Jurnal Sains dan Teknologi
Volume 5 No. 2 | Oktober-Desember 2023 |pp: 679-686
E-ISSN : 2714-8661 | DOI : https://doi.org/10.55338/saintek.v5i2.2347

Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman *Cybersecurity*

Mohammad Omer Hoshmand[1*], Suci Ratnawati[2]

[1,2] Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah, Indonesia

Email Penulis Korespondensi: [1]mohammadomer561@gmail.com

Abstrak− Keamanan infrastruktur Teknologi Informasi (TI) telah menjadi kebutuhan mendesak di era digital yang terus berkembang. Penelitian ini bertujuan untuk menganalisis keamanan TI dan mengidentifikasi strategi efektif dalam menghadapi ancaman keamanan siber. Metode penelitian yang digunakan adalah penelitian kualitatif dengan pendekatan studi pustaka, memfokuskan literatur terkini tentang keamanan siber, infrastruktur TI, dan teknologi terkait. Analisis dilakukan terhadap kerangka kerja keamanan umum dan tren terkini untuk mengatasi ancaman siber. Hasil penelitian menunjukkan bahwa keberhasilan keamanan infrastruktur TI memerlukan pendekatan holistik yang mencakup aspek teknis, kebijakan, dan pelatihan sumber daya manusia. Strategi proaktif, seperti pembaruan perangkat lunak, implementasi teknologi keamanan canggih, dan pemantauan proaktif, dapat mengurangi risiko ancaman siber. Model Keamanan Triad, Kerangka Kerja NIST Cybersecurity, prinsip Zero Trust, dan Framework COBIT menjadi strategi yang efektif. Regulasi seperti UU ITE dan PP 82/2012 serta koordinasi antar kementerian diakui sebagai landasan keamanan siber di Indonesia.Pelatihan sumber daya manusia, melalui simulasi serangan siber dan program pelatihan keamanan, menjadi kunci meningkatkan kesadaran dan keterampilan karyawan. Meskipun perubahan sikap dan perilaku karyawan menjadi tantangan, pemahaman psikologi manusia esensial untuk membangun budaya keamanan yang efektif. Integrasi langkah-langkah ini memungkinkan organisasi mencapai keberhasilan melindungi infrastruktur TI, menciptakan lingkungan yang aman dan tahan terhadap ancaman keamanan siber.

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

Abstract− The security of Information Technology (IT) infrastructure has become an urgent necessity in the continually evolving digital era. This research aims to analyze IT security and identify effective strategies to face cybersecurity threats. The research method used is qualitative literature review, focusing on recent literature regarding cybersecurity, IT infrastructure, and related technologies. Analysis was conducted on common security frameworks and current trends in addressing cyber threats. The results indicate that the success of IT infrastructure security requires a holistic approach encompassing technical, policy, and human resource training aspects. Proactive strategies, such as regular software updates, advanced security technology implementation, and proactive monitoring, can mitigate cybersecurity risks. Models like the Security Triad, NIST Cybersecurity Framework, the Zero Trust principle, and the COBIT Framework are identified as effective strategies. Regulations such as the ITE Law and Government Regulation 82/2012, along with inter-ministerial coordination, are acknowledged as the foundation for cybersecurity in Indonesia. Human resource training, through simulated cyber-attacks and security training programs, is key to enhancing employee awareness and skills. Although changing employee attitudes and behaviors pose challenges, understanding human psychology is essential in building an effective security culture. The integration of these measures allows organizations to achieve success in protecting IT infrastructure, creating a secure and resilient environment against cybersecurity threats.

Keywords: IT Infrastructure Security; Cybersecurity Threats; Cybersecurity Trend Analysis

I. PENDAHULUAN

Dalam menghadapi era transformasi digital yang mempercepat adopsi Teknologi Informasi (TI), organisasi dihadapkan pada tantangan signifikan terkait keamanan siber. Keberlanjutan bisnis dan integritas data kini menjadi sangat tergantung pada sejauh mana infrastruktur TI dapat mempertahankan diri dari ancaman siber yang semakin canggih. Meskipun banyak perkembangan teknologi keamanan, tantangan tersebut memunculkan kebutuhan akan pemahaman yang mendalam tentang strategi dan pendekatan terbaru dalam melindungi aset digital [1].

Penelitian ini memfokuskan diri pada analisis keamanan infrastruktur TI dan identifikasi strategi yang efektif dalam menghadapi ancaman keamanan siber. Seiring dengan kompleksitas dan evolusi ancaman tersebut, pemahaman mendalam tentang kerangka kerja keamanan yang diterapkan, tren terkini, dan perbandingan kinerja teknologi keamanan menjadi esensial.

Salah satu kelemahan dalam penelitian keamanan siber saat ini adalah kurangnya pemahaman menyeluruh tentang sejauh mana teknologi keamanan yang diterapkan dapat melindungi infrastruktur TI. Sedangkan literatur keamanan siber telah menyajikan berbagai kerangka kerja dan teknologi, masih ada kebutuhan untuk memetakan keberhasilan implementasi ini dalam situasi dunia nyata. Pemahaman terhadap kesenjangan ini menjadi penting untuk memberikan panduan praktis bagi organisasi dalam meningkatkan ketahanan mereka terhadap ancaman siber. Oleh karena itu, penelitian ini tidak hanya bertujuan untuk mengidentifikasi kerangka kerja keamanan terkini tetapi juga untuk mengisi kesenjangan pengetahuan dalam sejauh mana implementasinya dapat mengatasi ancaman yang semakin kompleks.

Jurnal Sains dan Teknologi
Volume 5 No. 2 | Oktober-Desember 2023 |pp: 679-686
E-ISSN : 2714-8661 | DOI : https://doi.org/10.55338/saintek.v5i2.2347

Melalui analisis literatur dan identifikasi kesenjangan ini, penelitian ini diharapkan dapat memberikan wawasan yang mendalam dan memberikan kontribusi nyata terhadap pengembangan strategi keamanan yang lebih efektif dan adaptif dalam menghadapi ancaman siber yang terus berkembang.

Dalam merinci landasan teoritis yang membentuk dasar penelitian keamanan infrastruktur Teknologi Informasi (TI), beberapa konsep utama perlu dipahami. Konsep-konsep ini memberikan pandangan mendalam tentang prinsip-prinsip dan kerangka kerja yang mendukung perlindungan efektif terhadap ancaman siber yang terus berkembang. Berikut ini adalah pemahaman kerangka kerja yang mendukung perlindungan efektif terhadap ancaman siber:

1.1. *Teori Tritunggal Keamanan (T3)*

Teori Tritunggal Keamanan (T3) adalah suatu pendekatan konseptual dalam keamanan informasi yang menekankan tiga dimensi utama: kerahasiaan, integritas, dan ketersediaan. Ketiga dimensi ini membentuk dasar dari keamanan informasi secara menyeluruh, menyediakan kerangka kerja untuk merancang strategi keamanan yang seimbang dan komprehensif [2].

- Kerahasiaan: Dimensi pertama, kerahasiaan, berkaitan dengan perlindungan terhadap akses yang tidak sah atau tidak diizinkan terhadap informasi. Fokus utamanya adalah menjaga informasi agar hanya dapat diakses oleh pihak yang berwenang. Ini melibatkan penerapan kontrol akses, enkripsi data, dan strategi keamanan lainnya yang mencegah orang atau entitas yang tidak berhak untuk melihat atau menggunakan informasi yang sensitif [3].
- Integritas: Integritas berhubungan dengan keotentikan dan kebenaran informasi. Tujuannya adalah memastikan bahwa informasi tidak diubah atau dimanipulasi secara tidak sah selama penyimpanan, pengiriman, atau pemrosesan. Melalui penerapan tanda tangan digital, verifikasi checksum, dan kontrol integritas data lainnya, organisasi dapat memastikan bahwa informasi tetap utuh dan dapat dipercaya[4].
- Ketersediaan: Dimensi terakhir, ketersediaan, fokus pada ketersediaan dan aksesibilitas informasi ketika dibutuhkan. Ini mencakup langkah-langkah untuk mencegah atau merespons terhadap gangguan layanan, serangan DoS (*Denial of Service*), atau situasi darurat lainnya yang dapat menghambat akses terhadap informasi. Strategi ini mencakup redundant systems, backup rutin, dan perencanaan bencana untuk memastikan bahwa layanan dan informasi tetap tersedia [5].

Implementasi Teori Tritunggal Keamanan membantu organisasi untuk merinci strategi keamanan yang tidak hanya fokus pada satu aspek keamanan, melainkan mencakup kerahasiaan, integritas, dan ketersediaan secara seimbang [6]. Pendekatan ini membantu mencegah penekanan berlebihan pada satu dimensi keamanan yang dapat mengakibatkan ketidakseimbangan dan risiko yang tidak terduga. Dengan mengadopsi T3, organisasi dapat membangun dasar keamanan yang kokoh, melibatkan semua aspek keamanan informasi untuk melindungi integritas, kerahasiaan, dan ketersediaan data dan sistem mereka.

1.2. *Teori Keamanan Berlapis (L3)*

Teori Keamanan Berlapis (L3) adalah konsep keamanan informasi yang menitikberatkan pada ide bahwa pertahanan yang kokoh terhadap ancaman dapat dicapai dengan menerapkan berbagai lapisan keamanan. Dikembangkan oleh ahli keamanan terkemuka, Bruce Schneier, pada tahun 1999, teori ini menciptakan pendekatan yang holistik dan terpadu untuk melindungi sistem dan informasi dari berbagai jenis serangan[7].

1. Berbagai Lapisan Keamanan: Teori Keamanan Berlapis menekankan pentingnya tidak hanya mengandalkan satu mekanisme keamanan, melainkan menerapkan sejumlah lapisan pertahanan. Ini bisa mencakup kombinasi teknologi keamanan seperti firewall, enkripsi, dan deteksi ancaman bersama dengan kebijakan keamanan, prosedur operasional, dan pelatihan karyawan. Dengan menggabungkan berbagai lapisan, organisasi dapat menciptakan dinding pertahanan yang lebih kuat dan tangguh[8].
2. Kombinasi Teknologi, Kebijakan, dan Kesadaran Pengguna: L3 mengakui bahwa keberhasilan keamanan tidak hanya bergantung pada teknologi, tetapi juga pada kebijakan dan kesadaran pengguna. Menerapkan teknologi keamanan tingkat tinggi saja tidak cukup. Organisasi juga perlu memiliki kebijakan keamanan yang jelas dan dapat diterapkan, serta meningkatkan kesadaran pengguna tentang praktik keamanan yang baik[9].
3. Prinsip Pertahanan Dalam Kedalaman: Konsep pertahanan dalam kedalaman (*defense in depth*) menjadi inti dari Teori Keamanan Berlapis. Dalam pertahanan dalam kedalaman, organisasi tidak hanya fokus pada pertahanan pada perimeter saja, tetapi juga menyertakan lapisan keamanan di dalam jaringan dan sistem. Jika satu lapisan keamanan terkompromi, lapisan lainnya dapat tetap melindungi sistem[10].
4. Adaptabilitas dan Fleksibilitas: Teori Keamanan Berlapis mengakui bahwa ancaman keamanan terus berkembang. Oleh karena itu, sistem keamanan harus dapat beradaptasi dan bersifat fleksibel untuk mengatasi ancaman baru yang muncul. Pembaruan reguler terhadap kebijakan keamanan dan teknologi keamanan menjadi penting dalam menjaga keefektifan lapisan keamanan[11]

Dengan menggabungkan berbagai lapisan keamanan, Teori Keamanan Berlapis menciptakan pendekatan yang kuat dan efektif dalam melindungi informasi dan sistem. Melibatkan unsur teknologi, kebijakan, dan kesadaran pengguna menjadikan teori ini sebagai dasar yang kokoh untuk strategi keamanan informasi yang komprehensif. Dengan implementasi L3, organisasi dapat meningkatkan ketahanan mereka terhadap serangan siber yang semakin kompleks dan canggih.

1.3. *Teori Mitigasi Risiko*

Teori Mitigasi Risiko adalah pendekatan sistematis yang menitikberatkan pada pengelolaan dan

Jurnal Sains dan Teknologi
Volume 5 No. 2 | Oktober-Desember 2023 |pp: 679-686
E-ISSN : 2714-8661 | DOI : https://doi.org/10.55338/saintek.v5i2.2347

pengurangan risiko dalam konteks keamanan Teknologi Informasi (TI). Teori ini membantu organisasi untuk secara efektif mengidentifikasi potensi risiko keamanan, menilainya, dan menerapkan strategi mitigasi yang tepat guna untuk mengurangi dampak dari ancaman cybersecurity[12]. Berikut adalah poin-poin utama dalam menjelaskan Teori Mitigasi Risiko:

1. Identifikasi Risiko: Teori Mitigasi Risiko dimulai dengan identifikasi risiko-risiko potensial yang dapat mempengaruhi keamanan TI. Ini melibatkan pengenalan dan pemahaman terhadap ancaman yang mungkin muncul, kerentanan dalam sistem, dan dampak yang mungkin terjadi jika risiko tersebut terealisasi [13].
2. Penilaian Risiko: Setelah identifikasi risiko dilakukan, langkah berikutnya adalah melakukan penilaian risiko. Ini melibatkan evaluasi lebih lanjut terhadap probabilitas terjadinya risiko dan dampak yang mungkin timbul. Penilaian ini membantu menentukan risiko mana yang memiliki prioritas tinggi dan memerlukan perhatian lebih lanjut[14].
3. Strategi Mitigasi: Dalam Teori Mitigasi Risiko, fokus utama adalah pada pengembangan strategi mitigasi. Strategi ini dirancang untuk mengurangi kemungkinan terjadinya risiko atau mengurangi dampaknya jika terjadi. Strategi ini bisa mencakup penerapan kontrol keamanan tambahan, pembaruan perangkat lunak secara berkala, atau pengembangan kebijakan dan prosedur keamanan[15].
4. Pemantauan dan Evaluasi: Pemantauan risiko adalah bagian integral dari teori ini. Organisasi perlu terus memantau lingkungan keamanan mereka untuk mengidentifikasi perubahan dalam ancaman atau kerentanan. Selain itu, evaluasi secara berkala terhadap efektivitas strategi mitigasi perlu dilakukan untuk memastikan bahwa strategi tersebut masih relevan dan berfungsi sesuai yang diharapkan[16].
5. Resiliensi dan Pemulihan: Teori Mitigasi Risiko juga mengakui pentingnya memiliki rencana resiliensi dan pemulihan. Jika risiko tersebut tetap terjadi, organisasi perlu siap untuk merespons dan memulihkan sistem mereka dengan cepat. Ini melibatkan perencanaan pemulihan setelah insiden, termasuk backup rutin, pemulihan data, dan latihan simulasi respons keamanan[17].

Dengan mengadopsi Teori Mitigasi Risiko, organisasi dapat mengelola risiko keamanan TI mereka secara proaktif. Identifikasi, penilaian, dan penerapan strategi mitigasi yang efektif membantu melindungi aset dan data organisasi dari ancaman cybersecurity. Pemahaman yang mendalam terhadap lingkungan keamanan membantu organisasi beradaptasi dengan perubahan dan tetap tangguh di tengah ancaman yang terus berkembang.

Dengan membangun landasan teori pada prinsip-prinsip ini, penelitian dapat menggali lebih lanjut tentang implementasi praktis dan efektivitas kerangka kerja keamanan siber dalam mengatasi ancaman yang berkembang dalam infrastruktur TI. Pemahaman mendalam terhadap prinsip-prinsip ini akan membantu merancang strategi keamanan yang terkini dan responsif.

II. METODE PENELITIAN

Metode penelitian yang akan digunakan dalam penelitian ini adalah penelitian kualiatif dengan pendekatan studi pustaka.[18] Langkah awal melibatkan pemilihan sumber literatur yang relevan dengan keamanan siber, infrastruktur TI, dan teknologi terkait. Jurnal ilmiah, buku referensi, laporan penelitian, dan artikel terkini akan menjadi fokus utama untuk mendapatkan wawasan mendalam. Setelah pemilihan sumber, penelitian akan melibatkan review dan analisis terperinci terhadap literatur yang terpilih. Fokus utama analisis adalah pada kerangka kerja keamanan yang umum diterapkan, tren terkini dalam ancaman siber, serta teknologi dan strategi keamanan yang dapat efektif dalam melindungi infrastruktur TI.

Selanjutnya, temuan literatur akan diklasifikasikan ke dalam kategori-kategori utama, seperti aspek teknis, kebijakan keamanan, pelatihan sumber daya manusia, dan integrasi teknologi keamanan. Tujuannya adalah memberikan pemahaman yang lebih sistematis tentang elemen-elemen kunci yang mempengaruhi keamanan infrastruktur TI. Pemahaman mendalam tentang area-area di mana informasi mungkin belum memadai atau di mana diperlukan penelitian lebih lanjut akan menjadi dasar bagi pengembangan penelitian ini.

Hasil dari studi pustaka ini akan digunakan untuk merangkum temuan literatur dan mengembangkan kesimpulan tentang kondisi keamanan infrastruktur TI saat ini. Lebih lanjut, penelitian ini akan menyusun rekomendasi praktis berdasarkan literatur yang telah dianalisis, memberikan panduan bagi organisasi dalam meningkatkan strategi keamanan mereka menghadapi ancaman siber yang terus berkembang. Dengan pendekatan studi pustaka ini, diharapkan penelitian dapat memberikan kontribusi yang berharga terhadap pemahaman dan penanganan efektif terhadap ancaman keamanan siber dalam konteks infrastruktur TI.

III. HASIL DAN PEMBAHASAN

3.1. Ancaman Cybersecurity

Ancaman cybersecurity merupakan kompleksitas tantangan yang memerlukan pemahaman mendalam untuk melindungi infrastruktur TI dari ancaman yang terus berkembang. Ancaman ini dapat mengintai dari berbagai arah, baik dari luar maupun dari dalam organisasi [19]. Untuk memberikan pemahaman yang lebih rinci, kita dapat merinci ancama-anacaman tersebut ke dalam tiga kategori utama.

3.1.1. Ancaman Fisik

Ancaman fisik mencakup potensi kerusakan atau kehilangan terhadap komponen fisik infrastruktur TI. Ini dapat melibatkan pencurian perangkat keras, perusakan fisik, atau sabotase. Ancaman fisik dapat merusak integritas perangkat keras, pusat data, atau fasilitas fisik lainnya, dan dampaknya dapat mencakup gangguan operasional, kehilangan data, atau bahkan ketidakberlanjutan layanan[20]. Upaya pencegahan dan

Jurnal Sains dan Teknologi
Volume 5 No. 2 | Oktober-Desember 2023 |pp: 679-686
E-ISSN : 2714-8661 | DOI : https://doi.org/10.55338/saintek.v5i2.2347

perlindungan terhadap aset fisik, seperti pusat data dan perangkat keras kritis, menjadi esensial untuk memitigasi risiko fisik ini.

Ancaman fisik terhadap infrastruktur TI merupakan suatu ancaman yang memerlukan tindakan pencegahan dan perlindungan yang cermat. Potensi kerusakan atau kehilangan terhadap komponen fisik dapat memiliki dampak signifikan terhadap integritas, ketersediaan, dan operasional keseluruhan infrastruktur TI. Oleh karena itu, strategi pencegahan dan perlindungan terhadap ancama fisik menjadi krusial dalam memitigasi risiko fisik ini. Pencegahan Pencurian Perangkat Keras Pencurian perangkat keras dapat menyebabkan kerugian finansial dan kehilangan data yang penting. Untuk mencegah pencurian, langkah-langkah berikut dapat diimplementasikan:

- Menerapkan sistem keamanan fisik seperti kamera pengawas, kontrol akses, dan penjaga keamanan di lokasi pusat data atau ruang server.
- Melakukan pencatatan inventaris yang akurat dan pemantauan terhadap perangkat keras untuk mendeteksi setiap perubahan atau kehilangan.
- Membangun pusat data dengan pertimbangan desain tahan bencana untuk melindungi perangkat keras dari gempa, banjir, atau kejadian alam lainnya.
- Mengembangkan prosedur evakuasi dan pemulihan darurat untuk mengatasi ancaman fisik yang dapat menyebabkan kerusakan.
- Pemantauan Aktivitas Suspicious: Melakukan pemantauan terus-menerus terhadap aktivitas di sekitar fasilitas dan mengidentifikasi tanda-tanda kegiatan mencurigakan.
- Memberikan pelatihan kepada karyawan untuk mengenali potensi ancaman dan melaporkannya dengan segera.
- Backup Redundansi: Menyediakan backup dan sistem redundansi untuk memastikan kelangsungan operasional bahkan dalam situasi darurat.
- Menerapkan keamanan jaringan untuk mencegah akses yang tidak sah dan melindungi data yang disimpan di perangkat keras.

Ancaman fisik terhadap infrastruktur TI memerlukan respons holistik yang mencakup pencegahan, deteksi, dan respons cepat. Dengan menerapkan strategi perlindungan dan tindakan pencegahan yang cermat, organisasi dapat meminimalkan risiko fisik, menjaga integritas perangkat keras, dan melindungi layanan TI yang kritis. Penting untuk terus memperbarui strategi keamanan fisik sesuai dengan perkembangan teknologi dan ancaman baru yang muncul.

3.1.2. Acaman Logikal

Ancaman logikal terhadap infrastruktur TI melibatkan berbagai serangan yang ditujukan pada aspek digital. Memahami dan menghadapi ancaman logikal ini memerlukan strategi yang holistik, termasuk deteksi dini, pencegahan, dan respons cepat untuk meminimalkan dampak yang mungkin timbul. *Malware* merupakan istilah umum yang mencakup berbagai jenis perangkat lunak berbahaya, seperti virus, worm, dan trojan. Serangan malware bertujuan untuk menyusup ke dalam sistem komputer dan merusaknya [21]. Virus dapat menempel pada file atau program dan menyebar saat file atau program tersebut dieksekusi. Worm dapat menyebar sendiri melalui jaringan, sedangkan trojan menyamar sebagai program yang berguna untuk mengelabui pengguna dan kemudian mengeksploitasi sistem. Selain merusak sistem, malware juga dapat mencuri data sensitif seperti informasi login atau informasi keuangan.

Sementara itu, *Teknik phishing* melibatkan upaya untuk mendapatkan informasi rahasia atau sensitif dengan menyamar sebagai entitas tepercaya. Ini sering dilakukan melalui surel atau situs web palsu yang meniru tampilan situs resmi. Phishing dapat mencakup pengiriman surel palsu yang meminta pengguna untuk memasukkan kata sandi, informasi keuangan, atau data pribadi lainnya. Serangan phishing dapat sangat persuasif, menggunakan manipulasi psikologis untuk membuat pengguna terperangkap dan memberikan informasi sensitif mereka tanpa curiga.

Serangan *social engineering* memanfaatkan manipulasi psikologis pada manusia untuk mendapatkan informasi rahasia atau akses ke sistem. Penyerang dapat menggunakan berbagai taktik, seperti membangkitkan rasa urgensi atau menciptakan skenario palsu untuk mendapatkan kepercayaan korban. Ini dapat melibatkan panggilan telepon palsu, surel palsu, atau interaksi langsung dengan tujuan mengelabui orang untuk memberikan informasi yang seharusnya tidak mereka bagikan.

Ransomware adalah jenis malware yang mengenkripsi data pada suatu sistem dan kemudian menuntut pembayaran tebusan agar akses ke data tersebut dikembalikan. Penyerang sering menggunakan enkripsi yang sangat kuat, membuat sulit atau bahkan tidak mungkin untuk memulihkan data tanpa kunci enkripsi yang benar. Umumnya, tebusan diminta dalam bentuk mata uang kripto untuk mempersulit pelacakan. Ransomware dapat merugikan korban secara finansial dan dapat menyebabkan kerugian data yang signifikan jika tebusan tidak dibayar atau jika data tidak dapat dipulihkan dari cadangan yang memadai.

Untuk melindungi infrastruktur TI dari serangan logikal yang mencakup malware, phishing, social engineering, dan ransomware, diperlukan strategi pencegahan yang holistik. Berikut adalah langkah-langkah yang dapat diambil untuk mengurangi risiko dan memitigasi dampak serangan tersebut:

- Penggunaan Firewall : Menerapkan firewall yang kuat untuk memantau dan mengontrol lalu lintas jaringan, menghalangi akses yang tidak sah, dan melindungi sistem dari serangan luar.
- Antivirus dan Anti-Malware : Memasang dan memperbarui perangkat lunak antivirus dan anti-malware secara teratur untuk mendeteksi dan menghilangkan ancaman malware yang mungkin muncul.
- Enkripsi Data : Menggunakan teknologi enkripsi untuk melindungi data, baik saat transit maupun saat disimpan, sehingga data yang dicuri tidak dapat dibaca oleh pihak yang tidak sah.

Jurnal Sains dan Teknologi
Volume 5 No. 2 | Oktober-Desember 2023 |pp: 679-686
E-ISSN : 2714-8661 | DOI : https://doi.org/10.55338/saintek.v5i2.2347

- Pelatihan Keamanan bagi Pengguna : Memberikan pelatihan keamanan kepada pengguna untuk meningkatkan kesadaran mereka terhadap ancaman phishing dan social engineering serta mengajarkan praktik keamanan yang baik.
- Pemantauan Sistem: Melakukan pemantauan aktif terhadap aktivitas sistem dan jaringan untuk mendeteksi pola atau perilaku yang mencurigakan.
- Sistem Intrusi: Menerapkan sistem deteksi intrusi yang dapat secara otomatis mendeteksi dan merespons serangan siber yang terjadi.
- Penanganan Kejadian Keamanan: Membangun prosedur penanganan kejadian keamanan yang jelas untuk merespons dengan cepat ketika serangan logikal terdeteksi.

Ancaman logikal terhadap infrastruktur TI memerlukan pendekatan yang menyeluruh, menggabungkan pencegahan, deteksi dini, dan respons cepat. Dengan menggunakan kombinasi teknologi keamanan, pelatihan untuk pengguna, dan sistem pemantauan yang efektif, organisasi dapat mengurangi risiko dari serangan logikal, melindungi integritas sistem, dan meminimalkan potensi kerugian data. Terus meningkatkan strategi keamanan sesuai dengan perkembangan teknologi dan taktik serangan siber yang baru akan menjadi kunci dalam menjaga keamanan infrastruktur TI.

3.1.3. Ancaman Operasional

Ancaman operasional merupakan tantangan serius yang timbul dari faktor internal di dalam suatu organisasi, dapat berupa kesalahan manusia, kelalaian, atau ketidakpatuhan terhadap prosedur keamanan. Kesalahan manusia seperti konfigurasi sistem yang salah atau penghapusan data tidak sengaja dapat merugikan keberlanjutan operasional. Untuk mengatasi hal ini, pelatihan karyawan secara rutin dan otomatisasi proses dapat menjadi langkah pencegahan yang efektif [22]. Kelalaian, yang mencakup kurangnya perhatian dalam tugas-tugas operasional, juga dapat menjadi sumber ancaman. Kebijakan keamanan yang jelas dan monitoring aktivitas pengguna membantu mengurangi risiko dari kelalaian ini.

Ancaman juga dapat muncul dari ketidakpatuhan terhadap prosedur keamanan yang telah ditetapkan. Edukasi karyawan tentang pentingnya mematuhi prosedur keamanan, bersamaan dengan sanksi atau konsekuensi untuk pelanggaran, menjadi kunci dalam mengurangi ancaman ini. Pengelolaan akses karyawan yang baik, melalui prinsip kepisahan kewenangan dan pemantauan akses, dapat membantu mengurangi potensi risiko.

Pentingnya menerapkan prinsip keamanan pada tingkat operasional juga tidak bisa diabaikan. Analisis risiko operasional secara teratur membantu organisasi mengidentifikasi potensi ancaman dan mengambil tindakan preventif yang sesuai. Perbaikan berkelanjutan berdasarkan temuan dari analisis risiko akan meningkatkan kemampuan organisasi dalam menghadapi ancaman operasional secara efektif. Dengan pendekatan yang holistik ini, organisasi dapat mengoptimalkan keamanan infrastruktur TI mereka dan melindungi kelangsungan operasional dari potensi risiko internal.

3.2. Pendekatan Strategis dalam Menghadapi ancaman Keamanan Siber

3.2.1. Implementasi Model Keamanan Triad

Dalam jurnal tersebut, penelitian oleh Žiga (2022), membahas pentingnya keamanan siber dalam industri konstruksi dan mengusulkan sebuah kerangka kerja. Model Keamanan Triad, yang melibatkan tiga elemen utama yaitu kerahasiaan, integritas, dan ketersediaan, dapat diintegrasikan ke dalam kerangka kerja ini untuk memperkuat strategi keamanan. Dalam konteks Model Keamanan Triad, kerahasiaan berkaitan dengan menjaga kerahasiaan informasi dan data yang krusial untuk industri konstruksi. Ini termasuk melindungi data desain, rencana konstruksi, dan informasi kritis lainnya dari akses yang tidak sah atau pencurian [23].

Integritas, sebagai elemen kedua dalam Model Keamanan Triad, mencakup upaya untuk mencegah dan mendeteksi perubahan yang tidak sah atau tidak diinginkan pada data. Dalam industri konstruksi, integritas data menjadi krusial untuk memastikan bahwa desain dan rencana tidak dimanipulasi atau diubah tanpa izin. Sementara itu, ketersediaan berfokus pada memastikan bahwa sistem dan layanan yang terlibat dalam industri konstruksi tetap beroperasi dan dapat diakses saat diperlukan. Ancaman terhadap ketersediaan dapat mencakup serangan DDoS atau upaya lain untuk menonaktifkan infrastruktur konstruksi digital. Dengan mengintegrasikan Model Keamanan Triad ke dalam kerangka kerja yang dikembangkan, penelitian ini dapat memberikan pendekatan yang holistik untuk keamanan siber dalam industri konstruksi. Penggunaan Model Keamanan Triad dapat memastikan bahwa tidak hanya aspek-aspek teknis keamanan tercakup, tetapi juga mencakup kebutuhan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi yang vital dalam konteks konstruksi.

3.2.2. Adopsi Kerangka Kerja NIST Cybersecurity

Penelitian yang dilakukan oleh Vicky Mahendra pada tahun 2023 menonjolkan beberapa kelebihan yang memberikan kontribusi penting dalam konteks manajemen risiko keamanan siber di Kementerian PUPR. Pertama, penggunaan Kerangka Kerja NIST Cybersecurity menunjukkan kebijakan penelitian yang kuat dan terukur, memberikan landasan yang jelas dan terstruktur untuk mengatasi tantangan keamanan siber. Kedua, pendekatan holistik Kerangka Kerja NIST yang mencakup tahap Identify, Protect, Detect, dan Respond memberikan pandangan menyeluruh terhadap aspek keamanan, membantu organisasi dalam mengidentifikasi, melindungi, mendeteksi, dan merespons serangan siber secara efektif. Selain itu, penelitian ini menghadirkan rekomendasi konkret dengan mengevaluasi kesenjangan antara kondisi saat ini dan yang diinginkan, memberikan panduan praktis bagi Kementerian PUPR untuk meningkatkan kematangan keamanan siber pada tingkat aplikasi[24]. Dengan demikian, kelebihan penelitian ini mencakup pendekatan metodologis yang kokoh, penggunaan kerangka kerja industri terkemuka, dan memberikan

Jurnal Sains dan Teknologi
Volume 5 No. 2 | Oktober-Desember 2023 |pp: 679-686
E-ISSN : 2714-8661 | DOI : https://doi.org/10.55338/saintek.v5i2.2347

solusi terukur untuk menghadapi ancaman keamanan siber.

3.2.3. Penerapan Prinsip Zero Trust

Penelitian yang dilakukan oleh Marcus Tanquea dan Harry J. Foxwellb pada tahun 2023 dalam artikel "Risiko Dunia Maya pada Platform IoT dan Solusi Zero Trust" membahas secara mendalam perkembangan solusi keamanan siber terkini. Mereka mengidentifikasi bahwa organisasi, dalam beberapa tahun terakhir, telah aktif mengembangkan kebijakan, prosedur, teknik, dan kerangka kerja keamanan siber untuk menanggulangi ancaman dan risiko terhadap sistem jaringan mereka. Fokus utama penelitian ini adalah pada keamanan, perlindungan, dan interoperabilitas perangkat Zero Trust dan Internet of Things (IoT). Para peneliti menjelaskan bagaimana konsep dan metode Zero Trust dapat memberikan solusi keamanan yang efektif untuk aplikasi dan titik akhir perusahaan, dengan penekanan khusus pada keamanan sistem IoT. Mereka mencermati perbedaan Zero Trust dengan perimeter jaringan tradisional dan membahas implementasi Arsitektur Jaringan Zero Trust yang berfokus pada verifikasi identitas perangkat dan kebijakan akses yang eksplisit. Selain itu, penelitian ini memberikan rekomendasi terkait solusi, kebijakan, dan kerangka kerja keamanan di masa depan, serta menegaskan bahwa organisasi perlu mengembangkan dan menerapkan praktik terbaik keamanan untuk memastikan federasi platform yang berkelanjutan di antara perangkat/objek IoT [25].

3.2.4. Menggunakan COBIT untuk Pengelolaan dan Pengukuran Kinerja

Penelitian yang dilakukan oleh Chrisandy Arya Frammy Haullussy pada tahun 2019 menunjukkan bahwa Framework COBIT (Control Objectives for Information and Related Technologies) digunakan sebagai landasan untuk mengelola dan mengamankan Teknologi Informasi (TI) secara efektif. Kerangka kerja ini difokuskan pada tiga aspek kunci: pengelolaan risiko, kontrol internal, dan pengukuran kinerja. Dengan menggunakan COBIT, penelitian ini mengarah pada pemahaman yang lebih mendalam terhadap bagaimana organisasi dapat mengidentifikasi, menilai, dan mengelola risiko terkait keamanan siber secara sistematis. Selain itu, COBIT memberikan panduan mengenai implementasi kontrol internal yang diperlukan untuk memitigasi risiko dan melindungi aset TI. Pemilihan COBIT juga menekankan pentingnya pengukuran kinerja untuk memastikan bahwa strategi keamanan yang diadopsi mencapai tujuan yang diinginkan.

Dengan demikian, menggunakan Framework COBIT sebagai dasar teoritis memberikan kerangka yang kokoh untuk memahami dan meningkatkan keamanan siber [26].

3.2.5. Peran Kebijakan Keamanan

Kebijakan keamanan yang ketat menjadi pilar esensial dalam melindungi infrastruktur TI dari serangan siber. Kebijakan tersebut tidak hanya mengatur penggunaan teknologi, tetapi juga memberikan pedoman untuk adaptasi terhadap ancaman baru. Namun, hasil penelitian menunjukkan bahwa tantangan utama dalam konteks kebijakan adalah kebutuhan untuk keseimbangan yang tepat antara ketatnya kontrol dan fleksibilitas untuk menanggapi ancaman baru. Kebijakan yang dapat disesuaikan dan responsif menjadi kunci dalam menghadapi ancaman yang berkembang.

Analisis tentang keterkaitan antara Keamanan Siber dan Pertahanan Siber serta dasar hukum yang mengatur keduanya telah dibahas dengan detail sebelumnya. Kedua konsep ini memiliki tujuan utama untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi elektronik atau Sistem Elektronik. Keamanan Siber diakui sebagai bentuk dari Pertahanan Siber, dan keduanya dapat diselenggarakan oleh individu, kelompok, atau negara, dengan fokus pada keamanan nasional dan kelangsungan pelayanan publik.

Pentingnya peran regulasi, khususnya UU ITE dan PP 82/2012, dalam membentuk dasar organik bagi keamanan dan pertahanan siber nasional telah diuraikan. Penekanan pada peraturan tersebut mencakup standar yang tinggi untuk Penyelenggara Sistem Elektronik, terutama yang bersifat publik, untuk memastikan keandalan, keamanan, dan ketersediaan sistem mereka. Selanjutnya, koordinasi antara Kementerian Komunikasi dan Informatika serta Kementerian Pertahanan dianggap penting untuk memastikan pengawasan dan pengaturan yang efektif dalam keamanan dan pertahanan siber. Pembentukan regulasi, pembangunan CSIRT di seluruh provinsi, penegakan hukum, dan budaya keamanan informasi merupakan langkah-langkah strategis yang diusulkan untuk membangun keamanan siber secara holistik. Dalam konteks pertahanan siber untuk kepentingan perang, peran aktif Tentara Nasional menjadi esensial. Namun, tantangan utama muncul dalam menghadapi perang siber yang bersifat laten, di mana serangan siber dapat terjadi tanpa identifikasi jelas dari negara tertentu. Oleh karena itu, perlunya Strategi Nasional Keamanan Siber dan Pertahanan Siber yang menyeluruh menjadi pokok pembahasan berikutnya.

Strategi nasional ini perlu mencakup penilaian ancaman dan kelemahan infrastruktur strategis, pengelolaan sumber daya untuk penguatan keamanan dan pertahanan siber, serta pengembangan sistem yang responsif. Prioritas penguatan Sistem Elektronik Infrastruktur Strategis dan komunikasi yang luas melibatkan teknologi internet menjadi fokus utama dalam menghadapi perkembangan pesat dalam bidang Teknologi Informasi dan Komunikasi (TIK) [27].

Sebagai kesimpulan, analisis ini menggambarkan kompleksitas dan urgensi perlunya keamanan dan pertahanan siber dalam konteks nasional Indonesia. Dengan dasar hukum yang kuat, regulasi yang responsif, dan koordinasi yang efektif, diharapkan strategi nasional dapat membentuk fondasi yang kokoh dalam menghadapi tantangan ancaman siber di masa depan.

3.2.6. Pelatihan Sumber Daya Manusia

Pelatihan sumber daya manusia diidentifikasi sebagai elemen kunci untuk mencapai keamanan yang optimal. Simulasi serangan siber dan program pelatihan

keamanan meningkatkan kesadaran dan keterampilan karyawan dalam menghadapi ancaman siber. Meskipun demikian, temuan penelitian menunjukkan bahwa perubahan sikap dan perilaku karyawan terhadap keamanan merupakan tantangan tersendiri. Pentingnya mendekati pelatihan dengan pemahaman psikologi dan motivasi manusia menjadi sorotan dalam membangun budaya keamanan yang efektif.

Dengan menggabungkan langkah-langkah ini, organisasi dapat mencapai keberhasilan dalam melindungi infrastruktur TI dari ancaman siber yang terus berkembang. Pendekatan holistik ini memastikan bahwa tidak hanya teknologi, tetapi juga kebijakan dan sumber daya manusia terlibat dalam menciptakan lingkungan yang aman dan tahan terhadap ancaman keamanan siber

IV. KESIMPULAN
V.

Dalam rangka menghadapi ancaman keamanan siber yang semakin kompleks, penelitian ini menunjukkan bahwa keberhasilan keamanan infrastruktur Teknologi Informasi (TI) memerlukan pendekatan holistik. Ancaman fisik, logikal, dan operasional menjadi fokus analisis, dengan strategi proaktif seperti pembaruan perangkat lunak, implementasi teknologi keamanan canggih, dan pelatihan karyawan diakui sebagai kunci kesuksesan. Beberapa pendekatan strategis yang disorot meliputi implementasi Model Keamanan Triad, adopsi Kerangka Kerja NIST Cybersecurity, penerapan prinsip Zero Trust, penggunaan Framework COBIT untuk pengelolaan dan pengukuran kinerja, dan peran penting kebijakan keamanan. Dalam konteks Indonesia, regulasi seperti UU ITE dan PP 82/2012 serta koordinasi antar kementerian diakui sebagai landasan untuk menghadapi ancaman siber.

Pelatihan sumber daya manusia menjadi kunci, dengan simulasi serangan siber dan program pelatihan keamanan berperan penting dalam meningkatkan kesadaran dan keterampilan karyawan. Meskipun demikian, perubahan sikap dan perilaku karyawan menjadi tantangan, dan pemahaman psikologi manusia dianggap esensial dalam membangun budaya keamanan yang efektif. Dengan mengintegrasikan langkah-langkah ini, organisasi dapat mencapai keberhasilan dalam melindungi infrastruktur TI dari ancaman siber, menciptakan lingkungan yang aman dan tahan terhadap ancaman keamanan siber dengan pendekatan holistik.

VI. REFERENSI

[1] Ar Rahman, L. L. (2020). Implications of Defense Diplomacy on Cybersecurity in Context Security Politics. Jurnal Diplomasi Pertahanan, 6(2), 1. ISSN 2746-8496.

[2] Kusumaatmadja, M. (1990). Keamanan Nasional Indonesia: Konsep, Strategi, dan Pelaksanaannya. Jakarta: Bina Aksara.

[3] Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & Suwarno, P. (2022). Ancaman Serangan Siber pada Keamanan Nasional Indonesia. Jurnal Kewarganegaraan, 6(1)

[4] Santoso, K. I. (2018). Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional. Lemhannas RI

[5] Al-Masri, M. A. (2018). A Framework for Information Availability Management. Journal of Information Security, 6(1).

[6] Andhika Gusni, R. S., Kraugusteeliana, & Pradnyana, I. W. W. (2021). Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan COBIT 2019. In Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA) (pp. 420). Jakarta, Indonesia: Universitas Pembangunan Nasional Veteran Jakarta. e-ISBN 978-623-93343-4-5.

[7] Farizy, S., & Eriana, E. S. (2022). Keamanan Sistem Informasi. Tangerang Selatan: Unpam Press. ISBN: 978-623-6352-68-7.

[8] Samal, A. K. (2018). A Security in Depth Framework for Enterprise Information Systems. ACM Transactions on Information Systems Security, 16(3).

[9] Budi, E. (2021). Strategies For Strengthening Cyber Security To Achieve National Security in Society 5.0. Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia, Volume 3, 223-234. DOI: 10.54706/senastindo.v3.2021.141

[10] Farizy, S., & Eriana, E. S. (2022). Keamanan Sistem Informasi. Tangerang Selatan: Unpam Press. ISBN: 978-623-6352-68-7.

[11] Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber dan Sandi Negara. Jurnal Dinamika Global, 7(2). https://doi.org/10.36859/jdg.v7i02.1187

[12] Whitman, M., & Mattord, H. (2018). Managing Information Security Risks: A Practical Approach. Pearson Education.

[13] Anshori, F. A., Suprapto, & Perdanakusuma, A. R. (2019). Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 3(2), 1701-1707. http://j-ptiik.ub.ac.id.

[14] Nurdin, I. M., & Budiman, M. A. (2021). Implementasi Manajemen Risiko dalam Meningkatkan Keamanan Informasi. Jurnal Manajemen Risiko, 3(2), Desember 2021.

[15] Nugraheni, A. F. D., & Nurcahyani, I. S. R. (2022). Penerapan Manajemen Risiko Keamanan Informasi dalam Organisasi. Jurnal Ilmiah Teknologi Informasi dan Komunikasi, 16(2), November 2022.

[16] Najib, W. (2020). Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things

(Review on Security Threat and Solution of Internet of Things Technology). Jurnal Nasional Teknik Elektro dan Teknologi Informasi, 9(4), 375. ISSN 2301-4156.

[17] Sanjaya, B. R., Efrianti, D., Ali, M., Prasetyo, T., Mukhtadi, M., Widasari, Y. K., & Khumairoh, Z. (2022). Pengembangan Cyber Security dalam Menghadapi Cyber Warfare di Indonesia. Journal of Advanced Research in Defense and Security Studies, 1(1), 19-34. Available online at: https://ejournal.hakhara-institute.org/index.php/JARDS

[18] Creswell, J. W., & Plano Clark, V. L. (1993). Qualitative Research: A Review of the Methods and Techniques. Journal of Social Work Education, 29(3), Fall 1993.

[19] Ramadhani, M. R. (2020). Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia. Yogyakarta: Fakultas Teknologi Industri UII.

[20] Rahmawati, C. (2019). Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0. Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO AAU), Vol. 1(1), 299-306. ISSN 2685-8991.

[21] Farizy, S., & Eriana, E. S. (2022). Keamanan Sistem Informasi. Tangerang Selatan: Unpam Press. ISBN: 978-623-6352-68-7.

[22] Budi, E. (2021). Strategies For Strengthening Cyber Security To Achieve National Security in Society 5.0. Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia, Volume 3, 223-234. DOI: 10.54706/senastindo.v3.2021.141.

[23] Turki, Ż., de Soto, B. G., Mantha, B. R. K., Maciel, A., & Georgescu, A. (2022). "A Systemic Framework for Addressing Cybersecurity in Construction." Automation in Construction, 133, 103988. https://doi.org/10.1016/j.autcon.2021.103988

[24] Mahendra, V. (2023). Perancangan Kerangka Kerja Keamanan Siber Menggunakan NIST Cybersecurity Framework dan CIS Controls. Universitas Bina Nusantara, Jakarta.

[25] Tanque, M., & Foxwell, H. J. (2023). Risiko Dunia Maya pada Platform IoT dan Solusi Zero Trust. Kemajuan Komputer, 131, 79-148. https://doi.org/10.1016/bs.adcom.2023.04.003

[26] TI. Haullussy, C. A. F. (2019). Audit Sistem Informasi Pelayanan Menggunakan Framework COBIT 4.1: Studi Kasus di Dinas Perpustakaan dan Kearsipan Kota Salatiga. Artikel Ilmiah. Universitas Kristen Satya Wacana, Salatiga

[27] Aptika. (2016, March 10). Kebijakan Keamanan dan Pertahanan Siber. Aptika. https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/