Jurnal Ilmiah Wahana Pendidikan, Desember 2024, 10 (23), 1157-1165
DOI: https://jurnal.peneliti.net/index.php/JIWP/article/view/9175
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

Keamanan Cyber Dalam Sistem Informasi Manajemen: Ancaman dan Solusi Terbaru

Agung Wijoyo[1], Bentar Abdillah[2], Fathurrahman Khalbi[3], Reza Adi Saputra[4], Wafiatul Khoiriyah[5]

Teknik Informatika, Universitas Pamulang

Received: 8 Oktober 2024
Revised: 22 Oktober 2024
Accepted: 6 November 2024

Abstract

In today's digital age, cybersecurity management information systems (SIMs) are getting more and more attention. In this article, we discuss major issues facing SIM cyber security, such as malware attacks, phishing, data hacking, and data information leaks, along with the latest solutions that can be applied to address these problems. Qualitative research methods are used to gain a better understanding of cyber security issues. The research focuses on the experience and perspectives of cyber security experts, SIM managers, and related practitioners. Research shows that to combat increasingly complex cyber threats in SIMs, careful security policies, making advanced security technologies, user training and awareness, active control of suspicious actions, and improved inter-agency cooperation are important measures.

Keywords: *Cyber Threats, Cyber Security, Management Information Systems*

(*) Corresponding Author: dosen01671@unpam.ac.id[1],bentar375@gmail.com[2], FathurrahmanKhalbi@gmail.com[3], rezaadi2040@gmail.com[4], www.wafiatulkhoiriyah@gmail.com[5]

How to Cite: Wijoyo, A., Abdillah, B., Khalbi, F., Saputra, R., & Khoiriyah, W. (2024). Keamanan Cyber Dalam Sistem Informasi Manajemen: Ancaman dan Solusi Terbaru. *Jurnal Ilmiah Wahana Pendidikan*, *10*(23), 1157-1165. Retrieved from https://jurnal.peneliti.net/index.php/JIWP/article/view/9175

PENDAHULUAN

Dalam era digital saat ini, keamanan cyber sistem informasi manajemen (SIM) menjadi semakin penting dan mendesak. Hal ini disebabkan oleh kemajuan dalam teknologi informasi dan komunikasi. Organisasi di berbagai industri bergantung pada SIM untuk melakukan tugas sehari-hari mereka, seperti manajemen data dan pengambilan keputusan strategis. (Suparjono, 2019).

Seiring dengan manfaat Sistem Informasi Manajemen (SIM), ada masalah keamanan cyber. Pengelola SIM dan organisasi yang mengandalkannya sangat khawatir tentang ancaman seperti serangan malware, phishing, peretasan data, dan kebocoran informasi. (Gloria, 2019).

Ada masalah keamanan cyber seiring dengan keuntungan Sistem Informasi Manajemen (SIM). Pelaksana SIM dan organisasi yang mempercayakannya sangat begitu khawatir tentang serangan tertuju kepada malware, phishing, peretasan informasi data, dan kebocoran informasi data.

Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mencuri data dari sistem data informasi. ada beberapa jenis malware ini yang termasuk kedalam virus, worm, trojan, dan ransomware, dan penyebab masalah utamanya adalah kemampuannya untuk merembet dengan cepat dan merusaki sistem, bahkan menyebabkan kecelakaan finansial atau kehilangan data yang signifikan. (Gloria, 2019).

Phishing merupakan salah satu serangan di mana pelaku berpura-pura menjadi

orang yang dipercaya untuk mendapatkan informasi data pribadi seperti sandi, nomor bank, atau informasi data password lainnya. Phishing dapat menipu orang dengan tautan atau pesan palsu yang terlihat meyakinkan, yang merupakan tantangan utamanya. Organisasi harus memberikan penataran akan kesadaran keamanan pada karyawan mereka untuk mengingat dan menghindari serangan dari phishing serta memanfaatkan teknologi anti-phishing yang dapat mengetahui dan memblokir cara dari phishing. (Koran Jakarta, 2019).

Serangan peretasan data terjadi ketika peretas memasuki sistem dan mengambil data sensitif atau vital organisasi. Peretasan data dapat membahayakan reputasi perusahaan, kehilangan harapan pelanggan, dan masalah hukum dan finansial. Organisasi harus mempergunakan lapisan keamanan yang kuat, contoh enkripsi data, kontrol akses, dan penemuan intrusi yang canggih, untuk mengatasi masalah ini.

Terdapat berbagai kebocoran informasi data terjadi dikarenakan kecerobohan internal, sebaran eksternal, atau kesalahan susuna sistem yang memungkinkan orang lain mengakses data sensitif. Cara agar mengamankan informasi rahasia organisasi, seperti desain produk, data pelanggan, atau rencana bisnis, sangat sulit. Kebocoran informasi ini dapat membahayakan keunggulan kompetitif dan kepercayaan masyarakat. Untuk mencegah kebocoran data, organisasi harus menerapkan prosedur keamanan yang ketat, melaksanakan keakuratan keamanan teratur, dan meningkatkan kontrol akses.

Organisasi harus secara proaktif mengidentifikasi ancaman yang dapat mengganggu integritas, kerahasiaan, dan ketersediaan data dalam Sistem Informasi Manajemen (SIM) agar lebih efektif dan aman. Mereka juga harus membuat dan menerapkan rencana keamanan yang tepat, yang mencakup teknologi canggih, kebijakan yang jelas, pelatihan karyawan, dan pengawasan yang ketat. Dengan menggunakan metode yang komprehensif dan terus-menerus, organisasi dapat meminimalkan risiko kebocoran data, serangan siber, atau gangguan lainnya. Ini memastikan integritas, kerahasiaan, dan ketersediaan informasi yang sangat penting untuk operasi lancar organisasi.

Organisasi harus menerapkan strategi keamanan cyber yang holistik untuk mengatasi masalah ini. Ini mencakup penerapan teknologi keamanan yang canggih seperti pada firewall, antivirus, dan sistem deteksi bahaya kelanjutan (Advanced Threat Detection), serta pelaksanaan kebijakan keamanan yang ketat dan pengamat aktif terhadap aksi yang mencurigakan. Pelatihan dan pendidikan tentang keamanan cyber untuk pengguna SIM juga penting untuk meningkatkan kesadaran dan kewaspadaan terhadap serangan cyber yang semakin kompleks. Dengan menggabungkan semua langkah ini, organisasi dapat menambahkan pertahanan mereka terhadap serangan keamanan cyber dan melindungi SIM dan data yang dikelola. (Karyoto, 2019).

Untuk melindungi integritas, kerahasiaan, dan ketersediaan data dalam SIM, penelitian dan inovasi dalam bidang keamanan cyber menjadi sangat penting karena masalah keamanan cyber dalam SIM tidak hanya bersifat teknis tetapi juga mencakup elemen kebijakan dan manajemen risiko.

METODE PENELITIAN

Tujuan dari penelitian ini adalah untuk mendapatkan pemahaman yang lebih mendalam tentang masalah keamanan cyber dalam sistem informasi manajemen (SIM). Untuk mencapai tujuan ini, studi kasus ini berfokus pada organisasi atau antar lembaga yang memiliki banyak pengalaman dalam mengelola keamanan cyber SIM.

Para peserta penelitian terdiri dari ahli keamanan cyber, manajer SIM, dan praktisi terkait dari berbagai organisasi atau antar lembaga. Penelitian ini mengumpulkan data melalui pengamtan langsung, tanya jawab mendalam, dan analisis dokumen seperti kebijakan keamanan, keterangan insiden keamanan, dan salinan data terkait lainnya untuk mendapatkan pemahaman yang luas tentang situasi.

Wawancara mendalam akan digunakan dalam penelitian ini untuk mendapatkan pemahaman langsung dari responden tentang subjek yang diteliti. Tanya jawab akan dilakukan dengan menggunakan pertanyaan yang terstruktur dan terbuka sehingga responden dapat memberikan jawaban yang mendalam dan mendalam. Setelah tanya jawab selesai, data akan diselidiki secara tematis untuk menemukan pola dan hasil penting yang berkaitan dengan tujuan penelitian.

Pengamatan secara langsung akan dilakukan untuk memperoleh pengertian langsung tentang situasi atau petunjuk yang diamati. Sebagai contoh, pengamatan langsung tentang penerapan kebijakan keamanan di lingkungan kerja mungkin dilakukan dalam penelitian ini. Peneliti akan mencatat semua pengamatan, perilaku, dan interaksi yang terjadi sambil memperhatikan faktor lingkungan dan konteks yang relevan. Mereka akan menganalisis data dari pengamatan untuk menemukan pola perilaku, kecenderungan, dan kemungkinan masalah yang perlu diteliti lebih lanjut dalam konteks penelitian keamanan.

Bagian penting yang terdapat dari penelitian ini adalah analisis dokumen. Dokumen seperti kebijakan keamanan, keterangan kejadian keamanan, dan dokumen terkait lainnya akan diperiksa secara menyeluruh. Tujuan dari analisis ini adalah untuk mendapatkan pemahaman tentang kerangka kerja keamanan saat ini, kebijakan yang berlaku, praktik keamanan yang diterapkan, dan catatan laporan insiden yang relevan.

Dengan menggunakan gabungan metode ini, penelitian diharapkan akan menghasilkan pemahaman yang mendalam dan menyeluruh tentang topik keamanan yang sedang diselidiki. Informasi yang diperoleh dari analisis dokumen akan membantu mengisi kekosongan pengetahuan, memverifikasi atau menjelaskan hasil wawancara dan pengamatan, dan memberikan pemahaman yang lebih menyeluruh tentang konteks keamanan yang sedang diselidiki.

Pendekatan induktif digunakan untuk menganalisis data kualitatif yang diperoleh dari wawancara tanya jawab, pengamatan, dan penyelidikan dokumen. Ancangan ini melibatkan proses pengkodean data, identifikasi pola dan tema, dan pembentukan kerangka konseptual yang mengilustrasikan masalah dan solusi terbaru dalam keamanan cyber dalam SIM. Keabsahan internal diperoleh melalui triangulasi data, yaitu membandingkan hasil dari berbagai sumber data, sementara keabsahan eksternal diperoleh melalui penilaian rekan satu sama lain dari data.

Penelitian kualitatif ini bertujuan untuk mendapatkan pengetahuaan yang mendalam dan kontekstual tentang keamanan cyber SIM dan memberikan perspektif yang lebih mendalam tentang masalah tersebut. Hasil penelitian dapat disajikan dalam bentuk narasi mendalam yang menguraikan masalah utama dalam keamanan cyber SIM serta solusi terbaru yang telah diterapkan. Selain itu, hasil dapat disajikan dalam bentuk tabel, diagram, atau model konseptual untuk memperjelas hubungan antara masalah dan solusi tersebut.

HASIL DAN PEMBAHASAN

Hasil penelitian ini menemukan banyak hal penting tentang masalah dan solusi keamanan cyber untuk Sistem Informasi Manajemen (SIM). Berikut adalah beberapa poin penting dari temuan penelitian:

Sebagian besar orang yang menjawab mengidentifikasi serangan ransomware dan malware sebagai bahaya utama yang mengganggu keamanan cyber SIM. Serangan ini dapat membuat pengambilan data, kerusakan pada sistem, dan kerugian finansial yang besar. Serangan ransomware, di sisi lain, mengenkripsi data dan meminta tebusan untuk memperoleh kunci dekripsi. Untuk melindungi SIM dari bahaya yang ditimbulkan oleh serangan-serangan ini, keduanya menjadi fokus utama dalam strategi keamanan cyber.

Serangan phishing dan teknik social engineering mengancam keamanan informasi sensitif dalam SIM beberapa organisasi. Serangan ini menggunakan email palsu untuk menipu pengguna untuk memberikan informasi sensitif seperti kata sandi atau rincian akun. Namun, teknik sosial engineering termasuk manipulasi psikologis untuk memaksa pengguna untuk melakukan hal-hal yang menguntungkan penyerang, seperti memberikan akses tidak sah ke sistem atau data. Keduanya menekankan betapa pentingnya pengguna SIM dilatih tentang keamanan agar mereka dapat menemukan dan menghindari tindakan manipulatif ini.

Selain itu, responden menekankan bahwa kelemahan infrastruktur jaringan dan perangkat keras merupakan tantangan yang signifikan untuk memastikan keamanan cyber Sistem Informasi Manajemen (SIM). Pihak yang tidak berwenang dapat memanfaatkan kelemahan perangkat keras, seperti bug firmware atau pengaturan yang tidak aman, untuk meretas sistem. Sebaliknya, infrastruktur jaringan yang kurang terlindungi atau aktivitasnya kurang dipantau dapat meningkatkan risiko serangan dari dalam maupun dari luar. Mengatasi kelemahan ini dalam SIM berfokus pada peningkatan keamanan infrastruktur jaringan dan perangkat keras.

Organisasi yang telah menggunakan teknologi keamanan terkini, seperti sistem deteksi ancaman tingkat lanjut (Advanced Threat Detection) dan perlindungan endpoint yang kuat, untuk mengatasi masalah keamanan cyber Sistem Informasi Manajemen (SIM). Sistem deteksi ancaman tingkat lanjut memungkinkan organisasi untuk secara proaktif mengidentifikasi dan merespons serangan cyber dengan mengidentifikasi pola perilaku mencurigakan yang mungkin tidak terdeteksi oleh sistem keamanan utama. Dalam strategi keamanan cyber untuk SIM, kedua teknologi ini memberikan lapisan pertahanan penting, yang memungkinkan organisasi menghadapi ancaman yang terus berkembang dan kompleks.

Melakukan investasi dalam pelatihan keamanan cyber dan meningkatkan kesadaran pengguna sangat penting untuk mengurangi insiden seperti phishing dan *social engineering*. Pengguna memperoleh pengetahuan dan keterampilan yang diperlukan untuk mengidentifikasi dan menanggapi serangan cyber, seperti mengidentifikasi email phishing yang mencurigakan atau menghindari upaya manipulasi sosial, melalui pelatihan keamanan cyber. Selain itu, meningkatkan kesadaran pengguna tentang praktik keamanan cyber yang baik, seperti menjaga kerahasiaan data dan menggunakan kata sandi yang kuat, dapat mengurangi kemungkinan mereka menjadi korban serangan cyber. Upaya ini meningkatkan keamanan cyber SIM dan mengurangi celah yang sering dimanfaatkan oleh penyerang.

Organisasi yang berhasil mengelola keamanan cyber sistem informasi manajemen (SIM) menerapkan kebijakan keamanan yang ketat, seperti penggunaan

sandi kuat, akses terbatas, dan pengawasan aktif terhadap aktivitas mencurigakan. Kebijakan sandi kuat mencakup standar kombinasi huruf, angka, dan simbol, serta pembaruan berkala. Akses terbatas mengurangi risiko pelanggaran keamanan dengan memastikan bahwa hanya orang yang memerlukan dapat masuk. Pemantauan aktif menggunakan alat deteksi ancaman memungkinkan respons cepat terhadap serangan cyber. Kebijakan ini memungkinkan organisasi untuk meningkatkan pertahanan mereka terhadap ancaman cyber dan melindungi SIM dari serangan cyber yang mungkin terjadi.

Pengguna harus menjaga keamanan siber mereka. Organisasi harus mengalokasikan sumber daya untuk pelatihan terus menerus dan meningkatkan pengetahuan pengguna tentang praktik keamanan siber yang baik. Karena pengguna adalah sumber utama serangan siber, peran mereka dalam menjaga keamanan siber tidak boleh diabaikan. Selama aktivitas online yang tidak aman, pengguna yang ceroboh atau tidak berpengalaman mengeklik tautan phishing atau membocorkan informasi pribadi dapat menyebabkan serangan. (Prasetyo, Hoedi dan Wahyudi Sutopo, 2018)

Akibatnya, organisasi harus mengalokasikan sumber daya untuk memberikan pelatihan berkelanjutan kepada karyawan mereka. Pelatihan ini tidak hanya memberikan pengetahuan tentang ancaman cyber dan teknik serangan umum, tetapi juga mengajarkan keterampilan praktis untuk mengidentifikasi dan menanggapi serangan yang mungkin terjadi. Meningkatkan pengetahuan pengguna tentang praktik keamanan cyber yang baik, seperti menggunakan kata sandi yang kuat, menghindari mengklik tautan atau lampiran yang mencurigakan, dan melaporkan aktivitas yang mencurigakan, dapat membantu mengurangi risiko serangan cyber.

Oleh karena itu, pelatihan dan peningkatan kesadaran pengguna yang berkelanjutan merupakan bagian penting dari strategi keamanan cyber organisasi. Pemakai yang terlatih dan sadar akan risiko dapat bertindak aktif dalam menjaga SIM dan data sensitif organisasi dari serangan cyber. (Yahya, Muhammad, 2018).

Karena serangan cyber semakin canggih dan terus bertumbuh pesat, pemeliharaan teknologi keamanan canggih menjadi sangat penting untuk menghadang ancaman cyber yang semakin kompleks. Teknologi canggih seperti sistem deteksi ancaman lanjutan (Advanced Threat Detection), keamanan endpoint yang kuat, dan solusi keamanan jejaring yang terintegrasi mampu mengecek dan menjawab serangan cyber dengan lebih baik. (Librianty, Andina, 2019).

Organisasi harus terus memperbaiki dan meluaskan infrastruktur keamanan mereka untuk beradaptasi dengan perubahan teknologi dan strategi serangan cyber. Ini termasuk penerapan prosedur keamanan yang kuat, memperbarui perangkat lunak keamanan secara berkala, dan investasi dalam metode keamanan yang mampu melawan ancaman yang akan muncul.

Dengan memperbarui dan meningkatkan infrastruktur keamanan secara konsisten, organisasi dapat meningkatkan pertahanan mereka terhadap serangan cyber yang semakin maju dan kompleks karena perbaikan ini melibatkan perbaikan perangkat keras dan perangkat lunak serta pelatihan dan pengembangan tim keamanan IT untuk mengerjakan teknologi keamanan yang kompleks. (Rahmani, Aziz, 2019).

Untuk menyusut risiko serangan secara lengkap, langkah penting adalah penerapan kebijakan keamanan yang ketat dan pengawasan yang aktif terhadap ancaman cyber. Aturan keamanan yang ketat meliputi berbagai komponen, layaknya manajemen akses, penggunaan sandi yang kuat, enkripsi data, perbaharuan perangkat lunak secara berkala, dan pemilihan keamanan jaringan yang sesuai.

Pengawasan aktif terhadap ancaman cyber mengikutsertakan penggunaan sistem pemantauan dan mengecek ancaman yang dapat mendeteksi tanda-tanda serangan cyber segera setelah terjadi. Dengan memantau kegiatan jaringan dan sistem secara terus-menerus, organisasi dapat memantau serangan segera setelah terjadi dan mengambil langkah upaya mencegah atau respons yang cepat untuk meminimalkan dampaknya. (Abidin, D. Z, 2015).

pemeriksaan log keamanan, pengujian penetrasi, dan pembaruan kebijakan keamanan untuk menangani ancaman baru juga merupakan bagian dari pengawasan aktif. Dengan menerapkan metode ini, organisasi dapat meningkatkan pertahanan keamanan cyber mereka, mengurangi kemungkinan serangan, dan menjamin integritas, kerahasiaan, dan ketersediaan data dalam sistem informasi manajemen (SIM). Selain metode utama pemungutan data seperti wawancara tanya jawab mendalam, observasi langsung, dan analisis dokumen, ada beberapa metode tambahan yang dapat diambil oleh organisasi dalam hal keamanan cyber. (Dewi, R, et al, 2018).

Pemeriksaan log keamanan mengikutsertakan pengawasan dan analisis kegiatan log dari berbagai sistem dan perangkat dalam infrastruktur IT organisasi. Dengan melakukan pemeriksaan log secara berkala, tim keamanan dapat mendeteksi pola-pola yang mencurigakan atau kegiatan yang tidak biasa yang mungkin menunjukkan serangan atau pelanggaran keamanan. Dengan melakukan pemeriksaan log secara berkala, organisasi dapat melakukan penelusuran lebih lanjut, dan menjawab lebih cepat terhadap insiden keamanan.

Pemeriksaan penetrasi adalah latihan serangan keamanan yang dilakukan secara kontrol untuk mendeteksi kelemahan dan celah keamanan dalam sistem dan jaringan organisasi. Pemeriksaan penetrasi memungkinkan organisasi untuk menyadari seberapa rawan sistem mereka terhadap serangan dari luar, mencakup serangan yang bertujuan untuk mengambil data atau merusak sasaran. Hasil pemeriksaan penetrasi dapat digunakan untuk memperbarui kekurangan pada sistem dan jaringan organisasi.

Karena bahaya keamanan cyber terus berkembang, penting bagi organisasi untuk secara teratur memperbaharui aturan keamanan mereka untuk mengantisipasi bahaya baru. Rencana keamanan, pengaturan perangkat keamanan, dan pengawasan aktivitas keamanan adalah beberapa contoh perubahan atau penambahan kebijakan keamanan. Dengan menerapkan langkah-langkah ini, perusahaan dapat meningkatkan keamanan cyber mereka, mengurangi kemungkinan serangan, dan memastikan keutuhan, kerahasiaan, dan kelengkapan data dalam SIM.

Menggabungkan pengawasan aktif, analisis log keamanan, pemeriksaan penetrasi, dan pembaharuan aturan keamanan merupakan rencana penting dalam meningkatkan kekuatan sebuah organisasi terhadap bahaya keamanan cyber yang terus berkembang, serta menjaga data dan sistem informasi mereka dengan lebih baik. Berikut adalah penjelasan dan informasi lebih lanjut tentang manfaat dan penerapan pendekatan ini.

Pengawasan aktif berarti mengawasi sistem dan jaringan organisasi secara terus menerus untuk mengidentifikasi aktivitas yang meragukan atau bahaya keamanan yang sedang berlangsung. Dengan melakukan pengawasan aktif, organisasi dapat menimalkan efek serangan atau insiden keamanan dan menghentikannya secepat mungkin. Perangkat lunak pengawasan keamanan, sensor keamanan, dan analisis otomatis biasanya digunakan untuk mendeteksi ancaman potensial. (Kwarto, F., & Angsito, M, 2018).

Pemeriksaan log keamanan menjadikan organisasi untuk memiksa kegiatan yang telah terjadi dalam infrastruktur IT mereka, seperti log perangkat jaringan, server, dan aplikasi. Dengan melakukan pemeriksaan log keamanan secara teratur, organisasi dapat menemukan cara anomali atau gejala serangan yang mungkin terlupakan oleh sistem deteksi bahaya yang otomatis. Pemeriksaan log keamanan juga membantu memeriksa kepatuhan terhadap kebijakan keamanan. (Hansen, L & Nissenbaum, H, 2009).

Pemeriksaan penetrasi, yang dilakukan secara berkala, menggambarkan serangan dari luar yang disepakati secara etis. Hasil pengujian menunjukkan kerentanan sistem, jaringan, atau aplikasi yang dapat dimanfaatkan oleh penyerang dan membantu organisasi menemukan dan mengatasi celah keamanan sebelum mereka digunakan oleh penyerang. Untuk memperkuat keamanan cyber organisasi, kebijakan keamanan harus terus diperbaharui dan dicocokan dengan tren dan bahaya keamanan baru. Perubahan ini meliputi rencana keamanan yang disesuaikan, perbaikan pengawasan, perubahan dalam tata kelola akses, dan pembaharuan teknologi keamanan yang digunakan. (Islami, M. J, 2017).

Selain itu, organisasi harus memberikan pelatihan dan kesadaran keamanan kepada karyawannya sehingga mereka dapat memahami dan mematuhi kebijakan keamanan baru. Dengan menggabungkan semua langkah ini, organisasi dapat meningkatkan pertahanan cyber mereka dengan cara yang proaktif, adaptif, dan efisien. Hal ini meminimalkan dampak insiden keamanan dan membantu melindungi data dan sistem informasi mereka dari serangan. (Kalakuntla, R, et al. 2019).

Didasarkan pada temuan ini, organisasi dapat membangun program pembelajaran keamanan cyber yang komprehensif, "penanaman modal dalam teknologi keamanan yang canggih, dan pemeriksaan berkala kebijakan keamanan. Dengan cara ini, organisasi dapat meningkatkan pertahanan pertahanan mereka terhadap bahaya cyber yang terus berkembang di lingkungan SIM.

KESIMPULAN

Ada masalah keamanan cyber seiring dengan keuntungan Sistem Informasi Manajemen (SIM). Pelaksana SIM dan organisasi yang mempercayakannya sangat begitu khawatir tentang serangan tertuju kepada malware, phishing, peretasan informasi data, dan kebocoran informasi data.

Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mencuri data dari sistem data informasi. ada beberapa jenis malware ini yang termasuk kedalam virus, worm, trojan, dan ransomware, dan penyebab masalah utamanya adalah kemampuannya untuk merembet dengan cepat dan merusaki sistem, bahkan menyebabkan kecelakaan finansial atau kehilangan data yang signifikan. (Gloria, 2019).

Phishing merupakan salah satu serangan di mana pelaku berpura-pura menjadi orang yang dipercaya untuk mendapatkan informasi data pribadi seperti sandi, nomor bank, atau informasi data password lainnya. Phishing dapat menipu orang dengan tautan atau pesan palsu yang terlihat meyakinkan, yang merupakan tantangan utamanya. Organisasi harus memberikan penataran akan kesadaran keamanan pada karyawan mereka untuk mengingat dan menghindari serangan dari phishing serta memanfaatkan teknologi anti-phishing yang dapat mengetahui dan memblokir cara dari phishing. (Koran Jakarta, 2019).

Sebagian besar orang yang menjawab mengidentifikasi serangan ransomware dan malware sebagai bahaya utama yang mengganggu keamanan cyber SIM. Serangan ini dapat membuat pengambilan data, kerusakan pada sistem, dan kerugian finansial yang besar. Serangan ransomware, di sisi lain, mengenkripsi data dan meminta tebusan untuk memperoleh kunci dekripsi. Untuk melindungi SIM dari bahaya yang ditimbulkan oleh serangan-serangan ini, keduanya menjadi fokus utama dalam strategi keamanan cyber.

DAFTAR PUSTAKA

Abidin, D. Z, 2015. Kejahatan dalam Teknologi Informasi dan Komunikasi. Jurnal Ilmiah Media Processor, Vol. 10, No. 2, 509-516.

Dewi, R, et al. 2018. Pemanfaatan Internet sebagai Sumber Informasi kesehatan bagi Masyarakat. Jurnal MKK, Vol. 1, No. 2, 162-172. doi: 10.24198/mkk.vli2.18721

Dewi, S. (2011). Cybercrime dalam Abad 21: Suatu Perspektif Menurut Hukum Internasional. Jurnal MMH, Jilid 40 No. 4 , 522-530. doi:10.14710/mmh.40.4.2011.522-530

Gloria. 2019. Kesiapan Keamanan Siber Indonesia di Era Revolusi Industri 4.0 diakses dari https://www.ugm.ac.id/id/news/17376kesiapan.keamanan.siber.indonesia.di.era. revolusi.industri.40, pada tanggal 20 April 2024 pukul 10.35 WIB.

Hansen, L., & Nissenbaum, H, 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly (53) , 1155-1175. doi:10.1111/j.14682478.2009.00572.x

Islami, M. J, 2017. Tantangan dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index. Jurnal Masyarakat Telematika dan Informasi Vol 8 (2) , 137-144. doi:10.17933/mti.v812.108

Kalakuntla, R, et al. 2019. Cybersecurity. Holistica Vol. 10 Issue. 2 , 115-128. doi:10.2478/hjbpa-2019-0020

Karyoto. 2019. Ancaman Cyber Security di Era Industri 4.0 Bakal Semakin Beragam dan Masif. Diakses dari https://eksekutif.id/ancaman-cyber-security-di-era-industri-4-0-bakal-semakin-beragam-dan-masif/. Pada tanggal 20 April 2024, pukul 18.59 WIB.

Koran Jakarta. 2019. Perusahaan Mesti Punya Standar Digital Industri 4.0 diakses dari http://www.koranjakarta.com/perusahaan-mesti-punya-standar-digital-industri-4-0/ pada tanggal 19 April 2024 pukul 22.49 WIB.

Kwarto, F., & Angsito, M, 2018. Pengaruh Cyber Crime Terhadap Cyber Security Compliance di Sektor Keuangan. Jurnal Akuntansi Bisnis Vol. 11 No. 2 , 99-110. doi: http://dx.doi.org./10.30813/jab.v11i2.1382

Librianty, Andina. 2019. Ini 3 Tantangan Keamanan Siber di Industri 4.0. Diakses dari https://www.liputan6.com/tekno/read/3689405/ini-3-tantangan-keamanan-siber-di-industri-40, tanggal 20 April 2024, Pukul 18.40 WIB.

Prasetyo, Hoedi dan Wahyudi Sutopo, 2018. Industri 4.0: Telaah Klasifikasi Aspek dan Arah Perkembangan Riset. J@ti Undip: Jurnal Teknik Industri, Vol. 13, No. 1, Januari 2018. Hlm 18.

Rahmani, Aziz. 2019. Information Warfare and Cyber Security. Materi Sekolah Keamanan Nasional, Universitas Bhayangkara Jakarta, Puskamnas Ubhara Jaya, 19 April 2024.

Suparjono. 2019. Revolusi Industri 4.0 dan Dampak terhadap Sumber Daya Manusia. Diakses dari : https://www.kompasiana.com/suparjono46018/5b3fa2fecaf7db4f2b538085/revolusi-industri-4-0-dandampak-terhadap-sumber-daya-manusia. Pada tanggal 20 April 2024, pukul 19.39 WIB.

Yahya, Muhammad. 2018. Era Industri 4.0: Tantangan dan Peluang Perkembangan Pendidikan Kejuruan Indonesia. Orasi Ilmiah Professor bidang Ilmu Pendidikan Kejuruan Universitas Negeri Makassar Tanggal 19 April 2024.