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

KEAMANAN INFRASTRUKTUR TEKNOLOGI INFORMASI: ANALISIS ANCAMAN SIBER DAN PENDEKATAN MITIGASI

Rizki Sandrina Ayu[1], Muhammad Marshell Rivai[2], Naufal Al Mubarak[3], Dicky Pratama[4]
[1,2,3,4] Program Studi Sistem Informasi, Fakultas Ilmu Komputer dan Rekayasa, Universitas Multi Data Palembang
neechan354@mhs.mdp.ac.id[1], rizkisandrina19@mhs.mdp.ac.id[2], rizkisandrina19@mhs.mdp.ac.id[3], dqpratama@mdp.ac.id[4]

Abstract

The rapid development of information technology has increased the risks to information technology (IT) infrastructure, potentially jeopardizing the operational continuity of organizations. This study aims to provide a comprehensive analysis of cyber threats and applicable solutions to protect IT infrastructure. The research method employed is a literature review that explores theories from previous studies, books, articles, and other sources. This study seeks to understand various cyber threats, including external threats such as viruses, ransomware, DDoS attacks, and hacking, as well as internal threats related to data breaches and human error. Based on the analysis of existing threats, the study identifies several mitigation strategies, including enhancing threat detection capabilities, educating users on cybersecurity practices, and developing effective early warning systems. The findings indicate that strengthening internal controls and implementing frameworks such as COBIT 2019, NIST Cybersecurity, and ISO/IEC 27001 can improve organizational resilience against increasingly complex threats. This research provides practical guidance to assist organizations in raising awareness of the importance of cybersecurity and building systems that are more secure and resilient against evolving threats.
Keywords**:** IT Infrastructure, Cyber Threats, Cybersecurity

Abstrak

Perkembangan teknologi informasi yang cepat telah meningkatkan risiko terhadap infrastruktur teknologi informasi (TI), yang dapat membahayakan kelangsungan operasional organisasi. Penelitian ini bertujuan untuk memberikan analisis menyeluruh tentang ancaman siber dan solusi yang dapat diterapkan untuk melindungi infrastruktur TI. Metode yang digunakan dalam penelitian ini adalah studi literatur yang menggali teori-teori terkait dari penelitian sebelumnya, buku, artikel, dan sumber lainnya. Penelitian ini bertujuan untuk memahami berbagai ancaman siber, baik yang bersumber dari luar seperti virus, ransomware, DDoS, dan peretasan, maupun ancaman internal yang terkait dengan kebocoran data dan kesalahan manusia. Berdasarkan analisis ancaman yang ada, penelitian ini mengidentifikasi beberapa strategi mitigasi, termasuk peningkatan kemampuan deteksi ancaman, edukasi pengguna mengenai praktik keamanan siber, serta pengembangan sistem deteksi dini yang efektif. Hasil penelitian menunjukkan bahwa penguatan kontrol internal dan penerapan kerangka kerja seperti COBIT 2019, NIST

Cybersecurity, dan ISO/IEC 27001 dapat meningkatkan ketahanan organisasi terhadap ancaman yang semakin kompleks. Penelitian ini memberikan panduan praktis untuk membantu organisasi dalam meningkatkan kesadaran akan pentingnya keamanan siber serta membangun sistem yang lebih aman dan tangguh terhadap ancaman yang terus berkembang.
Keywords : Infrastruktur TI, Ancaman Siber, Keamanan Siber

PENDAHULUAN

Ar-Rahman menyatakan bahwa, Organisasi menghadapi tantangan besar dalam memastikan keamanan siber di tengah percepatan transformasi digital yang mendorong adopsi Teknologi Informasi (TI). Kelangsungan operasional dan integritas data kini sangat bergantung pada kemampuan infrastruktur TI untuk melawan ancaman siber yang terus meningkat. Tantangan ini menunjukkan bahwa pemahaman mendalam tentang strategi dan teknik terkini untuk melindungi aset digital sangat penting. Ini terlepas dari fakta bahwa teknologi keamanan telah mengalami banyak kemajuan[1].

Seiring dengan pesatnya perkembangan teknologi informasi, infrastruktur teknologi informasi (TI) menjadi komponen vital bagi organisasi dalam menunjang aktivitas bisnis dan operasional. Infrastruktur TI yang kuat memberikan kemudahan pengelolaan data secara efisien serta memungkinkan organisasi mencapai produktivitas yang optimal. Namun, seiring dengan kemajuan teknologi, risiko terhadap keamanan informasi juga meningkat secara signifikan. Ancaman seperti kebocoran data, serangan siber, hingga kerentanan teknis telah menjadi tantangan utama yang dapat mengancam keberlangsungan operasional organisasi.

Keamanan siber (cybersecurity) muncul sebagai solusi untuk melindungi sistem TI, data, serta jaringan dari ancaman siber yang semakin kompleks. National Institute of Standards and Technology (NIST) mendefinisikan keamanan siber sebagai rangkaian teknik, kebijakan, dan praktik untuk melindungi informasi digital dari risiko pencurian, kerusakan, atau gangguan. Berbagai upaya seperti penerapan framework COBIT, ISO/IEC 27001, hingga pendekatan berbasis NIST telah digunakan untuk memperkuat keamanan siber dan mengelola risiko terkait ancaman siber.

Ancaman terhadap infrastruktur TI dapat dikategorikan menjadi ancaman fisik, manusia, dan teknis. Ancaman fisik mencakup kerusakan perangkat keras dan kebakaran, sedangkan ancaman manusia, seperti insider threat dan phishing, seringkali melibatkan kelalaian atau tindakan disengaja oleh individu dalam organisasi. Di sisi lain, ancaman teknis seperti malware, ransomware, hingga serangan Distributed Denial of Service (DDoS) terus menjadi tantangan signifikan dalam dunia maya.

Penelitian ini bertujuan untuk memberikan analisis komprehensif terhadap ancaman siber serta solusi yang dapat diterapkan untuk melindungi infrastruktur TI. Melalui kajian literatur dan studi kasus, penelitian ini juga diharapkan dapat memberikan panduan bagi organisasi dalam meningkatkan kapabilitas keamanan siber serta menciptakan sistem yang lebih tangguh terhadap serangan di masa depan.

KAJIAN TEORITIS

Infrastruktur TI

Meskipun efisiensi dan produktivitas telah meningkat, perusahaan masih menghadapi ancaman keamanan yang dapat membahayakan keberlangsungan bisnis. Infrastruktur TI menjelaskan keberagaman dan keselarasan komponen TI yang diperlukan untuk mendukung aplikasi bisnis. Seiring dengan pesatnya perkembangan teknologi Internet, akses ke alat peretasan canggih menjadi lebih mudah. Selain itu, kebocoran informasi semakin sering menyerang individu dan organisasi. Selain memungkinkan pengumpulan data yang tepat dan akurat serta memfasilitasi berbagi data secara efisien, penggunaan berbagai teknologi juga menyediakan platform yang terintegrasi untuk pengelolaan data dan proses yang umum.[2].

Keamanan Siber

Cybersecurity, juga dikenal sebagai keamanan siber, adalah istilah yang berasal dari dua kata: "cyber", yang merujuk pada dunia maya atau internet, dan "security", yang berarti keamanan. Akibatnya, istilah "cybersecurity" secara sederhana berarti keamanan dunia maya. Menurut L. Siagian (2018), keamanan siber bertujuan untuk mencegah dan memperbaiki ancaman siber (cyber threats) dan serangan siber (cyber attacks). Selain itu, keamanan siber juga mencakup perlindungan seluruh bagian sistem siber, seperti infrastruktur, perangkat keras, data, dan perangkat lunak, agar terlindung dari ancaman yang dapat mengancam keamanannya.

Proses yang dilakukan untuk melindungi sistem komputer, data, dan jaringan dari serangan dunia maya disebut keamanan siber. National Institute of Standards and Technology (NIST) mendefinisikan keamanan siber sebagai kumpulan teknik, kebijakan, dan praktik yang bertujuan melindungi informasi digital dari risiko pencurian, kerusakan, atau gangguan. Di Indonesia, ancaman siber terhadap sektor penting seperti pemerintahan, perbankan, dan kesehatan semakin meningkat. Menurut laporan Badan Siber dan Sandi Negara (BSSN), serangan siber di Indonesia tidak hanya berpotensi menimbulkan kerugian finansial tetapi juga dapat mengancam keamanan data pribadi dan negara[3]

Analisis dan Peningkatan Keamanan Siber

Menurut Handrini Ardiyanti(2014), Studi kasus yang berfokus pada ancaman dan solusi dalam lingkungan digital memberikan wawasan praktis mengenai serangan siber yang telah terjadi beserta langkah-langkah mitigasinya. Analisis terhadap berbagai kasus serangan siber dapat memberikan pemahaman yang komprehensif terkait taktik serta strategi yang berhasil diterapkan untuk menghadapi ancaman tersebut. Hasil dari studi ini dapat menawarkan solusi perbaikan yang efektif, seperti peningkatan kapabilitas deteksi ancaman, edukasi pengguna tentang praktik keamanan siber, dan pengembangan sistem deteksi dini yang lebih tangguh untuk memperkuat perlindungan terhadap serangan di masa depan[4].

Studi kasus tentang ancaman dan solusi dalam lingkungan digital memberikan wawasan praktis tentang serangan yang telah terjadi dan tindakan yang diambil untuk menanganinya. Studi kasus tentang serangan siber dapat dianalisis dalam penelitian ini untuk memberikan gambaran yang komprehensif tentang taktik dan strategi yang berhasil dalam memerangi serangan siber. Peningkatan kesadaran pengguna tentang praktik keamanan, upaya yang lebih besar untuk mendeteksi ancaman, dan pengembangan sistem deteksi dini yang lebih kuat adalah beberapa contoh perbaikan yang dapat dilakukan.

Kesadaran Keamanan Siber

Kesadaran keamanan siber (*cybersecurity awareness*) dapat didefinisikan sebagai pemahaman atau kemampuan individu dalam menerapkan praktik keamanan saat menggunakan situs jejaring internet. Selain itu, kesadaran ini juga mencakup pemahaman tentang pentingnya melindungi data pribadi maupun data organisasi ketika memutuskan untuk mengakses atau menggunakan platform jejaring internet[5].

METODE PENELITIAN

Studi literatur dilakukan dengan menelusuri dan mempelajari teori-teori yang relevan dari penelitian sebelumnya dalam jenis ini atau dari sumber lainnya, seperti buku, jurnal, dan buku elektronik. Langkah ini bertujuan untuk mendukung penelitian, sekaligus memahami teknik dan metode yang akan diterapkan dalam pengumpulan, pengolahan data, serta penyelesaian masalah yang diteliti[6]

Langkah awal dalam metode ini melibatkan identifikasi literatur yang relevan untuk mendapatkan pemahaman mendalam tentang konsep keamanan siber, ancaman yang dihadapi, serta strategi mitigasi yang telah diterapkan.

Tujuan utama dari metode ini adalah untuk memberikan landasan teoritis yang kuat dalam merancang pendekatan dan strategi keamanan siber yang lebih efektif. Selain itu, kajian literatur ini diharapkan dapat menjadi acuan bagi pengambilan keputusan terkait kebijakan keamanan informasi di masa depan.

HASIL DAN PEMBAHASAN

Ancaman Siber Secara Umum

Untuk melindungi infrastruktur teknologi informasi dari bahaya yang terus berkembang, ancaman *cybersecurity* adalah kompleks. Ini adalah bahaya yang dapat datang dari dalam dan luar organisasi. Untuk memberikan gambaran yang lebih lengkap, bahaya tersebut dapat dikategorikan ke dalam tiga kategori utama.[7].

Ancaman Fisik

Dalam menghadapi ancaman fisik terhadap infrastruktur TI, diperlukan pendekatan menyeluruh yang mencakup tindakan pencegahan, deteksi, dan respons cepat. Organisasi dapat mengurangi risiko, melindungi perangkat keras, dan memastikan keberlangsungan layanan TI yang penting dengan menerapkan strategi keamanan fisik yang terencana. Selain itu, penting untuk secara rutin mengubah strategi keamanan fisik sesuai dengan perkembangan teknologi dan ancaman baru.[1].

Ancaman fisik mencakup tindakan pencurian atau kerusakan terhadap perangkat keras, *server*, atau infrastruktur fisik milik organisasi. Jenis serangan ini dapat menyebabkan kehilangan atau kerusakan data dalam jumlah besar[8]. Meskipun ancaman ini tidak selalu berkaitan langsung dengan serangan siber, dampaknya terhadap ketersediaan informasi bisa sangat serius, terutama bagi organisasi yang sangat bergantung pada data dalam menjalankan operasionalnya.

Ancaman fisik dapat diminimalkan melalui implementasi kontrol lingkungan, seperti pemasangan sistem pemadam kebakaran dan penerapan backup data di lokasi geografis yang berbeda. Sementara itu, ancaman teknis membutuhkan strategi yang lebih kompleks, seperti penggunaan *firewall*, sistem deteksi intrusi (IDS), serta penerapan enkripsi data yang andal untuk melindungi informasi sensitif[9]

Ancaman Manusia

Ancaman manusia, yang sering disebut sebagai insider *threat*, mencakup risiko yang ditimbulkan oleh perilaku individu dalam organisasi, baik akibat kelalaian, kesalahan, maupun

tindakan yang disengaja. Ancaman ini sering dianggap lebih berbahaya daripada ancaman teknis, karena individu yang memiliki akses ke sistem dapat melewati kontrol keamanan yang ada. Sebagai contoh, seorang karyawan yang tanpa sengaja membuka lampiran email berisi *phishing* dapat memungkinkan malware menyusup ke jaringan organisasi, sehingga berpotensi mengakibatkan kebocoran data. Sementara itu, pada ancaman yang disengaja, karyawan dengan akses tinggi dapat memanfaatkan hak istimewanya untuk memanipulasi data atau mencuri informasi sensitif demi keuntungan pribadi atau tindakan balas dendam. Untuk memitigasi ancaman ini, organisasi disarankan menerapkan pendekatan keamanan berbasis *Zero Trust*, yang mengharuskan verifikasi identitas secara berkelanjutan, serta menerapkan prinsip least privilege untuk membatasi hak akses sesuai kebutuhan operasional[9].

Ancaman Teknis

Ancaman teknis adalah jenis ancaman yang paling umum dikaitkan dengan serangan siber. Ancaman ini mencakup serangan yang memanfaatkan metode digital untuk mengeksploitasi kerentanan pada perangkat lunak, sistem operasi, atau jaringan[9].

Malware

- *Virus*

Virus adalah jenis *malware* yang menempel pada program atau file lain dan membutuhkan interaksi pengguna untuk menyebar ke sistem lain. *Virus* dapat menyebabkan berbagai kerusakan, seperti menghapus data, merusak sistem operasi, atau mencuri data sensitif. "*Brain*" adalah *virus* komputer pertama yang dikenal yang muncul pada tahun 1986 dan menyebar melalui *floppy disk*[9].

- *Worm*

Worm adalah jenis *malware* yang dapat menyebar secara otomatis menggunakan kerentanan jaringan dan seringkali menyebabkan penggunaan bandwidth yang tinggi dan mengganggu operasional jaringan.

- *Trojan*

Trojan Horse, atau yang lebih dikenal dengan sebutan *Trojan*, adalah jenis perangkat lunak berbahaya (*malware*) yang dirancang untuk merusak sistem jaringan dengan cara menyamar sebagai program yang tampak sah atau tidak berbahaya[9].

Ransomware

Salah satu jenis malware yang menjadi ancaman yang semakin serius dalam beberapa tahun terakhir adalah ransomware. Serangan ini mengenkripsi data sistem korban dan meminta

tebusan, biasanya dalam bentuk mata uang kripto, untuk memulihkan data. Ransomware biasanya menyebar melalui email dengan lampiran berbahaya atau dengan menggunakan celah keamanan dalam perangkat lunak. Korban, termasuk pelanggan atau lembaga seperti bank syariah, mungkin harus membayar tebusan untuk mendapatkan kunci dekripsi setelah data berhasil dienkripsi. Serangan ransomware ini dapat mengganggu operasi bank syariah dan menyebabkan kerugian besar.[10].

- Infeksi awal

  Ransomware biasanya memasuki sistem melalui lampiran email phishing, situs web yang terinfeksi, atau exploit kit.

- Enkripsi data

  Enkripsi adalah teknik yang sering digunakan dalam komunikasi digital, seperti email, transaksi keuangan, dan penyimpanan data, untuk mencegah pihak yang tidak berwenang mengakses data yang tidak diinginkan dengan mengubah data atau informasi menjadi format yang tidak dapat dibaca atau dipahami tanpa kunci tertentu.

- Pemulihan data

  Mengelola sistem cadangan data secara rutin dan memastikan bahwa rencana pemulihan data berjalan sesuai dengan kebijakan yang telah ditetapkan oleh organisasi.

Phising

Teknik phishing adalah metode yang digunakan untuk mencuri informasi sensitif dengan menyamar sebagai pihak yang dapat dipercaya. Serangan ini biasanya dilakukan melalui email atau situs web palsu yang dirancang menyerupai platform resmi. *Phishing* sering melibatkan permintaan agar korban memberikan data seperti kata sandi, informasi keuangan, atau detail pribadi lainnya. Taktik ini sering kali memanfaatkan manipulasi psikologis untuk meyakinkan pengguna agar tanpa sadar menyerahkan informasi penting mereka[11].

Social Engineering

(Dikutip dari Suherman, 2017)Terdapat berbagai contoh kasus kejahatan siber, salah satunya adalah serangan yang memanfaatkan teknik *social engineering*[12]. Teknik ini melibatkan manipulasi psikologis untuk mengelabui individu agar memberikan informasi sensitif, seperti kata sandi, data keuangan, atau akses ke sistem tertentu. *Social engineering* sering digunakan karena cenderung mengeksploitasi kelemahan manusia, bukan kelemahan teknis, sehingga menjadi salah satu bentuk serangan yang paling sulit diantisipasi.

Indrajit (2017) menyatakan bahwa, Social engineering adalah sebuah metode untuk memperoleh data maupun informasi penting dari seseorang dengan memanfaatkan pendekatan yang melibatkan interaksi sosial secara langsung atau tidak langsung[12]. Salah satu target utama dari social engineering adalah pengguna aktif media sosial. Remaja, khususnya, cenderung memiliki sifat terbuka karena dorongan untuk tetap eksis dengan mengunggah berbagai aktivitas mereka dalam bentuk foto, video, atau tulisan. Unggahan tersebut sering kali mengandung informasi pribadi yang dapat menempatkan mereka dalam situasi berisiko, termasuk potensi hilangnya privasi dan ancaman terhadap keamanan data pribadi[13].

Distribution Denial of Servis (DDoS)

Serangan DDoS (*Distributed Denial of Service*) merupakan salah satu ancaman paling signifikan dalam keamanan siber saat ini. Serangan ini menggunakan jaringan komputer yang tersebar secara geografis untuk mengirimkan lalu lintas data dalam jumlah besar secara bersamaan ke target tertentu, dengan tujuan mengganggu atau menghentikan layanan yang disediakan oleh target tersebut. Teknik ini mengeksploitasi kelemahan infrastruktur jaringan, seperti keterbatasan bandwidth atau sumber daya komputasi, dengan membanjiri target menggunakan permintaan lalu lintas yang melebihi kapasitas normal. Kemajuan teknologi telah semakin memperumit dan memperparah dampak serangan DDoS ini[14]. Serangan *Distributed Denial of Service* (DDoS) tidak hanya menimbulkan tantangan teknis tetapi juga dapat berdampak signifikan secara finansial bagi korbannya. *Downtime* yang tak terduga pada layanan sering kali menyebabkan kerugian besar bagi perusahaan, termasuk penurunan reputasi dan hilangnya kepercayaan pelanggan. Untuk mengatasi ancaman ini, industri keamanan siber terus mengembangkan teknologi dan strategi mitigasi yang lebih efektif. Upaya tersebut mencakup penerapan sistem deteksi dini yang lebih canggih, pendekatan inovatif untuk mengelola lalu lintas serangan, serta pemanfaatan layanan perlindungan DDoS yang disediakan oleh penyedia keamanan atau *Content Delivery Network* (CDN)[15].

Hacking

Hacking merupakan salah satu ancaman signifikan di dunia e-*commerce*, di mana individu atau kelompok mencoba mengakses sistem, data, atau jaringan secara ilegal untuk mendapatkan informasi atau merusak fungsionalitas. Platform *e-commerce* sangat rentan terhadap serangan ini karena volume transaksi yang besar dan data pelanggan yang sensitif, termasuk informasi pembayaran dan data pribadi, yang menarik bagi para peretas[16].

Ancaman Organisasi dan Dampaknya

Meskipun 5G menawarkan kecepatan data dan kapasitas yang lebih tinggi, teknologi ini juga membawa risiko keamanan siber yang kompleks. Namun, ancaman terhadap organisasi di Indonesia mencakup kebocoran data dan informasi diplomatik akibat spionase siber. Keadaan hukum yang mengatur keamanan dan pertahanan siber menjadi tantangan besar, ditambah dengan ancaman serangan hacktivism, kejahatan siber, dan dampak negatif terhadap pertumbuhan ekonomi. Sementara perang informasi melalui berita bohong, cyberbullying, dan ujaran kebencian semakin meningkat, kesadaran akan pentingnya keamanan siber semakin menurun. Selain itu, adopsi teknologi oleh masyarakat 5.0 dapat menimbulkan risiko baru ketika teknologi informasi dan komunikasi (TIK) digunakan untuk pelanggaran hukum.

Strategi dalam Menghadapi Tantangan keamanan Siber

Penerapan Cobit 2019

Sebuah penelitian yang dilakukan oleh Chrisandy Arya Frammy Haullussy pada tahun 2019 menunjukkan bahwa Framework COBIT (Control Objectives for Information and Related Technologies) adalah metode yang berguna untuk mengelola dan melindungi teknologi informasi (TI). Tiga komponen utama digariskan dalam framework ini: manajemen risiko, pengendalian internal, dan evaluasi kinerja. Penelitian COBIT memberikan wawasan mendalam tentang bagaimana organisasi dapat mengidentifikasi, mengevaluasi, dan mengelola risiko terkait keamanan siber secara sistematis. Selain itu, COBIT memberikan pedoman untuk menerapkan pengendalian internal untuk meminimalkan risiko dan melindungi aset TI. Penekanan pada pengukuran kinerja juga menekankan pentingnya memastikan bahwa strategi keamanan yang diterapkan mampu mencapai hasil yang diharapkan. Oleh karena itu, Framework COBIT sebagai dasar teoretis memberikan dasar yang kokoh untuk meningkatkan dan memperkuat keamanan siber perusahaan[18].

NIST Cybersecurity

Menurut penelitian yang dilakukan oleh Vicky Mahendra pada tahun 2023, ada banyak keuntungan yang ditawarkan oleh manajemen risiko keamanan siber di Kementerian PUPR. Pertama, Kerangka Kerja Keamanan Siber NIST menggunakan pendekatan holistik, yang mencakup tahap Identify, Protect, Detect, dan Respond, yang memberikan wawasan yang menyeluruh tentang elemen keamanan, membantu organisasi untuk menemukan, melindungi, mendeteksi, dan menanggapi ancaman siber. Penelitian ini juga mengevaluasi perbedaan antara kondisi saat ini dan yang diinginkan, dan menawarkan pedoman praktis bagi Kementerian PUPR untuk meningkatkan kematangan keamanan siber pada tingkat aplikasi[19].

ISO/IEC 27001

Menguraikan kontrol yang tersedia untuk organisasi untuk mencapai tujuan kontrol, menjelaskan berbagai contoh penerapan keamanan informasi. Semua kontrol yang disebutkan di atas termasuk empat belas area klausul kontrol yang ditemukan dalam ISO/IEC 27001. *ISO/IEC 27001* menyediakan struktur yang terorganisir untuk memastikan bahwa organisasi dapat mengimplementasikan langkah-langkah yang tepat dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi yang dikelola[20].

Dengan mengadopsi *framework ISO 27001*, lembaga pemerintahan dapat melakukan penilaian terhadap risiko keamanan informasi dengan memberikan kategori dan peringkat level, sehingga memudahkan identifikasi area yang perlu diperbaiki, dievaluasi, dan ditingkatkan. Pendekatan ini sangat sistematis karena lembaga pemerintahan mengikuti kebijakan dan prosedur yang sesuai dengan standar ISO 27001, yang memberikan panduan formal untuk mengelola keamanan informasi. Sebelum menggunakan *framework* ISO 27001, penerapan manajemen risiko dengan standar sebelumnya bisa berisiko dan berpotensi mengarah pada kebocoran informasi penting. Dengan ISO 27001, setiap aspek memiliki standar yang jelas dan disesuaikan dengan kontrol yang dibutuhkan oleh lembaga[21].

KESIMPULAN

Penelitian ini mengidentifikasi berbagai bahaya di dunia maya yang berpotensi merusak infrastruktur teknologi informasi dan mengganggu kelangsungan operasional suatu organisasi. Ancaman tersebut, seperti serangan *DDoS*, *ransomware*, *phishing*, *Distribution Denial of Servis (DDoS), Social Engineering*, dan *Hacking* menjadi semakin rumit seiring dengan kemajuan teknologi yang sangat cepat. Organisasi harus mengembangkan rencana yang lebih baik untuk menghadapi ancaman tersebut, dengan meningkatkan kemampuan dalam mendeteksi ancaman serta memberikan edukasi kepada pengguna tentang pentingnya praktik keamanan siber.

Berdasarkan analisis yang telah dilakukan, disarankan kepada organisasi untuk menerapkan sistem deteksi yang efektif dan mengadopsi berbagai kerangka kerja yang telah terbukti berhasil, seperti COBIT, *NIST Cybersecurity Framework*, dan ISO/IEC 27001, guna meningkatkan ketahanan terhadap serangan. Penelitian ini juga menekankan pentingnya meningkatkan kesadaran mengenai keamanan siber di semua level organisasi sebagai langkah proaktif untuk menjaga data dan aset penting. Dengan mengimplementasikan kebijakan

keamanan yang lebih kuat serta strategi mitigasi yang lebih canggih, organisasi dapat memperkokoh perlindungan terhadap infrastruktur TI dan mengurangi risiko kerugian akibat ancaman di dunia maya.

REFERENSI

M. O. Hoshmand, S. Ratnawati, and E. P. Korespondensi, "Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity," *J. Sains dan Teknol.*, vol. 5, no. 2, pp. 679–686, 2023, [Online]. Available: https://doi.org/10.55338/saintek.v5i2.2347

S. Kim, B. Kim, and M. Seo, "Impacts of sustainable information technology capabilities on information security assimilation: The moderating effects of policy-technology balance," *Sustain.*, vol. 12, no. 15, 2020, doi: 10.3390/su12156139.

P. A. Khairunnisa, N. Annisa, and Y. J. Parhusip, "Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI : Studi Kasus di Indonesia," vol. 4, pp. 9–16, 2024.

Chintya Pradilla Putri, Widya Anggraini, Yuda Mahendra Hasibuan, and N. Nurbaiti, "Strategi Pengamanan Cyber: Lingkup Kerjasama dalam Menghadapi Ancaman Cyber," *INSOLOGI J. Sains dan Teknol.*, vol. 2, no. 6, pp. 1124–1130, 2023, doi: 10.55123/insologi.v2i6.2847.

I. A. Afandi, A. Kusyanti, and N. H. Wardani, "Analisis Hubungan Kesadaran Keamanan , Privasi Informasi , Perilaku Keamanan Pada Para Pengguna Media Sosial Line," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 9, pp. 783–792, 2017.

F. Ahdi Anshori, Suprapto, and A. Reza Perdanakusuma, "Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 2, pp. 1701–1707, 2019, [Online]. Available: http://j-ptiik.ub.ac.id

V. A. Kairupan and A. A. Rahman, "Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Kalangan Mahasiswa Kota Bandung," *J. Darma Agung*, vol. 30, no. 1, p. 1164, 2022, doi: 10.46930/ojsuda.v30i1.3167.

L. Adi Saputra, F. Muhammad Akbar, F. Cahyaningtias, M. Puspa Ningrum, and A. Fauzi, "Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan," *J. Pendidik. Siber Nusant.*, vol. 1, no. 2, pp. 58–66, 2023, doi: 10.38035/jpsn.v1i2.48.

M. A. Helmiawan, Y. H. Akbar, and F. Mahardika, "Keamanan Teknologi Informasi Teori, risiko, dan strategi pertahanan di era digital," p. 6, 2024.

M. A. Faizal, Z. Faizatul, B. N. Asiyah, and R. Subagyo, "Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman Dan Tantangan Terkini," *J. Asy-Syarikah J. Lemb. Keuangan, Ekon. dan Bisnis Islam*, vol. 5, no. 2, pp. 87–100, 2023, doi: 10.47435/asy-syarikah.v5i2.2022.

M. O. Hoshmand, S. Ratnawati, and E. P. Korespondensi, "Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity," *Appl. Inf. Technol.*

Comput. Sci., vol. 5, no. 2, pp. 679–686, 2023, [Online]. Available: https://doi.org/10.55338/saintek.v5i2.2347

Y. Hartiwi, Y. Arvita, M. Purnasari, and Nurhayati, "Sosialisasi Edukasi Bahaya dan Upaya Pencegahan Social Engineering Untuk Meningkatkan Keamanan Informasi," *J. Pengabdi. Masy. UNAMA*, vol. 3, no. 1, pp. 65–72, 2024.

E. W. Tyas Darmaningrat *et al.*, "Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi," *Sewagati*, vol. 6, no. 2, 2022, doi: 10.12962/j26139960.v6i2.92.

V. Puspitasari, M. Z. Abdillah, M. A. Alfa, D. Steyer, and S. N. Neyman, "Deteksi dan Respons Terhadap Ddos Attacks pada Website Dinamis," *J. Ilmu Tek.*, vol. 1, no. 4, pp. 18–25, 2024, [Online]. Available: https://doi.org/10.62017/tektonik

R. Rahman and G. R. . Odja, "Analisis dan Pencegahan Serangan DDoS Pada Jaringan Skala Besar," vol. d, pp. 0–3, 2024.

A. Nur and D. A. Hafid, "PERANAN IT SECURITY DALAM MENGAMANKAN INFRASTRUKTUR DAN TRANSAKSI DI PERUSAHAAN E-COMMERCE Aryanto," vol. 4, no. 10, pp. 1–20, 2024.

Y. Ginanjar, "Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara," *J. Din. Glob.*, vol. 7, no. 02, pp. 291–312, 2022, doi: 10.36859/jdg.v7i02.1187.

C. A. F. Haullussy, "Audit Sistem Informasi Pelayanan Menggunakan Framework Cobit 4.1 (Studi Kasus di Dinas Perpustakaan dan Kearsipan Kota Salatiga)," vol. 1, pp. 1–23, 2019.

T. Tan and B. Soewito, "Manajemen Risiko Serangan SiberMenggunakan Framework NistCybersecurity Di Universitas Zxc," *J. Inf. Syst. Applied, Manag. Account. Res.*, vol. 6, no. 2, pp. 411–422, 2022, doi: 10.52362/jisamar.v6i2.781.

T. S. Putri, N. M. Mutiah, and D. P. Prawira, "ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN NIST CYBERSECURITY FRAMEWORK DAN ISO/IEC 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat)," *Coding J. Komput. dan Apl.*, vol. 10, no. 02, p. 237, 2022, doi: 10.26418/coding.v10i02.54972.

B. Aurabillah, L. Aprillia Putri, N. Citra Fadhlilla, and A. Wulansari, "Implementasi Framework Iso 27001 Sebagai Proteksi Keamanan Informasi Dalam Pemerintahan (Systematic Literature Review)," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 1, pp. 454–460, 2024, doi: 10.36040/jati.v8i1.8736.