and operating system security, which includes advanced technology, user awareness, and strong policies. By addressing these challenges, organizations can better protect their digital assets and reduce the risk from increasingly complex cyberattacks.

CONCLUSION

This study highlights some of the key challenges in the security of modern computer networks and operating systems, and provides a deep insight into the factors that influence the successful implementation of security strategies. Based on the analysis conducted, several important issues affecting network and operating system security can be concluded. One of the main challenges is the increasingly sophisticated cyberattacks. Types of attacks such as phishing, malware, and Advanced Persistent Threat (APT) attacks are increasingly complex and difficult to detect. This emphasizes the need for the adoption of more advanced security technologies and more responsive and adaptive detection systems to counteract these types of threats. In addition, low user awareness and understanding of security practices is a significant risk factor. Many users still lack awareness of the importance of basic security practices, such as using strong passwords and not clicking on suspicious links. To address this, continuous security education and training is necessary. By increasing user awareness, the risk of unsafe behavior can be minimized. Effective implementation of security policies is also a challenge. While many organizations have security policies in place, their implementation is often inconsistent and ineffective. The main barriers to implementation include lack of adequate resources as well as resistance to change from certain parties within the organization. Overcoming these barriers requires a strong commitment from management and the provision of sufficient resources for security policies to be implemented effectively and consistently.

Overall, addressing these challenges requires a comprehensive approach involving technology, education, and effective policies. Based on the above conclusions, here are some suggestions for improving security in modern computer networks and operating systems:

1. Security Technology Reinforcement: Organizations should invest in advanced security technologies such as AI-based intrusion detection systems, end-to-end data encryption, and regularly updated firewalls. This will help in detecting and preventing increasingly sophisticated cyberattacks.
2. Security training and education: provide comprehensive training to employees on the importance of information security and good security practices. The Program should include attack simulations, case studies, and regular training to maintain awareness and relevant skills.
3. Regular audits and monitoring: conduct regular security audits to evaluate compliance with existing security policies and identify areas that require improvement. Active monitoring of network traffic and user activity is also important for early detection of attacks.
4. Organizational and leader awareness: build a strong safety culture throughout the organization, starting from the managerial level to the factory floor. Leaders need to support and encourage compliance with security policies as well as integrate security in the overall business strategy.
5. Cooperation and collaboration: sharing information about cyber threats and best practices with the security community and business partners. This collaboration can help in developing more holistic and effective strategies in the face of evolving threats.

By implementing these suggestions, it is hoped that organizations can strengthen their defenses against cyberattacks and improve security in their modern computer networks and operating systems. These measures not only protect data and infrastructure, but also build stakeholder confidence in the overall operation of Information Technoloy.

REFERENCE

Admin. (2023). Pengertian, Fungsi, Dan Jenis Sistem Operasi. *Pengertian, Fungsi, Dan Jenis Sistem Operasi*.

Aksenta, A., Irmawati, Hayati, N., Sepriano, Herlinah, Silalahi, A. T., Pipin, S. J., Abdurrohim, I., Boari, Y., Mardiana, S., Sutoyo, M. N., Sumardi, Gani, I. P., & Ginting, T. W. (2023). LITERASI DIGITAL: Pengetahuan & Transformasi Terkini Teknologi Digital Era Industri 4.0 dan Sociaty 5.0. In *Perspektif* (Vol. 1, Issue 2).

Anastasya Zalsabilla Hermawan, M. Novianto Anggoro, Ditha Lozera, & Asif Faroqi. (2023). STUDI LITERATUR: ANCAMAN SERANGAN SIBER ARTIFICIAL INTELLIGENCE (AI) TERHADAP KEAMANAN DATA DI INDONESIA. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, *3*(1), 581–591. https://doi.org/10.33005/sitasi.v3i1.363

Arfan Dwi Madya, Bagas Djoko Haryanto, & Devi Putri Ningsih. (2023). Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity. *Indonesian Journal of Education And Computer Science*, *1*(3), 127–135. https://doi.org/10.60076/indotech.v1i3.236

Aulia, B. W., Rizki, M., Prindiyana, P., & Surgana, S. (2023). Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital. *JUSTINFO | Jurnal Sistem Informasi Dan Teknologi Informasi*, *1*(1), 9–20. https://doi.org/10.33197/justinfo.vol1.iss1.2023.1253

Babys, J. Y., Kusrini, & Sudarmawan. (2013). Analisis Aspek Keamanan Informasi Jaringan Komputer (Studi Kasus : STIMIK Kupang). *Seminar Nasional INformatika 2013*.

Elan Maulani, I., & Faisal umam, A. (2023). Evaluasi Efektivitas Sistem Deteksi Intrusi Dalam Menjamin Keamanan Jaringan. *Jurnal Sosial Teknologi*, *3*(8), 662–667. https://doi.org/10.59188/jurnalsostech.v3i8.907

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). ANALISIS RISIKO TEKNOLOGI INFORMASI PADA BANK SYARIAH : IDENTIFIKASI ANCAMAN DAN

TANTANGAN TERKINI. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *5*(2), 87–100. https://doi.org/10.47435/asy-syarikah.v5i2.2022

Fitria, E. Y., & Mutijarsa, K. (2023). Survei Penelitian Metode Kecerdasan Buatan untuk Mendeteksi Ancaman Teknologi Serangan Siber. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*(6), 1185–1196. https://doi.org/10.25126/jtiik.1067341

Glen Maxie Taberima, & Ramayanti, D. (2024). MENGOPTIMALKAN MANAJEMEN DAN KEAMANAN TI MELALUI IMPLEMENTASI LAYANAN DOMAIN ACTIVE DIRECTORY STUDI KASUS PADA INFRASTRUKTUR TI PERUSAHAAN. *Jurnal Informatika Teknologi Dan Sains (Jinteks)*, *6*(1), 79–89. https://doi.org/10.51401/jinteks.v6i1.3884

Hafid, M., Firjatullah, F. Z., Pamungkaz, B. W., Magister, S., Hukum, I., Wijaya, U., & Surabaya, K. (2023). Tantangan Menghadapi Kejahatan Cyber dalam Kehidupan Bermasyarakat dan Bernegara Muhammad. *Pendidikan Tambusai*, *7*(2), 9548–9556.

Laksana, T. G., & Mulyani, S. (2024). PENGETAHUAN DASAR IDENTIFIKASI DINI DETEKSI SERANGAN KEJAHATAN SIBER UNTUK MENCEGAH PEMBOBOLAN DATA PERUSAHAAN. *Jurnal Ilmiah Multidisiplin*, *3*(01), 109–122. https://doi.org/10.56127/jukim.v3i01.1143

Oktaviani, S., Rizky, F., & Gunawan, I. (2023). Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES). *Jurnal Media Informatika*, *4*(2), 97–101. https://doi.org/10.55338/jumin.v4i2.435

Prasetia, O., Machfud, S., & ... (2023). Sosialiasi Pengenalan Pentingnya Cyber Security Guna Menjaga Keamanan Data di Era Digital Pada Siswa/i SMK Bakti Idhata Jakarta. *JIPM: Jurnal Inovasi ...*, *2*(1), 16–20. https://jurnal.astinamandiri.com/index.php/JIPM/article/view/141%0Ahttps://jurnal.astinamandiri.com/index.php/JIPM/article/download/141/101

Ramadhani, A. (2018). KEAMANAN INFORMASI. *Nusantara - Journal of Information and Library Studies*, *1*(1), 39. https://doi.org/10.30999/n-jils.v1i1.249

Rohan, D. H., & Hayati, N. (2019). Persamaan Lorenz untuk Keamanan Nomor Serial Sistem Operasi Window7. *Jurnal Ilmiah FIFO*, *10*(2), 1. https://doi.org/10.22441/fifo.2018.v10i2.001

Santoso, K. P., Madany, F. A., & Suryotrisongko, H. (2023). Dan Augmentasi Data NSL-KDD Menggunakan Deep Generative Adversarial Networks Untuk Meningkatkan Performa Algoritma Extreme Gradient Boosting Dalam …. *ArXiv Preprint ArXiv …*.

Sari, M. W. (2013). Analisis keamanan jaringan Virtual Private Network (VPN) pada Sistem Online Microbanking. *Informatika*, 13.

Surahman, F. (2023). Tantangan Dalam Menjaga Keamanan Data Official Statistics dari Serangan Cybercrime. *Jurnal Ilmiah Multidisiplin*, *1*(11), 904–907. https://doi.org/10.5281/zenodo.10371686

Sutriawan, S., Khatimah, N. H., & Sanusi, G. (2023). Sosialisasi Pentingnya Menjaga Privasi Dan Keamanan Data Di Era Digital. *SEWAGATI: Jurnal Pengabdian Kepada Masyarakat*, *2*(1), 8–14. https://doi.org/10.61461/sjpm.v2i1.10

Syahputri, N. I., Harahap, H., Siregar, R., & Tommy, T. (2023). Penyuluhan Pentingnya Two Factor Authentication dan Aplikasinya Di Era Keamanan Digital. *Jurnal Pengabdian Masyarakat Bangsa*, *1*(6), 768–773. https://doi.org/10.59837/jpmba.v1i6.256

Syamsu, M., Terisia, V., & Masduki, U. (2023). Buku Ajar Jaringan Komputer : Praktis & Mudah disertai Studi Kasus. *Eureka Media Aksara*.

Tan, T., Sama, H., Wijaya, G., & Aboagye, O. E. (2023). Studi Perbandingan Deteksi Intrusi Jaringan Menggunakan Machine Learning: (Metode SVM dan ANN). *Jurnal Teknologi Dan Informasi*, *13*(2), 152–164. https://doi.org/10.34010/jati.v13i2.10484

Vansuri, R., Fauzi, A., Teguh Prasetyo, E., Negara, R., Ramadhan, R., Mada Restu, A., & Raffi Firmansyah, R. (2023). Peran CIA (Confidentiality, Integrity, Availability) Terhadap Manajemen Keamanan Informasi. *Jurnal Ilmu Multidisplin*, *2*(1), 106–113.

https://doi.org/10.38035/jim.v2i1.234
Wicaksono, D. (2022). Firewall Sistem Keamanan Jaringan Menggunakan Firewall dengan Metode Port Blocking dan Firewall Filtering. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *9*(2), 1380–1392. https://doi.org/10.35957/jatisi.v9i2.2103.