TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 4, Tahun 2026
ISSN 3024-8256 (media online)
Hal 650-655

Kajian Sistematis: Ancaman dan Solusi Keamanan Jaringan pada Organisasi dan Individu

Ryan Maulana Rizqi[1], Rangga Irawan[2], Arya Ardiansyah[3]

[123]Ilmu Komputer, Sistem Informasi, Universitas Pamulang, Tangerang Selatan, Indonesia
Email: [1]ryanrizqi357@yahoo.com, [2]ranggairwns11@gmail.com, [3]aryacank.08@gmail.com
(*correspondng author)

Abstrak−Keamanan jaringan telah berkembang menjadi salah satu isu strategis utama di era digital saat ini, tidak hanya bagi organisasi berskala besar, tetapi juga bagi organisasi kecil hingga pengguna individu. Seiring dengan meningkatnya ketergantungan terhadap sistem dan layanan berbasis jaringan, berbagai bentuk ancaman siber, seperti phishing, ransomware, serta serangan *man-in-the-middle*, menunjukkan tren peningkatan baik dari sisi kompleksitas teknik maupun frekuensi kejadiannya. Penelitian ini menerapkan metode *narrative literature review* dengan menelaah 15 jurnal ilmiah terkini yang diterbitkan pada periode 2020–2025, dengan tujuan mengidentifikasi jenis ancaman keamanan jaringan yang paling dominan serta solusi mitigasi yang direkomendasikan dalam literatur. Hasil kajian menunjukkan bahwa faktor manusia (*human error*), konfigurasi jaringan yang tidak optimal, serta kurangnya pembaruan perangkat lunak secara berkala merupakan penyebab utama munculnya kerentanan keamanan. Untuk mengatasi permasalahan tersebut, berbagai solusi dinilai efektif, antara lain penerapan *firewall*, penggunaan enkripsi *end-to-end* untuk melindungi data dalam proses transmisi, pelaksanaan pelatihan kesadaran keamanan siber bagi pengguna, serta penerapan arsitektur *zero trust* sebagai pendekatan pengamanan berlapis. Secara keseluruhan, kajian ini menawarkan rekomendasi praktis yang dapat diimplementasikan tanpa memerlukan infrastruktur teknologi yang mahal, sehingga relevan dan aplikatif bagi organisasi skala kecil maupun pengguna individu.

Kata Kunci: keamanan jaringan; ancaman siber; solusi keamanan; *zero trust*; phishing

Abstract−*Network security has evolved into one of the main strategic issues in the digital era, affecting not only large organizations but also small organizations and individual users. As dependence on networked systems and services increases, various forms of cyber threats, such as phishing, ransomware, and* man-in-the-middle *attacks, are showing an upward trend in both technical complexity and frequency. This study employed a* narrative literature review *method, examining 15 scientific journals published between 2020 and 2025. The objective was to identify the most prevalent types of network security threats and the recommended mitigation solutions in the literature. The results show that human error, suboptimal network configuration, and insufficient regular software updates are the main causes of security vulnerabilities. Effective solutions include the implementation of firewalls, end-to-end encryption, cybersecurity awareness training, and the adoption of zero trust architecture. Overall, this study offers practical recommendations that can be implemented without expensive technological infrastructure, making them relevant and applicable for small organizations and individual users.*

Keywords: *network security; cyber threats; security solutions; zero trust; phishing*

1. PENDAHULUAN

Perkembangan teknologi informasi yang berlangsung sangat pesat dalam beberapa tahun terakhir telah mendorong terjadinya transformasi digital di hampir seluruh sektor kehidupan, termasuk pendidikan, bisnis, industri, pemerintahan, serta berbagai bentuk layanan publik. Pemanfaatan sistem informasi dan aplikasi berbasis jaringan internet memungkinkan proses pertukaran data, komunikasi, serta pengambilan keputusan dilakukan secara lebih cepat, efisien, dan terintegrasi lintas wilayah dan waktu. Digitalisasi proses kerja ini memberikan berbagai keuntungan dari sisi peningkatan produktivitas, fleksibilitas operasional, dan kemudahan akses terhadap informasi. Namun, di sisi lain, kondisi tersebut juga meningkatkan ketergantungan yang sangat tinggi terhadap infrastruktur jaringan yang dituntut untuk beroperasi secara aman, stabil, dan andal. Tingginya tingkat ketergantungan ini secara tidak langsung memperluas permukaan serangan (*attack surface*) dan membuka peluang bagi munculnya berbagai bentuk ancaman keamanan jaringan yang semakin kompleks dan sulit dideteksi.

Ancaman keamanan jaringan terus berkembang seiring dengan meningkatnya konektivitas global serta masifnya adopsi teknologi digital di berbagai lingkungan organisasi dan individu. Serangan siber seperti malware, *distributed denial-of-service* (DDoS), eksploitasi kerentanan sistem, serta serangan *man-in-the-middle* (MITM) menunjukkan tren peningkatan baik dari sisi

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 4, Tahun 2026
ISSN 3024-8256 (media online)
Hal 650-655

kompleksitas teknik serangan maupun frekuensi kejadiannya. Selain ancaman yang bersifat teknis, ancaman non-teknis seperti *social engineering*, khususnya phishing, juga menjadi salah satu metode serangan yang paling sering digunakan karena memanfaatkan kelemahan pada aspek perilaku dan kesadaran pengguna (Wang, 2020; Alshammari, 2022).

Dampak dari insiden keamanan jaringan tidak hanya bersifat teknis, tetapi juga menimbulkan konsekuensi ekonomi yang besar. Laporan IBM Security (2023) mencatat bahwa biaya rata-rata pelanggaran data secara global mencapai USD 4,45 juta, yang merupakan angka tertinggi dalam satu dekade terakhir. Nilai tersebut mencerminkan besarnya kerugian yang harus ditanggung organisasi, tidak hanya dalam bentuk kerugian finansial langsung, tetapi juga kerusakan reputasi, penurunan kepercayaan pengguna, serta gangguan terhadap keberlangsungan operasional. Fenomena ini menegaskan bahwa serangan siber tidak lagi hanya menargetkan organisasi besar atau institusi pemerintah, melainkan juga menyasar organisasi skala kecil, usaha mikro, serta individu yang menggunakan perangkat pribadi dan terhubung ke jaringan publik atau jaringan rumah tangga dengan tingkat pengamanan yang minim.

Sejumlah studi juga mengungkapkan bahwa penyebab utama kerentanan keamanan jaringan tidak selalu berasal dari kelemahan teknologi semata, melainkan sering kali dipicu oleh faktor manusia (*human factor*). Kesalahan seperti penggunaan kata sandi yang lemah, pengabaian pembaruan perangkat lunak, rendahnya pemahaman terhadap ancaman phishing, serta kelalaian dalam pengelolaan akses jaringan menjadi faktor dominan terjadinya berbagai insiden keamanan. (Kumar, 2023) menegaskan bahwa aspek manusia merupakan salah satu titik terlemah dalam sistem keamanan informasi, sehingga upaya mitigasi tidak dapat hanya berfokus pada solusi teknis semata.

Di sisi lain, penerapan solusi keamanan jaringan sering kali dipersepsikan sebagai sesuatu yang kompleks, mahal, dan membutuhkan sumber daya teknis yang tinggi. Persepsi tersebut menyebabkan banyak organisasi skala kecil maupun pengguna individu enggan atau tidak mampu mengadopsi mekanisme keamanan yang memadai. Padahal, berbagai pendekatan keamanan modern seperti penggunaan firewall, penerapan enkripsi data, pelaksanaan pelatihan kesadaran keamanan siber, serta penerapan arsitektur zero trust dapat diimplementasikan secara bertahap dan relatif terjangkau apabila disesuaikan dengan kebutuhan dan kapasitas pengguna (Lee, 2021).

Selain itu, perkembangan teknologi seperti komputasi awan (cloud computing), Internet of Things (IoT), dan kerja jarak jauh (remote working) turut memperluas kompleksitas pengelolaan keamanan jaringan. Integrasi berbagai perangkat dan layanan lintas platform meningkatkan potensi terjadinya kesalahan konfigurasi serta eksploitasi celah keamanan apabila tidak disertai dengan kebijakan keamanan yang memadai (Behl, 2020). Kondisi ini menuntut pendekatan keamanan jaringan yang tidak hanya berfokus pada perlindungan perimeter, tetapi juga mempertimbangkan kontrol akses yang adaptif dan pemantauan berkelanjutan terhadap aktivitas jaringan.

Sejumlah penelitian juga menekankan pentingnya pendekatan keamanan berbasis risiko dalam menghadapi ancaman siber modern. Pendekatan ini memungkinkan organisasi untuk memprioritaskan perlindungan terhadap aset kritis berdasarkan tingkat risiko yang dihadapi, sehingga sumber daya yang terbatas dapat dimanfaatkan secara lebih efektif (Sharma, 2021). Dalam konteks ini, penerapan prinsip keamanan berlapis (defense in depth) menjadi salah satu strategi yang banyak direkomendasikan dalam literatur.

Di samping itu, meningkatnya ketergantungan terhadap sistem digital juga menuntut adanya keselarasan antara kebijakan keamanan, teknologi, dan perilaku pengguna. Studi terbaru menunjukkan bahwa ketidakseimbangan antara aspek teknis dan aspek manusia dapat melemahkan efektivitas sistem keamanan jaringan secara keseluruhan, meskipun teknologi pengamanan yang digunakan tergolong mutakhir (Niekerk, 2023). Oleh karena itu, keamanan jaringan perlu dipandang sebagai isu sosio-teknis yang membutuhkan pendekatan komprehensif.

Berbagai kajian terkini juga menegaskan bahwa tantangan keamanan jaringan di negara berkembang memiliki karakteristik tersendiri, terutama terkait keterbatasan sumber daya, tingkat literasi keamanan yang beragam, serta kesiapan infrastruktur teknologi. Hal ini menjadikan kebutuhan akan solusi keamanan yang sederhana, terjangkau, dan mudah diimplementasikan semakin relevan, khususnya bagi organisasi skala kecil dan institusi pendidikan (Alshaikh, 2020).

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengkaji berbagai ancaman keamanan jaringan yang paling relevan dalam konteks perkembangan teknologi saat ini, serta mengidentifikasi solusi mitigasi yang dinilai efektif, terjangkau, dan mudah

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 4, Tahun 2026
ISSN 3024-8256 (media online)
Hal 650-655

diimplementasikan. Penelitian ini menggunakan pendekatan narrative literature review dengan menganalisis literatur ilmiah terkini yang diterbitkan pada periode 2020–2025. Diharapkan, hasil kajian ini dapat memberikan wawasan dan rekomendasi praktis yang bersifat aplikatif bagi organisasi maupun individu dalam upaya meningkatkan postur keamanan jaringan, tanpa memerlukan sumber daya teknis maupun finansial yang tinggi.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan *narrative literature review*, yaitu metode penelitian kualitatif yang bertujuan untuk mengumpulkan, mengevaluasi, dan mensintesis temuan-temuan utama dari berbagai publikasi ilmiah guna membangun pemahaman konseptual yang komprehensif terhadap suatu topik penelitian (Green, 2021). Pendekatan ini dipilih karena sesuai untuk mengkaji isu keamanan jaringan yang bersifat luas, dinamis, dan multidimensional, serta memungkinkan peneliti mengidentifikasi pola ancaman dan solusi mitigasi berdasarkan penelitian sebelumnya tanpa terikat pada prosedur kuantitatif yang ketat seperti pada *systematic review* (Snyder, 2020).

Proses penelusuran literatur dilakukan pada beberapa basis data ilmiah bereputasi, yaitu ScienceDirect, IEEE Xplore, dan SpringerLink. Literatur yang dikaji dipilih berdasarkan kriteria yang telah ditetapkan, meliputi artikel yang diterbitkan pada rentang tahun 2020–2025, berasal dari jurnal bereputasi internasional maupun nasional terakreditasi, serta memiliki Digital Object Identifier (DOI) aktif. Selain itu, artikel yang dipilih harus memiliki relevansi langsung dengan topik ancaman keamanan jaringan dan solusi mitigasi yang dibahas dalam konteks sistem dan infrastruktur jaringan.

Dari penelusuran awal, diperoleh sebanyak 42 artikel yang berpotensi relevan. Selanjutnya, artikel-artikel tersebut diseleksi melalui proses penyaringan bertahap yang mencakup evaluasi judul, abstrak, dan teks penuh (*full-text*), sehingga diperoleh 15 artikel yang memenuhi seluruh kriteria inklusi dan digunakan sebagai sumber utama dalam penelitian ini. Data yang diekstraksi dari artikel terpilih kemudian dianalisis menggunakan pendekatan analisis tematik, dengan tujuan mengidentifikasi, mengelompokkan, dan mensintesis berbagai jenis ancaman serta solusi keamanan jaringan berdasarkan kesamaan karakteristik, frekuensi kemunculan, dan konsistensi rekomendasi yang ditemukan dalam literatur (Criado, 2020).

Melalui tahapan analisis tersebut, penelitian ini diharapkan mampu menghasilkan pemetaan ancaman dan solusi keamanan jaringan yang sistematis dan aplikatif, serta memberikan dasar konseptual yang kuat bagi pembahasan dan kesimpulan penelitian.

3. ANALISA DAN PEMBAHASAN

Berdasarkan hasil tinjauan terhadap literatur ilmiah yang dianalisis, dapat disimpulkan bahwa ancaman keamanan jaringan yang muncul dalam kurun waktu lima tahun terakhir menunjukkan pola yang cenderung konsisten dari waktu ke waktu. Meskipun demikian, teknik, metode, dan media yang digunakan dalam serangan terus mengalami perkembangan dan penyempurnaan seiring dengan kemajuan teknologi serta meningkatnya kompleksitas sistem jaringan. Ancaman-ancaman tersebut tidak muncul secara acak, melainkan dapat diidentifikasi dan dikelompokkan ke dalam beberapa kategori utama berdasarkan kesamaan karakteristik, mekanisme serangan yang digunakan, serta sumber kerentanan yang dieksploitasi. Proses pengelompokan atau klasifikasi ini dilakukan untuk mempermudah analisis secara terstruktur, sekaligus memberikan gambaran yang lebih sistematis dan komprehensif mengenai jenis-jenis ancaman keamanan jaringan yang paling dominan dan relevan dalam konteks kondisi keamanan jaringan saat ini.

Serangan berbasis malware masih menempati posisi sebagai salah satu ancaman keamanan jaringan yang paling signifikan dan banyak dibahas dalam berbagai kajian ilmiah. Jenis malware seperti ransomware, spyware, dan trojan secara luas dilaporkan sebagai penyebab utama terjadinya gangguan layanan sistem, kehilangan maupun kerusakan data, serta kerugian finansial yang tidak sedikit bagi organisasi dan pengguna individu. Malware dapat menyebar melalui berbagai media, seperti email berbahaya, unduhan tidak resmi, maupun celah keamanan pada sistem yang belum diperbarui. Salah satu contoh kasus yang sering dijadikan rujukan dalam literatur adalah serangan WannaCry pada tahun 2017, yang mengeksploitasi kerentanan pada protokol layanan Server Message Block versi 1 (SMBv1). Kasus ini menjadi pengingat penting bahwa sistem dan perangkat

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 4, Tahun 2026
ISSN 3024-8256 (media online)
Hal 650-655

lunak yang tidak diperbarui secara berkala tetap sangat rentan terhadap eksploitasi, meskipun kerentanan tersebut telah lama diketahui dan solusi penambalan (*patch*) telah tersedia.

Dalam perkembangannya, ransomware tidak lagi hanya mengandalkan mekanisme penguncian data sebagai bentuk pemerasan. Teknik serangan ini telah berevolusi menjadi model yang lebih kompleks, salah satunya dikenal sebagai skema *double-extortion*. Pada pendekatan ini, penyerang tidak hanya mengenkripsi data korban sehingga tidak dapat diakses, tetapi juga menyalin dan menyimpan data sensitif tersebut di server eksternal yang mereka kuasai. Data yang dicuri kemudian digunakan sebagai alat tekanan tambahan dengan ancaman akan dipublikasikan atau diperjualbelikan apabila korban menolak membayar tebusan. Strategi ini secara signifikan meningkatkan dampak serangan, karena korban tidak hanya menghadapi risiko kehilangan data operasional, tetapi juga potensi kebocoran informasi rahasia yang dapat merusak reputasi dan kepercayaan pengguna.

Selain malware, ancaman keamanan jaringan juga banyak berasal dari teknik *social engineering*, dengan phishing sebagai vektor serangan yang paling umum digunakan. Phishing umumnya dilakukan melalui email, pesan instan, atau komunikasi digital lainnya dengan menyamar sebagai pihak yang sah dan dipercaya, seperti institusi resmi, penyedia layanan, atau rekan kerja. Pesan yang dirancang menyerupai komunikasi asli, pelaku berupaya memancing korban untuk mengklik tautan berbahaya atau memberikan informasi sensitif. Tingginya tingkat keberhasilan phishing menunjukkan bahwa aspek manusia masih menjadi titik lemah utama dalam sistem keamanan jaringan, terutama ketika pengguna tidak memiliki kesadaran dan kewaspadaan yang memadai terhadap potensi ancaman.

Efektivitas teknik *social engineering* tidak bergantung pada kelemahan teknis sistem atau perangkat lunak, melainkan pada eksploitasi aspek psikologis manusia, seperti rasa percaya, urgensi, rasa takut, maupun kelalaian dalam memverifikasi informasi. Kondisi ini menyebabkan serangan dapat berhasil bahkan pada lingkungan jaringan yang telah dilengkapi dengan teknologi keamanan yang relatif baik. Oleh karena itu, pengamanan jaringan yang hanya berfokus pada aspek teknis tanpa disertai peningkatan kesadaran pengguna cenderung tidak mampu memberikan perlindungan yang optimal terhadap ancaman jenis ini.

Selain malware dan *social engineering*, ancaman keamanan jaringan juga muncul dalam bentuk eksploitasi teknis terhadap kerentanan sistem, protokol, dan konfigurasi jaringan. Serangan seperti *distributed denial-of-service* (DDoS), *man-in-the-middle* (MITM), dan SQL injection secara langsung menargetkan kelemahan dalam arsitektur jaringan maupun aplikasi yang digunakan. Sebagai contoh, serangan MITM sering terjadi pada jaringan Wi-Fi publik yang tidak dilengkapi dengan mekanisme enkripsi yang memadai. Dalam kondisi tersebut, penyerang dapat menyadap, memodifikasi, atau mencuri data pengguna secara *real-time* tanpa disadari oleh korban. Situasi ini menunjukkan bahwa lemahnya konfigurasi keamanan dasar masih menjadi celah yang sering dimanfaatkan oleh pelaku serangan.

Temuan-temuan tersebut mengindikasikan bahwa konfigurasi jaringan yang tidak aman, penggunaan protokol lama, serta kurangnya pemantauan dan pemeliharaan sistem secara berkala masih menjadi faktor utama yang memungkinkan terjadinya eksploitasi teknis. Risiko ini cenderung lebih tinggi pada lingkungan jaringan dengan keterbatasan sumber daya teknis.

Hasil kajian literatur juga menunjukkan bahwa terdapat sejumlah solusi keamanan jaringan yang dinilai efektif, relatif terjangkau, dan dapat diimplementasikan oleh berbagai skala organisasi maupun pengguna individu. Secara umum, solusi-solusi tersebut dapat diklasifikasikan ke dalam beberapa pendekatan utama yang saling melengkapi antara aspek teknis dan non-teknis, sehingga mampu membentuk sistem pertahanan berlapis.

Firewall berperan sebagai lapisan pertahanan awal yang mengontrol lalu lintas jaringan masuk dan keluar berdasarkan kebijakan keamanan yang telah ditetapkan. Dengan memfilter akses yang tidak sah serta membatasi komunikasi yang mencurigakan, firewall mampu mencegah berbagai jenis serangan sebelum mencapai sistem internal. Sistem deteksi dan pencegahan intrusi (IDS/IPS) melengkapi peran firewall dengan kemampuan memantau pola lalu lintas jaringan secara *real-time*, sehingga aktivitas anomali atau indikasi serangan dapat segera diidentifikasi dan ditangani sejak dini.

Penerapan enkripsi end-to-end merupakan langkah penting dalam menjaga kerahasiaan dan integritas data selama proses transmisi. Dengan menggunakan protokol keamanan modern, data

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 4, Tahun 2026
ISSN 3024-8256 (media online)
Hal 650-655

yang dikirimkan melalui jaringan tidak dapat dibaca atau dimodifikasi oleh pihak yang tidak berwenang. Mekanisme enkripsi ini menjadi sangat krusial terutama untuk komunikasi yang bersifat sensitif, seperti pertukaran data bisnis, informasi pribadi, maupun transaksi keuangan, yang memiliki nilai tinggi dan sering menjadi target penyadapan.

Zero trust architecture mengusung prinsip "*never trust, always verify*", yang menekankan bahwa tidak ada entitas yang diberikan kepercayaan secara otomatis, baik berasal dari dalam maupun dari luar jaringan. Setiap permintaan akses harus diverifikasi berdasarkan identitas, perangkat, serta konteks akses yang relevan. Pendekatan ini membantu meminimalkan risiko serangan lateral dan penyalahgunaan hak akses, terutama pada lingkungan jaringan yang kompleks dan terdistribusi.

Selain solusi teknis, literatur juga menegaskan pentingnya peningkatan kesadaran pengguna melalui program edukasi dan pelatihan keamanan siber secara berkelanjutan. Pelatihan yang terstruktur, seperti simulasi serangan phishing, sosialisasi praktik penggunaan sandi yang kuat, serta pemahaman dasar mengenai ancaman siber, terbukti mampu menurunkan tingkat kesalahan manusia secara signifikan. Pendekatan non-teknis ini relatif mudah diadopsi, tidak memerlukan biaya besar, dan memberikan kontribusi yang nyata dalam memperkuat postur keamanan jaringan secara keseluruhan.

4. KESIMPULAN

Ancaman keamanan jaringan bersifat dinamis dan terus berevolusi seiring dengan perkembangan teknologi informasi serta meningkatnya tingkat konektivitas global. Pola dan teknik serangan siber mengalami perubahan yang cepat, sehingga menuntut adanya pendekatan keamanan yang adaptif dan berkelanjutan. Meskipun demikian, hasil kajian ini menunjukkan bahwa penerapan kombinasi solusi teknis dan non-teknis, seperti penggunaan firewall, penerapan enkripsi data untuk melindungi informasi selama proses transmisi, implementasi arsitektur *zero trust*, serta pelaksanaan edukasi dan pelatihan kesadaran keamanan siber bagi pengguna, terbukti mampu memperkuat postur keamanan jaringan secara signifikan. Pendekatan yang bersifat menyeluruh dan berlapis ini memungkinkan organisasi maupun individu untuk mengurangi risiko serangan, baik yang berasal dari kelemahan teknis maupun dari faktor manusia.

Penelitian ini juga menegaskan bahwa upaya perlindungan jaringan tidak selalu harus melibatkan teknologi yang mahal atau sistem yang kompleks. Faktor kunci dalam meningkatkan keamanan jaringan justru terletak pada konsistensi dalam penerapan kebijakan keamanan, pemantauan sistem secara berkala, serta pembaruan perangkat lunak dan konfigurasi jaringan yang berkelanjutan. Dengan perencanaan yang tepat dan pemanfaatan solusi yang sesuai dengan kebutuhan, organisasi skala kecil maupun pengguna individu tetap dapat meningkatkan tingkat keamanan jaringan mereka secara efektif.

Untuk penelitian selanjutnya, disarankan agar dilakukan studi empiris yang mengkaji secara langsung efektivitas berbagai solusi keamanan jaringan tersebut dalam konteks lingkungan lokal. Fokus penelitian dapat diarahkan pada sektor usaha mikro, kecil, dan menengah (UMKM) serta institusi pendidikan Indonesia yang umumnya memiliki keterbatasan sumber daya teknis dan finansial. Melalui pendekatan empiris, diharapkan dapat diperoleh pemahaman yang lebih mendalam mengenai tantangan implementasi, tingkat efektivitas solusi, serta rekomendasi yang lebih kontekstual dan aplikatif sesuai dengan kondisi lokal.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada dosen pembimbing atas bimbingan, arahan, dan masukan konstruktif yang diberikan selama proses penyusunan artikel ini. Selain itu, penulis juga menyampaikan apresiasi kepada rekan-rekan yang telah berkontribusi melalui diskusi, saran, dan dukungan yang sangat berharga, sehingga artikel ini dapat diselesaikan dengan baik. Seluruh masukan dan dukungan tersebut memberikan peran penting dalam meningkatkan kualitas dan kelengkapan isi penelitian ini.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 4, Tahun 2026
ISSN 3024-8256 (media online)
Hal 650-655

REFERENCES

Alshaikh. 2020. "Developing cybersecurity culture to influence employee behavior" Computers & Security 98, 102003. https://doi.org/10.1016/j.cose.2020.102003.

Alshammari. 2022. "Phishing attacks: A comprehensive analysis and detection framework." Computers & Security 115, 102631. https://doi.org/10.10161/j.cose.2022.102631.

Behl, Behl. 2020. "Cybersecurity and cyberwar: What everyone needs to know." Journal of Business. Research 111, 312-320. https://doi.org/10.10161/j.jbusres.2019.12.064.

Behl. 2021. "Cyber-security and cyberwar: What everyone needs to know." Oxford University Press.

Criado, Paul &. 2020. "The art of writing literature review: What do we know and what do we need to know?" International Business Review 29(4), 101717. https://doi.org/10.1016/j.ibusrev.2020.101717.

EN1SA. 2022. "ENISA Threat Landscape 2022." European Union Agency for cybersecurity.

Green. 2021. "Narrative reviews in information security research: Methodological considerations and best practices." Information and Software Technology 135, 106567. https://doi.org/10.1016/j.infsof.2021.106567.

Kumar. 2023 "Human factors in cybersecurity: A systematic review." Journal of Information Security and Applications 74, 103456. https://doi.org/10.1016/j.jisa..2023.103456.

Lee, Smith. 2021. "Zero Trust Networks: Building secure systems in untrusted networks." IEEE Access 9, 12345-12356. https://doi.org/10.1109/ACCESS.2021.3051234.

Mattord, Whitman. 2021. "Principles of information security (7th ed.)." Cengage Learning.

Niekerk, Von Solms & Van. 2023. "From information security to cybersecurity culture." Computers & Security 123, 102946. https://doi.org/10.1016/j.cose.2022.102946.

Security, IBM. 2023. "Cost of a Data Breach Report 2023."

Sharma, Kumar_ 2021, -Risk-based cybersecurity framework for modern network environments." Computers & Security 105, 102236. https://doi.org110_1016/j.cose.2021.102236.

Snyder. 2020. "Literature review as a research methodology: An overview and guidelines." Journal of Business Research 104, 333-339. https://doi.org/l0 .1016/j jbusres.2019.07.039.

Wang. 2020. "A survey on DDoS attack detection and defense' Journal of Network and Computer Applications 161, 102631. https://doi.org/10.1016/j.jnca.2020.102631.