Journal of Data Analytics, Information, and Computer Science (JDAICS)
Volume 2, No 1 – Januari 2025
e-ISSN : 3032-4696

ANALISIS KEAMANAN INFRASTRUKTUR TEKNOLOGI INFORMASI DALAM MENGHADAPI ANCAMAN CYBERSECURITY

Suryayusra[1], Derri Anjuju[2], Maria Ulfa[3] , Dedi irawan*[4]
[1,2,3]Universitas Bina Darma, Palembang, Sumatera Selatan, Indonesia
* Penulis Korespondensi: 211420117@student.binadarma.ac.id

Received: 02-01- 2025	Revised: 15-01-2025	Approved: 27-01-2025

ABSTRAK

Keamanan infrastruktur Teknologi Informasi (TI) semakin menjadi prioritas penting di era digital yang berkembang pesat. Penelitian ini bertujuan untuk menganalisis aspek keamanan TI dan mengeksplorasi strategi efektif untuk menghadapi ancaman siber. Pendekatan yang digunakan adalah penelitian kualitatif dengan studi pustaka, dengan fokus pada literatur terbaru mengenai keamanan siber, infrastruktur TI, dan teknologi terkait. Analisis dilakukan pada kerangka kerja keamanan umum dan tren terkini dalam menghadapi ancaman siber. Temuan penelitian menunjukkan bahwa keberhasilan keamanan infrastruktur TI memerlukan pendekatan menyeluruh yang mencakup aspek teknis, kebijakan, dan pelatihan sumber daya manusia. Strategi proaktif seperti pembaruan perangkat lunak, penerapan teknologi keamanan canggih, dan pemantauan aktif dapat mengurangi risiko ancaman siber. Model Keamanan Triad, Kerangka Kerja NIST Cybersecurity, prinsip Zero Trust, dan Framework COBIT diidentifikasi sebagai strategi yang efektif. Regulasi seperti UU ITE dan PP 82/2012, serta koordinasi antar kementerian, dianggap sebagai landasan penting dalam keamanan siber di Indonesia. Pelatihan sumber daya manusia melalui simulasi serangan siber dan program pelatihan keamanan berperan krusial dalam meningkatkan kesadaran dan keterampilan karyawan. Meskipun perubahan perilaku karyawan menjadi tantangan, pemahaman terhadap psikologi manusia sangat penting dalam membangun budaya keamanan yang kuat. Integrasi langkah-langkah ini memungkinkan organisasi untuk melindungi infrastruktur TI dengan lebih baik, menciptakan lingkungan yang aman dan tahan terhadap ancaman siber.Kata kunci: Smart Grid, SCADA, Cyber Security, Risk Management

***Kata Kunci**: Keamanan Infrastruktur TI; Ancaman Cybersecurity; Analisis Tren Cybersecurity.*

PENDAHULUAN

Misalnya, penggunaan internet terus meningkat di Indonesia. Sampai saat ini, dua alat keamanan internet yang sangat penting adalah Virtual Private Networks (VPN) dan The Onion Router (TOR). Namun, ada fenomena di mana personel keamanan dapat menggunakan teknologi ini untuk memelihara server, sehingga mereka dipertanyakan oleh pihak terkait setiap kali menggunakannya.(Indah et al., 2023). Keamanan siber memiliki kedudukan, yang berarti sangat membantu Untuk melindungi data karena perihals Sangat penting untuk melindungi informasi di media. untuk penelitian serta untuk memastikan bahwa data disimpan di lingkungan yang aman dan melindungi sistem data yang terhubung ke siber. Pada (Sudarmadi & Runturambi, 2019)

di Indonesia, budaya Maya tercermin di beberapa platform, termasuk platform media sosial seperti Facebook, Instagram, dan Twitter, serta media arus utama yang digunakan oleh banyak orang dan menyebarkan informasi pribadi. (Setiawan, 2020)

Selain jangkauan siber, data kebocoran juga mewakili potensi teknologi siber di sektor energi. Informasi yang penting dan rahasia, seperti rencana bisnis, informasi pelanggan, dan detail bisnis, dapat dianalisis melalui berbagai sumber atau masalah manusia. Data Kebocoran dapat melindungi privasi pelanggan dan menciptakan pintu untuk infrastruktur penting yang lebih luas. Pada tahun.(Prabowo & Sihaloho, 2023)

Pendekatan terhadap keamanan siber harus ditekankan pada tahun 2023 untuk mengatasi ancaman yang terus memburuk. Tujuan artikel ini adalah untuk mengidentifikasi permasalahan utama yang dihadapi dunia pada tahun ini dan mencari solusi baru yang dapat digunakan untuk mengatasi permasalahan tersebut di atas. Artikel ini diharapkan dapat membantu individu dan organisasi melindungi diri mereka dari situasi yang semakin berbahaya dan merugikan dengan memahami kemajuan teknologi terkini dan ancaman mutakhir dalam keamanan siber.(Wiratama, 2023)

Saat kita memasuki era digital yang mempercepat adopsi Teknologi Informasi (TI), organisasi sangat bergantung pada integritas data dan ketajaman bisnis, karena infrastruktur TI dapat membantu mereka mengatasi siber yang semakin menantang. Terlepas dari banyak kemajuan dalam teknologi keamanan, tantangan ini telah menyebabkan perlunya pemahaman baru tentang strategi dan taktik dalam melindungi aset digital.

Berkaca pada berbagai ancaman yang ada, dapat dipahami bahwa kehadiran teknologi informasi telah membawa perubahan signifikan dalam kehidupan manusia. Sebelumnya, interaksi dan kegiatan manusia lebih banyak dilakukan di dunia nyata. Namun, seiring perkembangan teknologi, individu kini lebih familiar dan bergantung pada dunia maya untuk memenuhi berbagai kebutuhan mereka. Kemajuan teknologi ini telah mendorong masyarakat untuk mengakses dan menyebarkan berbagai informasi secara bebas melalui internet. Internet kini menjadi ruang baru yang memungkinkan komunitas untuk berbagi data, menyampaikan pendapat, serta mengikuti tren dan gaya hidup yang sedang berkembang. (Widiono & Muhammad Ridha Iswardhana, n.d.)

METODE KEGIATAN

Metode pelaksanaan adalah bagian penting dari penelitian ini yang mencakup langkah-langkah yang dilakukan untuk mencapai tujuan penelitian. Bab ini menjelaskan secara rinci bagaimana penelitian ini dilaksanakan, termasuk pendekatan yang digunakan, proses pengumpulan data, dan teknik analisis data yang relevan.

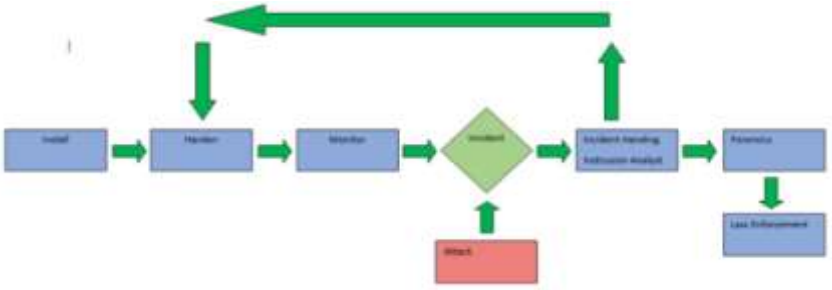
pengumpulan data di sektor energi. Dengan memahami spesifikasi data, peneliti dapat mengidentifikasi potensi risiko dan peluang, seperti bagaimana teknologi siber dapat digunakan untuk meningkatkan keamanan dan efisiensi di sektor terkait. Penelitian ini bertujuan untuk memberikan pemahaman yang lebih dalam. menyeluruh tentang fenomena tersebut dengan menawarkan wawasan hingga pemahaman yang lebih mendalam. Pendekatan kualitatif ini tidak hanya difokuskan pada resu terakhir. (Aji, 2023)

Rancangan penelitian yang digunakan dalam penelitian ini bersifat deskriptif dengan pendekatan kualitatif. Penelitian ini bertujuan untuk memahami secara mendalam konsep, tantangan, dan solusi terkait keamanan siber, khususnya di Indonesia. Studi kasus digunakan untuk mengeksplorasi ancaman siber DDOS yang pernah terjadi dan langkah-langkah mitigasi yang telah dilakukan.

HASIL DAN PEMBAHASAN

Tujuan pengumpulan data adalah untuk menggunakan data yang akurat dan komprehensif Sehingga hasil yang diperoleh tidak bertentangan dengan tujuan yang telah ditetapkan. Tujuan pengumpulan data adalah untuk menggunakan data yang akurat dan komprehensif Sehingga hasil yang diperoleh tidak bertentangan dengan

tujuan yang telah ditetapkan.



Gambar 1 . Ruang Lingkup Kebijakan Cyber Security

Ruang cakupan keamanan siber dimulai dengan instalasi dan dilanjutkan dengan keamanan keras perangkat keras yang digunakan dalam operasi internet dan monitor. Hal ini dilakukan untuk mencegah pencurian atau pencurian yang disebabkan oleh siber dan yang kemudian dapat diatasi dengan investigasi forensik sebagai bagian dari penyelidikan hukum terhadap siber.(Septasari, 2023)

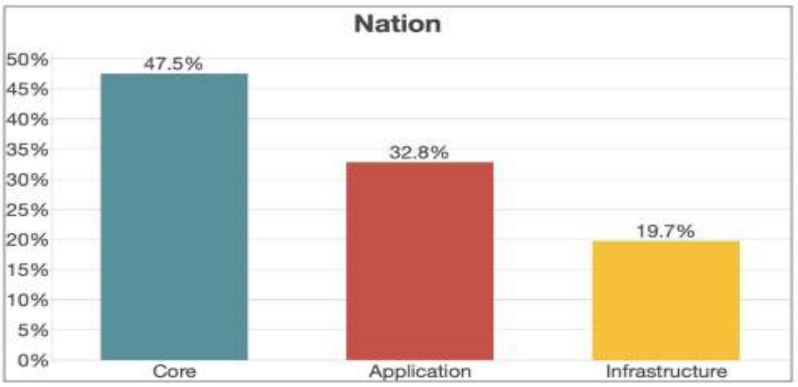
Gambar 2. Triad CIA

Menurut Gambar 1, ada tiga prinsip utama keamanan informasi, yaitu sebagai berikut: (Putri et al., 2022)

1. Kerahasiaan (Kerahasiaan), yang berarti mencegah akses tidak sah ke informasi dan melindungi data sensitif.
2. Ketersediaan (Ketersediaan), yang memastikan bahwa semua informasi dapat diakses dan digunakan kapan pun dibutuhkan tanpa masalah.
3. Integritas, juga dikenal sebagai integritas, adalah perlindungan informasi terhadap korupsi, kerusakan, dan perubahan, antara lain.

Gambar 3 Ketahanan Siber di Ekosistem

Selanjutnya, perlu untuk membantu para pemimpin bisnis dalam menilai risiko yang dihadapi Maya, menyelaraskan strategi mereka dengan tujuan bisnis mereka, dan mengintegrasikan bisnis mereka ke dalam keputusan dan anggaran mereka untuk memastikan manajemen program pendidikan Maya yang efektif. Akhirnya, pemimpin direksi dan pimpinan bisnis didorong untuk membuat pernyataan yang lebih bijaksana tentang risiko terhadap dunia Maya.(Prabowo & Sihaloho, 2023).



Gambar 4 Code Nation

Ada juga peningkatan yang signifikan dalam jumlah aplikasi angka yang digunakan. Hal ini mengindikasikan bahwa Kuwait juga tidak melarang kegiatan warganya online. Hal ini ditunjukkan dengan menyoroti penggunaan media digital di kegiatan publik seperti sektor perdagangan elektronik, sektor keuangan, dan kegiatan sosial. Selain itu, meskipun ada sekitar 20 responden, masalah ini tidak diprioritaskan dalam strategi Kuwait. Peralatan Modernisasi, Diolah Oleh, 2020. The information technology is not selalu menjadi topik utama yang dibahas dalam dokumen. strategis di atas.(Fajri, 2021)

KESIMPULAN

Dimungkinkan untuk mengoptimalkan penilaian keamanan dengan menerapkan kontra intelijen dan mengoptimalkan layanan yang disebutkan di atas. Namun, optimalisasi ini harus memperhatikan kaidah-aturan kerahasia intelijen yang dituangkan pada UU No. 17 Tahun 2011 tentang Intelijen Nasional. Optimalisasi Security Assessment akan berdampak pada faktor teknis, kerja tim, dan organisasi dalam survei Global Cybersecurity Index, sehingga diharapkan pertumbuhan Indonesia akan meningkat pada survei berikutnya.(RIDHO, 2023)

Selanjutnya, peneliti dapat menganalisis data Security Assessment BIN dengan melakukan survei dengan penerima BIN, seperti Juru Bicara atau Deputi Komunikasi dan Informasi BIN. Membandingkan kinerja layanan tersebut dengan hasil survei GCI sebelumnya. Selain itu, para peneliti sedang mempelajari inovasi dalam penilaian keamanan sehingga dapat berkontribusi pada pengembangan kapasitas dan hukum.(Samad, 2022)

Penelitian ini menyimpulkan bahwa keamanan siber di sektor energi, khususnya di Indonesia, memerlukan pendekatan yang holistik dan menyeluruh, mencakup aspek teknis, kebijakan, serta pengembangan sumber daya manusia. Dengan menggunakan pendekatan kualitatif deskriptif, penelitian ini berhasil menggali

tantangan, ancaman, dan solusi yang dihadapi dalam meningkatkan keamanan siber di sektor ini.

Keberhasilan dalam meningkatkan keamanan siber memerlukan integrasi berbagai strategi, termasuk pembaruan teknologi, penerapan kebijakan yang jelas, serta pelatihan dan peningkatan kesadaran sumber daya manusia. Dalam konteks ini, regulasi yang ada, seperti UU ITE dan PP 82/2012, serta koordinasi antar lembaga pemerintah, memberikan dasar yang kuat bagi upaya penguatan keamanan siber di Indonesia.

DAFTAR PUSTAKA

Aji, M. P. (2023). 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]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238.

Eva, N., Karina, R., Mutiara, S., & Saedudin, R. D. R. (2024). Analisis Jaminan Kualitas Sistem Keamanan Siber pada Sistem Informasi: sebuah Studi Literatur. *SITEKNIK: Information Systems, Engineering and Applied Technology*, *1*(2), 76–89.

Fajri, A. (2021). Analisis Konten dalam Strategi Keamanan Siber Kuwait Berdasarkan Teori Three Perspective Theory of Cyber Sovereignty. *Insignia: Journal of International Relations*, 66–80.

Indah, F., Sidabutar, A. Q., & Nasution, N. A. (2023). Peran cyber security terhadap keamanan data penduduk negara Indonesia (Studi kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika*, *1*(1), 57–64.

Jenius, S., MM, C., Santoso, D. R. I. T., & Bakri, T. Y. (2024). OPTIMALISASI KEMAMPUAN LABORATORIUM PENGAMANAN SISTEM DAN JARINGAN (LABPAMSISJAR) DISPAMSANAL GUNA MENGAMANKAN INFRASTRUKTUR INFORMASI VITAL (IIV) DALAM RANGKA MEWUJUDKAN KEAMANAN SIBER TNI ANGKATAN LAUT. *JURNAL ILMIAH KAJIAN KEANGKATANLAUTAN*, *6*(2), 61–70.

Khairunnisa, P. A., Annisa, N., & Parhusip, J. (2024). Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia. *Teknik: Jurnal Ilmu Teknik Dan Informatika*, *4*(2), 9–16.

Najib, W., & Sulistyo, S. (2020). Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi*, *9*(4), 375–384.

Prabowo, T. B., & Sihaloho, R. A. (2023). Analisis ketergantungan indonesia pada teknologi asing dalam sektor energi dan dampaknya pada keamanan nasional. *Jurnal Lemhannas RI*, *11*(1), 72–82.

Putri, T. S., Mutiah, N. M., & Prawira, D. P. (2022). Analisis Manajemen Risiko Keamanan Informasi Menggunakan NIST Cybersecurity Framework dan ISO/IEC 27001: 2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat). *Coding Jurnal Komputer Dan Aplikasi*, *10*(02), 237–248.

RIDHO, O. W. (2023). *ANALISIS SIYASAH DUSTURIYYAH TERHADAP KEGIATAN INTELIJEN OLEH BADAN INTELIJEN NEGARA DAN KOORDINASINYA ANTAR LEMBAGA INTELIJEN BERDASARKAN UNDANG-UNDANG NOMOR 17 TAHUN 2011 TENTANG INTELIJEN NEGARA*. UIN RADEN INTAN LAMPUNG.

Samad, M. Y. (2022). Optimalisasi Layanan Publik Badan Intelijen Negara Dalam Perspektif Global Cybersecurity Index. *AL ULUM: JURNAL SAINS DAN TEKNOLOGI*, *7*(1).

Septasari, D. (2023). The Cyber Security and The Challenge of Society 5.0 Era in Indonesia. *Aisyah Journal Of Informatics and Electrical Engineering (AJIEE)*, *5*(2), 227–233.

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), 7.

Widiono, S., & Muhammad Ridha Iswardhana, M. R. (n.d.). *DIPLOMASI SIBER DAN TEKNOLOGI MOBILE PADA MULTIDISIPLIN*.

Wiratama, A. D. (2023). Cyber Security In 2023: The Latest Challenges And Solutions. *Jurnal Komputer Indonesia*, *2*(1), 47–54.