Pediaqu : Jurnal Pendidikan Sosial dan Humaniora
https://publisherqu.com/index.php/pediaqu
Vol. 4, No. 2 April 2025
P-ISSN:2964-7142; E-ISSN:2964-6499

OPTIMALISASI INFRASTRUKTUR KEAMANAN TEKNOLOGI INFRASTRUKTUR DALAM MENGHADAPI ANCAMAN CYBERSECURITY

Annisa Rahmawati[1], Muhammad Nouval Ramadhani[2], Nitania Yevana[3], Rika Maulina[4], Achmad Daffa Fattah[5], Dicky Pratama[6]
[123456] Program Studi Sistem Informasi, Fakultas Ilmu Komputer dan Rekayasa, Universitas Multi Data Palembang
anisarahmawati2021@mhs.mdp.ac.id[1], nouvalramadhani61@mhs.mdp.ac.id[2], yevanatan@mhs.mdp.ac.id[3], rikamaulina@mhs.mdp.ac.id[4], adaff04@mhs.mdp.ac.id[5], dqpratama@mdp.ac.id[6]

Abstract
The rapid increase in the use of digital technology has triggered an increase in cyber threats that are increasingly sophisticated and diverse. This research identifies various types of cyber threats, from malware to DDoS attacks, and analyzes their significant impact on organizations, including financial and reputational losses. In addition, this research also evaluates various cybersecurity strategies that can be implemented, such as risk management, layered security, automation, and user awareness. The results of this research present a comprehensive framework that integrates technology, policy, and user awareness to build effective cyber defenses. The research also identified recent trends in the cyber threat landscape, such as increasingly sophisticated ransomware attacks and the use of artificial intelligence by cybercriminals. Further research is needed to evaluate the effectiveness of the proposed cybersecurity strategies in the context of different industry sectors and organizational sizes.
Keywords : Cyber Security, Information Technology Infrastructure, Security Strategy, Cyber Threats

PENDAHULUAN

Di era digital yang semakin maju, teknologi informasi (TI) telah menjadi dasar bagi berbagai operasi di sektor publik maupun swasta. Hampir semua aspek kehidupan manusia, mulai dari aktivitas pribadi, bisnis, hingga pemerintahan, bergantung pada teknologi digital. Namun, seiring dengan kemajuan teknologi, ancaman terhadap keamanan data dan informasi juga meningkat. Kejahatan siber kini menjadi ancaman besar yang dapat membahayakan kepentingan individu, perusahaan, bahkan negara [1]. Kejahatan siber adalah jenis kejahatan virtual yang memanfaatkan media komputer yang terhubung ke internet dan mengeksploitasi komputer lain yang juga terhubung ke internet. Apabila sistem operasi memiliki celah

keamanan, peretas (hacker), perusak (cracker), dan pelaku siber tidak berpengalaman (script kiddies) dapat memanfaatkan celah tersebut untuk menyusup ke dalam komputer [2].

Serangan siber seperti ransomware, phishing, dan distributed denial of service (DDoS)semakin marak dan memiliki dampak signifikan di dunia yang kian terhubung. Baik organisasi kecil maupun besar menghadapi resiko kehilangan data pribadi, gangguan operasional, kerugian finansial, serta hilangnya kepercayaan dari pelanggan dan mitra bisnis. Serangan siber ini dapat mengganggu operasional perusahaan mengacaukan layanan publik, menyebabkan kerugian finansial yang besar, serta merusak reputasi yang dibangun selama bertahun-tahun. Serangan siber juga berdampak pada masalah yang lebih luas, seperti stabilitas ekonomi, keamanan nasional, dan kepercayaan masyarakat terhadap sistem digital yang digunakan oleh pemerintah dan perusahaan swasta. Oleh karena itu, pengelolaan infrastruktur keamanan teknologi informasi kini menjadi kebutuhan mendesak bagi setiap organisasi dan entitas yang bergantung pada teknologi digital.

Situasi ini semakin parah karena adanya peningkatan jumlah serangan siber yang terus meningkat setiap tahunnya, seperti yang dijelaskan dalam penelitian terdahulu yang dilakukan oleh [3] Menurut penelitian tersebut, terjadi peningkatan serangan siber di Indonesia dari Januari hingga Juli 2021 dengan jumlah 741.441.648 serangan yang tercatat. Ancaman tersebut meliputi serangan Denial of Service (DoS), phishing, dan pencurian data pribadi. Risiko siber meningkat sebesar 6,15% dari tahun 2020 ke 2021, yang disebabkan oleh lemahnya perlindungan hukum. Contoh kasus yang dibahas dalam penelitian tersebut meliputi pencurian data melalui penyebaran informasi palsu (hoaks), eksploitasi celah keamanan pada aplikasi, serta phishing melalui situs web palsu.

Contoh lain dari serangan siber yang meningkat dalam konteks Pencemaran nama baik yaitu peretasan data pribadi atau tindakan seseorang dengan sengaja dan tanpa hak membagikannya. Kondisi tersebut disebabkan oleh masyarakat yang tidak menyadari bahaya dari ancaman siber dan kurangnya Kebijakan dan undang-undang yang kuat untuk melindungi keamanan nasional [4]

Dengan mempertimbangkan temuan penelitian sebelumnya, dapat disimpulkan bahwa memperkuat infrastruktur keamanan siber negara merupakan komponen penting dari rencana pembangunan digital yang berkelanjutan. Oleh karena itu, penelitian ini akan berfokus pada strategi penerapan infrastruktur keamanan informasi untuk menghadapi ancaman *cyber* yang semakin kompleks dan beragam. Selain itu, penelitian ini juga bertujuan untuk mendukung

kebijakan pemerintah dalam meningkatkan keamanan siber nasional. Dengan demikian, diharapkan hasil penelitian ini dapat memberikan kontribusi yang signifikan dalam meningkatkan sistem keamanan TI yang lebih efisien dan berkelanjutan di Indonesia, serta mendukung terciptanya lingkungan digital yang lebih aman dan terlindungi.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah studi literatur. Studi literatur dipilih karena beberapa alasan. Pertama, metode ini memungkinkan peneliti untuk mempelajari teori, kerangka kerja, dan temuan penelitian sebelumnya yang relevan tanpa harus mengumpulkan data primer. Kedua, studi literatur memungkinkan peneliti untuk memahami konteks penelitian secara menyeluruh dengan menganalisis sumber sekunder, seperti jurnal ilmiah, buku referensi, artikel, dan dokumen online [1]

Tahap awal dalam metode ini melibatkan pencarian dan pemilihan literatur yang relevan, termasuk jurnal akademis, buku referensi, laporan penelitian, dan artikel terkini untuk dianalisis. Hasil analisis ini kemudian disatukan untuk memberikan pemahaman dan informasi yang terkait dengan strategi penerapan keamanan infrastruktur teknologi informasi dalam menghadapi ancaman siber. Studi literatur ini akan digunakan untuk merangkum kondisi keamanan infrastruktur TI saat ini, mencakup pendekatan yang berhasil digunakan dalam mengatasi ancaman siber.

HASIL DAN PEMBAHASAN

Identifikasi Ancaman Cybersecurity

Perkembangan teknologi membawa berbagai macam ancaman keamanan siber dengan memanfaatkan celah dari teknologi, pemrosesan, dan juga aktivitas manusia. *Cybersecurity threats* bertambah canggih dan memiliki pengaruh yang semakin bertambah besar terhadap organisasi. Pemahaman terhadap ancaman keamanan siber menjadi sangat penting pada implementasi keamanan Teknologi Informasi, berikut uraian berbagai bentuk yang termasuk serangan keamanan siber:

Malware

Sebuah perangkat lunak yang berbahaya yang diciptakan dengan maksud untuk mengganggu kegiatan dari sistem dalam komputer dengan mengambil data yang bersifat

rahasia atau melakukan akses yang tidak sah disebut sebagai *Malware*[5]. Terdapat beberapa jenis *malware* yang meliputi:

- *Virus*

  Software berbahaya yang disisipkan pada berkas atau usuatu aplikasi, yang penyebarannya melalui aktivitas pengguna pada saat membuka berkas yang telah terinfeksi, dan memanfaatkan kelemahan sistem dengan tujuan mencuri data atau mengakses secara ilegal disebut sebagai *virus* [6].

- *Worm*

  Malware dalam bentuk *Worm* adalah sebuah program yang merugikan dan beroperasi dengan mandiri dan merambat ke seluruh penjuru dengan memanfaatkan celah sistem. Berbeda dengan *virus*, yang menyisipkan dirinya pada program, *worm* justru melakukan penyebaran mandiri dan umumnya dimanfaatkan *hacker* via email, proses otomatis, dan pada saat login [7].

- *Trojan Horse*

  Program jahat yang menjelma dalam bentuk *software* yang legal disebut *Trojan* atau Troya. Ketika dijalankan, *trojan* akan menyebarkan kode berbahayan yang termasuk file, membajak aplikasi, dan mengambil data yang sifatnya rahasia seperti *password.* Lain halnya dengan *virus* dan *worm*, *trojan* memerlukan interaksi pengguna untuk melakukan penyebaran, yang membuat trojan menjadi sukar diidentifikasi sampai timbul dampak yang cukup parah. *Trojan* pun membuat penyerang menjadi memiliki kemungkinan dalam mengendalikan komputer pengguna secara *remote* dan mengambil data sesitif [8].

- *Ransomware*

  Ancaman *Ransomeware* merupakan banetuk ancaman yang paling berat pada perangkat *IoT*. *Malware* dalam bentuk *Ransomware* datang dari kombinasi kata “ransom”(tebusan) dan “ware”(perangkat lunak), merujuk pada jenis *malware* yang melakukan enkripsi informasi sensitif serta memblokir akses pengguna pada perangkat, yang mengharuskan pengguna melakukan pembayaran tebusan untuk dapat kembali menggunakan perangkat. Bentuk ancaman ini, penyerang memanfaatkan algoritma enksripsi yang rumit guna melakukan pengamanan terhadap data korban lalu menuntut uang tebusan yang merupakan syarat un tuk menyerahkan kode untuk deskripsi. Ancaman *Ransomeware* mampu mengakibatkan kehilangan data secara temporer ataupun permanen, terhambatnya jalannya sistem, kerugian materi [9].

- *Spyware*

Software yang diinstal di komputer secara terselubung dengan tujuan mengetahui kegiatan korban saat online ataupun offline, lalu menyerahkan informasi yang didapatkan kepada pihak tertentu adalah *malware* yang disebut sebagai spyware [7].

Phising

Salah satu tindakan kejahatan internet yang penyerangnya berpura-pura menjadi lembaga yang legal dengan tujuan mendapatkan data yang sifatnya rahasia didefinisikan sebagai *phising.* Teknik yang digunakan diantaranya melakukan manipulasi situs, halaman web palsu, pesan singkat, serta pemanggilan melalui telepon [10].

DDoS (Distributed Denial-of-Service)

Ancaman *DdoS* dimaksudkan untuk mengacaukan ketersediaan layanan untuk pengguna yang memiliki hak yang sah melalui penyerangan ketersediaan *network resources.* Mekanisme ancaman ini mengeksploitasi akses tersebar pada perangkat dengan memanfaatkan kelemahan keamanan yang sudah diketahui. Ancaman ini mengincar beragam tingkatan infrastruktur *network,* termasuk aplikasi, transportasi, serta lapisan lainnya [11].

Man-in-the-Middle (MitM) Attacks

Jenis ancaman peretasan yang pelakunya menyelinap pada kanal komunikasi antar kedua belah pihak yang sedang melakukan komunikasi dengan cara yang sah didefinisikan sebagai *Man-in-the-Middle (MitM) attacks.* Penyusup mampu melakukan pemantauan, memodifikasi, maupun mengubah informasi yang disampaikan tanpa sepengetahuan korban. Penyusupan ini biasanya mengeksploitasi media telekomunikasi semacam *LTE, GSM, Wi-Fi, NFC,* maupun *Radio Frequency* [12].

Peretasan Data *(Hacking)*

Hacking merupakan aktivitas penerobosan ke dalam sistem melalui tindakan eksploitasi kelemahan keamanan atau algoritma peretasan, salah satunya yaitu meretas *password.* Orang yang melakukannya yang dijuluki "*hacker",* ialah pihak yang mahir tentang sistem perangkat serta bahasa pemrograman, dan memiliki kemampuan melaksanakan hal tindakan yang tidak terencana oleh pihak yang membuat sistem [13].

SQL Injection

Injeksi dari serangan web yaitu *SQL Injection,* yang mana yang memberikan serangan menyisipkan masukan ke perangkat dengan tujuan melakukan tindakan berbahaya. Pihak yang menjadi target pada umumnya tidak memiliki kesiapan dalam menangani input ini, sehingga

menyebabkan bocornya informasi ataupun diberikannya izin untuk mengakses secara ilegal kepada penyerang. Penyerang mampu melakukan akses maupun mengubah data, yang berdampak terhadap seluruh komponen keamanan, seperti kerahasiaan, integritas, maupun ketersediaan data [14].

Credential Stuffing

Kejahatan penyerangan yang banyak ditemukan dalam penyerangan bertarget ialah *Credential Stuffing,* yaitu ketika penyeran melakukan percobaan memasuki akun korban melalui *password* yang bocor(Pal *et al.*, 2019).

Strategi Penerapan Infrastruktur Keamanan Teknologi Informasi

Dalam era digital yang terus berkembang, ancaman terhadap infrastruktur teknologi informasi (TI) semakin kompleks. Oleh karena itu, untuk mengelola infrastruktur keamanan TI dengan baik, diperlukan strategi yang komprehensif dan adaptif terhadap perkembangan ancaman siber. Strategi-strategi ini tidak hanya mencakup kebijakan keamanan tetapi juga implementasi teknologi yang tepat, pelatihan sumber daya manusia, serta perbaikan berkelanjutan. Berikut adalah beberapa strategi yang dapat diterapkan untuk mengelola infrastruktur keamanan TI secara efektif:

Manajemen Risiko

Pendekatan berbasis risiko merupakan langkah pertama yang sangat penting dalam pengelolaan infrastruktur keamanan TI. Organisasi perlu melakukan identifikasi dan penilaian risiko secara menyeluruh, mengidentifikasi potensi ancaman serta kerentanannya di seluruh infrastruktur TI, termasuk perangkat keras, perangkat lunak, dan data. Dengan menilai risiko yang ada, organisasi dapat memfokuskan upaya mitigasi pada area yang memiliki potensi kerusakan paling besar, misalnya data sensitif atau aplikasi penting. Dengan prioritas yang jelas, sumber daya TI dapat dialokasikan secara efisien untuk mengurangi risiko yang paling relevan[16].

Keamanan Berlapis

Keamanan berlapis adalah strategi yang menekankan perlindungan setiap komponen dalam infrastruktur TI dengan beberapa lapisan keamanan. Model pertahanan berlapis ini menggabungkan berbagai teknik, seperti penggunaan firewall di tingkat jaringan, kontrol akses pada aplikasi, serta enkripsi data untuk perlindungan pada tingkat penyimpanan. Selain itu, segmentasi dan micro-segmentation jaringan juga sangat dianjurkan untuk membatasi dampak dari potensi serangan dengan membagi infrastruktur menjadi bagian-bagian yang lebih kecil

dan lebih mudah dilindungi. Dengan demikian, apabila satu lapisan atau bagian disusupi, serangan tidak akan mudah meluas ke bagian lain [17].

Otomatisasi dan Orkestrasi Keamanan

Untuk meningkatkan efisiensi dan responsivitas dalam pengelolaan keamanan, organisasi perlu mengadopsi otomatisasi keamanan. Teknologi otomasi dapat digunakan untuk proses-proses seperti patching otomatis, deteksi ancaman, dan respon insiden. Dengan otomasi, ancaman dapat ditangani lebih cepat dan mengurangi beban operasional. Orkestrasi keamanan juga diperlukan untuk memastikan berbagai alat dan sistem keamanan seperti SIEM (Security Information and Event Management), IDS/IPS, firewall, dan antivirus bekerja secara koordinasi dalam mendeteksi dan merespons ancaman secara otomatis [18].

Pengelolaan Indentitas dan Akses (IAM).

Keamanan yang efektif sangat bergantung pada pengelolaan identitas dan akses (IAM). Dengan menerapkan sistem IAM yang kuat, organisasi dapat mengelola identitas pengguna dan kontrol akses secara terpusat. Hal ini mencakup penerapan prinsip *least privilege, yang hanya memberikan akses minimum yang dibutuhkan untuk setiap pengguna, serta Role-Based Access Control (RBAC) untuk memastikan akses yang tepat berdasarkan peran dan tanggung jawab. Autentikasi multi-faktor (MFA) juga harus diterapkan, terutama untuk akses ke data sensitif, guna menambah lapisan perlindungan dari akses yang tidak sah [19].

Pembaruan dan Pemeliharaan Sistem secara Berkala

Pembaruan perangkat lunak dan perangkat keras secara berkala sangat penting dalam memastikan ketahanan sistem terhadap ancaman yang baru. Manajemen patching yang baik memastikan bahwa semua sistem yang memiliki kerentanannya diperbarui dengan segera setelah pembaruan keamanan tersedia. Di samping itu, pemeriksaan keamanan rutin atau audit secara berkala diperlukan untuk menilai ketahanan infrastruktur TI dan mengidentifikasi potensi celah yang belum terdeteksi sebelumnya [20].

Pemantauan dan Analisis Keamanan Real-Time.

Untuk mendeteksi ancaman dengan cepat, pemantauan secara real-time sangat penting. Penggunaan Security Information and Event Management (SIEM) memungkinkan organisasi untuk mengawasi seluruh aktivitas dalam jaringan dan infrastruktur TI. SIEM mengumpulkan log dan informasi dari berbagai sumber untuk mendeteksi pola yang mencurigakan dan memberikan peringatan dini. Selain itu, analisis forensik pasca insiden sangat berguna untuk

mengidentifikasi penyebab serangan dan menentukan langkah-langkah perbaikan yang diperlukan [21].

Rencana Tanggap Insiden dan Pemulihan Bencana

Meskipun telah diterapkan langkah-langkah pencegahan, ancaman terhadap TI tetap mungkin terjadi. Oleh karena itu, organisasi harus memiliki rencana tanggap insiden yang jelas dan terstruktur untuk merespons insiden keamanan dengan cepat. Rencana ini harus mencakup langkah-langkah mitigasi, peran tim, prosedur pelaporan, serta pemulihan operasional. Pemulihan bencana juga menjadi elemen krusial, di mana organisasi harus memastikan ada backup data yang teratur dan tes pemulihan yang rutin untuk mengembalikan sistem beroperasi dalam waktu singkat setelah serangan atau kegagalan [22].

Kesadaran Dan Penddikan Keamanan.

Mengelola keamanan bukan hanya tanggung jawab departemen TI, tetapi seluruh anggota organisasi. Pelatihan pengguna secara rutin mengenai ancaman keamanan, seperti phishing dan malware, serta simulasi serangan siber untuk menguji kesiapsiagaan organisasi sangat diperlukan. Pendidikan dan kesadaran keamanan di kalangan pengguna dapat mengurangi potensi celah keamanan yang disebabkan oleh kesalahan manusia [23].

Kepatuhan terhadap Standar dan Regulasi.

Kepatuhan terhadap standar dan regulasi yang berlaku, seperti ISO/IEC 27001, NIST Cybersecurity Framework, dan GDPR, merupakan bagian penting dari pengelolaan infrastruktur TI yang aman. Audit keamanan dan kepatuhan secara teratur perlu dilakukan untuk memastikan bahwa kebijakan yang ada sudah sesuai dengan standar industri dan persyaratan hukum yang berlaku [24].

Perbaikan Berkelanjutan dan Evaluasi.

Keamanan TI adalah proses yang terus berkembang. Oleh karena itu, organisasi harus secara rutin mengevaluasi dan memperbarui kebijakan dan teknologi yang diterapkan. Melakukan evaluasi efektivitas kebijakan serta mengumpulkan umpan balik dari insiden yang terjadi dapat meningkatkan strategi dan pengelolaan keamanan di masa depan. Perbaikan berkelanjutan akan memastikan bahwa infrastruktur keamanan TI selalu siap menghadapi ancaman yang berkembang [25].

KESIMPULAN

Kesimpulan dari penelitian ini menunjukkan bahwa perlindungan terhadap teknologi informasi menjadi hal yang sangat penting di zaman digital akibat meningkatnya ancaman keamanan siber yang semakin rumit dan berdampak besar terhadap organisasi. Penelitian ini menyoroti betapa krusialnya memiliki rencana yang terorganisir dan menyeluruh untuk mengelola infrastruktur keamanan TI agar dapat mengatasi ancaman-ancaman ini. Berbagai ancaman seperti perangkat berbahaya, *phishing*, serangan *DDoS*, *Man-in-the-Middle (MitM*), pencurian data, *SQL Injection*, dan pengisian kredensial perlu diwaspadai, sebab metode serangan yang beragam dapat sangat merugikan data dan kinerja organisasi.

Penerapan sistem kerja seperti Kerangka Kerja Keamanan Siber NIST *CyberSecurity* dan ISO/IEC 27001 memberikan dasar yang baik untuk membangun, mengelola, dan meningkatkan perlindungan TI. Kerangka kerja ini membantu organisasi dalam mengenali risiko, melindungi aset berharga, mengamati aktivitas yang mencurigakan, merespons insiden, dan memulihkan sistem dengan cepat. Selain itu, penerapan teknologi keamanan canggih seperti firewall dan enkripsi, serta pengelolaan akses yang ketat melalui autentikasi multi-faktor (MFA), menjadi penting bersama dengan pelatihan dan edukasi keamanan siber bagi pengguna. Organisasi juga perlu memiliki rencana respons insiden yang jelas, melakukan pencadangan data secara berkala, dan meningkatkan kerja sama dengan lembaga yang terkait untuk berbagi informasi mengenai ancaman siber.

Hasil dari penelitian ini menunjukkan bahwa pengelolaan infrastruktur keamanan TI tidak hanya sekadar soal penerapan teknologi, tetapi juga memerlukan pendekatan menyeluruh yang mencakup kebijakan, manajemen risiko, serta peningkatan kesadaran akan keamanan di semua level organisasi. Strategi yang disampaikan memberikan organisasi kemampuan untuk mengembangkan sistem keamanan TI yang kuat dan responsif. Dengan melakukan langkah-langkah ini, organisasi tak hanya dapat menjaga aset digital mereka, tetapi juga memastikan kelangsungan operasional dan meningkatkan kepercayaan para pemangku kepentingan. Penelitian ini diharapkan dapat memberikan panduan bagi organisasi dalam merancang kebijakan dan strategi guna mengatasi tantangan keamanan siber di masa mendatang.

DAFTAR PUSTAKA

Nabila Aulia Agustin and Refania Meilani Firdos, “Studi Literatur : Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital,” *J. Mhs. Tek. Inform.*, vol. 3, no. 1, pp. 126–131, 2024, doi: 10.35473/jamastika.v3i1.2841.

E. Ketaren, “Cybercrime, Cyber Space, Dan Cyber Law,” *J. TIMES*, vol. 5, no. 2, pp. 35–42, 2017, doi: 10.51351/jtm.5.2.2016556.

S. Parulian, D. A. Pratiwi, and M. Cahya Yustina, “Ancaman dan Solusi Serangan Siber di Indonesia,” *Telecommun. Networks, Electron. Comput. Technol.*, vol. 1, no. 2, pp. 85–92, 2021.

M. Z. Rizaldi, R. D. Putra, and A. Ul Hosnah, “Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data,” *JUSTITIA J. Ilmu Huk. dan Hum.*, vol. 6, no. 2, p. 619, 2023, doi: 10.31604/justitia.v6i2.619-627.

M. Naseer *et al.*, “Malware Detection: Issues and Challenges,” in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Apr. 2021. doi: 10.1088/1742-6596/1807/1/012011.

M. Thakur, “Cyber Security Threats and Counter Measures in Digital Age,” *J. Appl. Sci. Educ.*, vol. 04, no. 042, pp. 1–20, 2024, doi: 10.54060/a2zjourna.

M. A. Hama Saeed, “Malware in Computer Systems: Problems and Solutions,” *IJID (International J. Informatics Dev.*, vol. 9, no. 1, p. 1, Apr. 2020, doi: 10.14421/ijid.2020.09101.

E. G. Dada, J. Stephen Bassi, Y. J. Hurcha, and A. H. Alkali, “Performance Evaluation of Machine Learning Algorithms for Detection and Prevention of Malware Attacks,” vol. 21, no. 3, pp. 18–27, doi: 10.9790/0661-2103011827.

J. H. Park, S. K. Singh, M. M. Salim, A. E. L. Azzaoui, and J. H. Park, “Ransomware-based Cyber Attacks: A Comprehensive Survey,” *J. Internet Technol.*, vol. 23, no. 7, pp. 1557–1564, 2022, doi: 10.53106/160792642022122307010.

E. Ginting, M. Pardomuan Sinaga, M. Rizal Nurdin, M. Dimas Putra, P. Studi Sistem Informasi, and K. Kunci, “ANALISIS ANCAMAN PHISING TERHADAP LAYANAN ONLINE PERBANKAN (STUDI KASUS PADA BANK BRI) PHISING THREAT ANALYSIS OF ONLINE BANKING SERVICES (CASE STUDY ON BANK BRI),” 2023.

S. Wani, M. Imthiyas, H. Almohamedh, K. M. Alhamed, S. Almotairi, and Y. Gulzar, “Distributed denial of service (Ddos) mitigation using blockchain—a comprehensive insight,” *Symmetry*, vol. 13, no. 2. MDPI AG, pp. 1–21, Feb. 2021. doi: 10.3390/sym13020227.

A. Mallik, “MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS,” 2018.

T. Aprilia *et al.*, “Pengaruh Keamanan Two Factor Authentication Terhadap Pencurian Data (Cyber Crime) Pada Media Sosial,” *Pengaruh Keamanan Two Factor*, vol. 2, no. 5, pp. 449–458, 2024, doi: 10.5281/zenodo.11496678.

M. Alghawazi, D. Alghazzawi, and S. Alarifi, “Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review,” *J. Cybersecurity Priv.*, vol. 2, no. 4, pp. 764–777, Dec. 2022, doi: 10.3390/jcp2040039.

B. Pal, T. Daniel, R. Chatterjee, T. Ristenpart, and C. Tech, “Beyond Credential Stuffing: Password Similarity Models using Neural Networks.”

G. Mochammad Husein and R. V. Imbar, “Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. JABAR TELEMATIKA

(JATEL)," *J. Tek. Inform. dan Sist. Inf.*, vol. 1, no. 2, pp. 75–87, 2015, doi: 10.28932/jutisi.v1i2.368.

S. N. Adzimi, H. A. Alfasih, F. N. G. Ramadhan, S. N. Neyman, and A. Setiawan, "Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi menggunakan Debian," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 12, 2024, doi: 10.47134/pjise.v1i4.2681.

A. Zulfikar and Y. Akbar, "Automation of Mikrotik Router Setting Configuration Backup Using Ansible with Network DevOps Method Otomasi Backup Konfigurasi Settingan Router Mikrotik Menggunakan Ansible dengan Metode Network DevOps," vol. 5, no. January, pp. 57–66, 2025.

G. D. Putra, S. Sumaryono, and W. Widyawan, "Rancang Bangun Identity and Access Management IoT Berbasis KSI dan Permissioned Blockchain," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 7, no. 4, pp. 384–390, 2018, doi: 10.22146/jnteti.v7i4.455.

M. Souppaya, K. Stine, M. Simos, S. Sweeney, and K. Scarfone, "Critical Cybersecurity Hygiene: Patching the Enterprise," *Natl. Inst. Stand. Technol.*, 2020, [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/ch-pe-project-description-final.pdf

G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures[Gestión de eventos e información de seguridad (SIEM): análisis, tendencias y uso en infraestructuras críticas]," *Sensors*, vol. 21, no. 14, pp. 1–28, 2021.

C. V. M. Kaliu, A. Mewengkang, and J. R. Batmetan, "Analisis Manajemen Insiden IT pada Sistem Informasi Akademik Universitas Negeri Manado," *Edutik J. Pendidik. Teknol. Inf. dan Komun.*, vol. 2, no. 6, pp. 940–949, 2022, doi: 10.53682/edutik.v2i6.6463.

T. Tan, H. Sama, T. Wibowo, G. Wijaya, and ..., "Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam," *J. Teknol. dan …*, vol. 14, no. September, pp. 163–173, 2024, doi: 10.34010/jati.v14i2.

M. Pajak and P. Zirman, "Faculty of Economic, Riau University," vol. 4, no. 1, pp. 294–308, 2013.

D. Herlinudinkhaji, "Evaluasi Layanan Teknologi Informasi ITIL Versi 3 Domain Service Desain pada Universitas Selamat Sri Kendal," *Walisongo J. Inf. Technol.*, vol. 1, no. 1, p. 61, 2019, doi: 10.21580/wjit.2019.1.1.4005.