IMEIJ
Indo-MathEdu Intellectuals Journal

p-ISSN: 2808 – 5604
e-ISSN: 2808 – 5078
Volume. 6, No. 2, 2025

KEAMANAN SISTEM INFORMASI AKUNTANSI DALAM ERA DIGITAL: KONSEP DAN IMPLEMENTASI

Hana Elisabet Simanjuntak[1], Hasna Cecilia Purba[2], Jesika Trimanda Br Ginting[3], Putri Angzelina Aruan[4], Ribka Joy Nejevrina Panjaitan[5], Jufri Darma[6]
[1, 2, 3, 4, 5, 6]Universitas Negeri Medan, Jl. William Iskandar Ps. V, Deli Serdang, Sumatera Utara, Indonesia
Email: hanaelisabetsimanjuntak@gmail.com

Article History

Received: 28-03-2025

Revision: 25-04-2025

Accepted: 27-04-2025

Published: 29-04-2025

Abstract. The development of digital technology has driven transformation in accounting information systems (AIS), improving efficiency and accuracy in financial data management. However, this progress is also accompanied by new challenges, especially related to information security risks such as cyber attacks, data leaks, and misuse of information. This research aims to analyze the concept of security in AIS and its implementation in the business world. Using the literature study method, this research examines various strategies implemented by companies to protect financial data, including the implementation of security policies, employee training, and the use of encryption technology and two-factor authentication (2FA). Case studies on PT Astra International and PT Herald Sulsel show that these measures are effective in improving the protection of financial information. However, challenges such as the increasing complexity of cyberattacks and lack of employee awareness are still obstacles that must be overcome. Therefore, strengthening security policies and continuous education for all stakeholders are needed so that accounting information systems remain safe and reliable in the face of evolving digital threats.

Keywords: Accounting Information System Security, Cyber Attacks, Risk Management

Abstrak. Perkembangan teknologi digital telah mendorong transformasi dalam sistem informasi akuntansi (SIA), meningkatkan efisiensi dan akurasi dalam pengelolaan data keuangan. Namun, kemajuan ini juga diiringi oleh tantangan baru, terutama terkait dengan risiko keamanan informasi seperti serangan siber, kebocoran data, dan penyalahgunaan informasi. Penelitian ini bertujuan untuk menganalisis konsep keamanan dalam SIA serta implementasinya dalam dunia bisnis. Metode yang digunakan adalah studi literatur, penelitian ini mengkaji berbagai strategi yang diterapkan perusahaan untuk melindungi data keuangan, termasuk penerapan kebijakan keamanan, pelatihan karyawan, dan penggunaan teknologi enkripsi serta autentikasi dua faktor (2FA). Kasus pada PT Astra Internasional dan PT Herald Sulsel menunjukkan bahwa langkah-langkah ini efektif dalam meningkatkan perlindungan terhadap informasi keuangan. Namun, tantangan seperti meningkatnya kompleksitas serangan siber dan kurangnya kesadaran karyawan masih menjadi kendala yang harus diatasi. Oleh karena itu, diperlukan penguatan kebijakan keamanan serta edukasi berkelanjutan bagi seluruh pemangku kepentingan agar sistem informasi akuntansi tetap aman dan dapat diandalkan dalam menghadapi ancaman digital yang terus berkembang.

Kata Kunci: Keamanan Sistem Informasi Akuntansi, Serangan Siber, Manajemen Risiko

How to Cite: Simanjuntak, H. E., Purba, H. C., Ginting, J. T. B., Aruan, P. A., & Panjaitan, R. J. N. (2025). Keamanan Sistem Informasi Akuntansi dalam Era Digital: Konsep dan Implementasi. *Indo-MathEdu Intellectuals Journal*, 6 (2), 2695-2705. http://doi.org/10.54373/imeij.v6i2.2950

PENDAHULUAN

Era digital telah membawa perubahan signifikan dalam berbagai aspek bisnis dan keuangan, termasuk dalam sistem informasi akuntansi (Safitri & Firdaus, 2024). Sistem informasi akuntansi hanya terbatas pada pengolahan data yang bersifat keuangan saja, sehingga informasi yang dihasilkan oleh sistem informasi akuntansi hanya informasi keuangan saja (Saputri et al., 2023). Digitalisasi telah meningkatkan efisiensi, transparansi, dan akurasi dalam pengelolaan data keuangan, memungkinkan pengambilan keputusan yang lebih cepat dan berbasis data *real-time* (Anriva, 2024). Namun, di balik berbagai manfaat tersebut, sistem informasi akuntansi juga menghadapi tantangan baru, terutama terkait dengan keamanan data dan risiko kejahatan siber, seperti peretasan, pencurian identitas, dan manipulasi data keuangan (Fitriyah, 2024).

Keamanan sistem informasi adalah bagaimana kita dapat mencegah penipuan (cheating) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik (Simons, 2018). Dimensi atau indikator keamanan sistem informasi membagi tiga komponen untuk mengukur objek yakni *cognition*, *affection*, dan *behaviour*. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai *knowledge* (pengetahuan seseorang), *attitude* (sikap seseorang), dan *behaviour* (perilaku seseorang) (Kruger & Kearney, 2006). Keamanan sistem informasi adalah informasi yang merupakan salah satu aset penting untuk dilindungi keamanannya (Nurul et al., 2022). Perusahaan perlu memperhatikan keamanan aset informasinya, karena kebocoran informasi dan kegagalan pada sistem dapat mengakibatkan kerugian, baik pada sisi finansial maupun produktivitas perusahaan (Whitman & Mattord, 2011). Dimensi atau indikator keamanan sistem informasi juga memiliki dua sisi, yaitu relevan dengan pengetahuan lingkungannya (*relevance*) dan patuh terhadap dasar yang ada (*rigor*) (Herver, 2004). Ancaman keamanan sistem informasi dapat menyebabkan kerusakan data, pencurian informasi, dan gangguan operasional yang signifikan. Oleh karena itu, organisasi dan perusahaan harus mengambil tindakan untuk mencegah, mendeteksi, dan merespons ancaman keamanan sistem informasi. Hal ini dapat dilakukan dengan mengimplementasikan strategi keamanan yang tepat, pelatihan karyawan, dan pengawasan sistem yang ketat (Fairuzabadi, et al., 2023).

Ancaman keamanan sistem informasi dapat berasal dari berbagai sumber, baik eksternal maupun internal. Malware merupakan perangkat lunak berbahaya yang dirancang untuk merusak atau mencuri data, seperti virus, worm, trojan, ransomware, dan spyware (Rodes-Ousley, 2013). Serangan siber juga menjadi ancaman serius, mencakup upaya peretasan yang dikategorikan ke dalam empat model: *interruption*, *interception*, *modification*, dan *fabrication*

(Stallings, 2017). Selain itu, kesalahan manusia seperti penggunaan kata sandi yang lemah atau kehilangan perangkat dapat meningkatkan risiko keamanan. Faktor lain adalah bencana alam seperti banjir dan gempa bumi yang dapat merusak infrastruktur sistem informasi, menyebabkan kehilangan atau kerusakan data. Tak kalah penting, ancaman internal dari dalam organisasi seperti karyawan yang tidak jujur atau mantan pegawai yang memiliki akses tidak sah juga dapat membahayakan keamanan sistem (Paryati, 2008; Muttaqin et al., 2023).

Keamanan dalam sistem informasi akuntansi menjadi aspek krusial yang harus diperhatikan oleh perusahaan di era digital. Ancaman seperti phishing, malware, dan serangan ransomware dapat menyebabkan kebocoran data keuangan, yang tidak hanya merugikan perusahaan secara finansial, tetapi juga mengancam kepercayaan pelanggan dan pemangku kepentingan (Sari, 2023). Oleh karena itu, penerapan teknologi keamanan seperti enkripsi data, otentikasi multi-faktor, serta sistem deteksi dan pencegahan intrusi menjadi langkah penting dalam menjaga integritas dan kerahasiaan data akuntansi (Mubarak & Firdaus, 2024)

Tabel 1. Komponen Sistem Informasi Akuntansi

No.	Komponen	Sub Komponen	Jenis
1	*Hardware*	- Bagian input - Bagian pengolahan/prosesor dan memori - Bagian output - Bagian komunikasi	Phisik
2	*Software*	- Sistem Operasi - *Software* aplikasi siklus penerimaan (penjualan) - *Software* aplikasi siklus pengeluaran (pembelian) - *Software* aplikasi siklus produksi - Penerimaan dan pengeluaran kas - *Software* aplikasi siklus GL dan laporan keuangan	Non Phisik
3	*Brainware*	- Manajer sistem informasi - Analisis sistem informasi - Ahli komunikasi - Administrator *database* - Programmer - Operator	Phisik
4	Prosedur	- Rangkaian aktivitas/transaksi dalam: ● Siklus penerimaan (penjualan) ● Siklus produksi dan penggajian ● Siklus pengeluaran (pembelian) ● Penerimaan dan pengeluaran kas ● Siklus GL dan pembuatan laporan Keuangan	Non Phisik
5	Database	- Eksternal data keuangan - Konseptual data keuangan - Internal data keuangan	Non Phisik
6	Jaringan komunikasi	- Server - Terminal	Phisik

- Network card *- Switching hub* - Saluran Komunikasi

Sumber: (Susanto, 2017)

Selain faktor teknologi, keberhasilan implementasi sistem keamanan dalam SIA juga bergantung pada kesiapan organisasi dalam mengadopsi budaya keamanan yang kuat. Banyak perusahaan masih menghadapi kendala dalam mengadaptasi sistem keamanan yang memadai, terutama karena kurangnya pemahaman tentang pentingnya proteksi data serta biaya tinggi yang terkait dengan penerapan teknologi keamanan yang canggih (Fitriyah, 2024). Oleh karena itu, diperlukan strategi menyeluruh yang tidak hanya mencakup aspek teknis tetapi juga edukasi bagi seluruh pemangku kepentingan dalam perusahaan.

Lebih lanjut, regulasi yang mengatur keamanan data dalam sistem informasi akuntansi juga menjadi faktor penting dalam implementasi keamanan (Mubarak & Firdaus, 2024). Perbedaan utama sistem informasi akuntansi dengan sistem informasi yang lainnya adalah sistem informasi akuntansi berfokus pada pengolahan data transaksi keuangan dan transaksi yang terkait dengan keuangan (Puspitawati, 2021). Sejumlah negara telah menerapkan standar kepatuhan seperti General Data Protection Regulation (GDPR) di Uni Eropa dan Peraturan Otoritas Jasa Keuangan (POJK) di Indonesia yang mewajibkan perusahaan untuk menjaga keamanan data keuangan mereka (Anriva, 2024). Dengan adanya regulasi ini, perusahaan dituntut untuk terus memperbarui kebijakan keamanan mereka guna menghindari sanksi dan memastikan perlindungan maksimal terhadap informasi finansial yang bersifat sensitif.

Selain itu, tantangan lain yang dihadapi dalam implementasi keamanan sistem informasi akuntansi adalah meningkatnya serangan siber yang semakin kompleks. Para peretas terus mengembangkan teknik baru untuk mengeksploitasi kelemahan dalam sistem, baik melalui serangan langsung terhadap infrastruktur TI perusahaan maupun melalui rekayasa sosial (social engineering) untuk mendapatkan akses ilegal ke informasi rahasia (Sari, 2023). Oleh karena itu, perusahaan harus menerapkan strategi keamanan berlapis dengan pembaruan sistem secara berkala serta pemantauan yang ketat terhadap aktivitas mencurigakan dalam jaringan mereka.

Penelitian ini bertujuan untuk mengeksplorasi konsep keamanan dalam sistem informasi akuntansi serta implementasinya dalam dunia bisnis. Dengan mengkaji berbagai studi literatur yang relevan, penelitian ini akan mengidentifikasi tantangan utama dalam penerapan keamanan SIA serta solusi yang dapat diterapkan untuk memastikan perlindungan optimal terhadap data keuangan perusahaan di era digital. Hasil penelitian ini diharapkan dapat memberikan wawasan yang lebih komprehensif bagi akademisi dan praktisi bisnis mengenai pentingnya keamanan

dalam sistem informasi akuntansi, serta langkah-langkah yang dapat diambil untuk meningkatkan proteksi data dalam lingkungan bisnis yang semakin terdigitalisasi.

Tujuan utama dari penelitian ini adalah memberikan wawasan mendalam tentang bagaimana keamanan sistem informasi akuntansi dapat diterapkan secara efektif di era digital. Dengan memahami berbagai konsep dan strategi yang telah dikembangkan, penelitian ini diharapkan dapat berkontribusi dalam meningkatkan kesadaran serta praktik keamanan informasi dalam dunia akuntansi. Hal ini penting untuk menjaga integritas, kerahasiaan, dan ketersediaan data akuntansi, terutama dalam menghadapi ancaman siber yang semakin kompleks.

METODE

Penelitian ini menggunakan metode studi literatur untuk mengkaji konsep dan implementasi keamanan sistem informasi akuntansi dalam era digital. Studi literatur dipilih karena memungkinkan peneliti untuk memperoleh wawasan yang komprehensif melalui analisis berbagai sumber referensi seperti buku, jurnal, dan artikel ilmiah. Menurut Sugiyono (2018), metode studi literatur mencakup penggunaan bahan pustaka yang berkaitan erat dengan topik penelitian, sehingga dapat memberikan landasan teoritis yang kuat. Selain itu, Damayanti et al. (2023) dan Rahayu (2018) menekankan pentingnya pemilihan literatur yang kredibel dan relevan agar hasil penelitian dapat dipertanggungjawabkan secara akademik.

Sumber data utama dalam penelitian ini adalah literatur yang secara spesifik membahas keamanan sistem informasi akuntansi. Sumber-sumber ini meliputi buku yang menjelaskan konsep dasar keamanan informasi serta prinsip-prinsip akuntansi dalam sistem digital, jurnal akademik yang mendokumentasikan implementasi keamanan dalam praktik nyata, dan artikel ilmiah yang mengkaji tantangan serta inovasi dalam bidang ini. Literatur yang digunakan dipilih berdasarkan kredibilitas dan relevansinya dengan penelitian, mengacu pada prinsip yang dijelaskan oleh Damayanti et al. (2023), yang menekankan bahwa studi literatur harus berlandaskan pada sumber yang valid dan mutakhir.

Teknik pengumpulan data dilakukan melalui beberapa tahap yang sistematis. Tahap pertama adalah pencarian literatur menggunakan kata kunci yang relevan dalam database akademik dan perpustakaan digital. Setelah itu, dilakukan seleksi literatur dengan mempertimbangkan relevansi, kredibilitas, dan kualitas data yang disajikan. Selanjutnya, literatur yang dipilih dibaca secara mendalam menggunakan teknik scanning dan skimming untuk mengidentifikasi informasi yang sesuai dengan tujuan penelitian. Analisis data dalam penelitian ini dilakukan dengan pendekatan sintesis dan interpretasi. Tahap pertama dalam

analisis adalah pengumpulan data yang memiliki keterkaitan langsung dengan keamanan sistem informasi akuntansi dalam era digital. Data yang telah dikumpulkan kemudian dianalisis untuk mengidentifikasi pola, tantangan, serta solusi yang telah dikembangkan dalam bidang ini. Berdasarkan teori yang dikemukakan oleh Sugiyono (2018), proses analisis dalam studi literatur mencakup penyimpulan hasil berdasarkan temuan yang telah dikaji secara mendalam. Penyajian hasil penelitian dilakukan secara sistematis agar dapat memberikan gambaran yang jelas mengenai penerapan keamanan dalam sistem informasi akuntansi.

HASIL

Keamanan Sistem Informasi Akuntansi (SIA) merupakan elemen fundamental dalam menjaga keandalan, kerahasiaan, dan ketersediaan data keuangan suatu perusahaan. Keamanan sistem mencakup upaya perlindungan terhadap sistem komputer dan jaringan dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan yang tidak sah (Whitman & Mattord, 2011). Untuk mencapai tujuan tersebut, berbagai tindakan, protokol, dan teknologi diterapkan guna memastikan informasi tetap aman dan terlindungi dari ancaman serta kerentanan yang dapat mengganggu operasional sistem (Stallings, 2017). Keamanan dalam SIA mencakup aspek perlindungan fisik maupun logis yang melibatkan perangkat keras, perangkat lunak, serta data, sehingga perusahaan dapat menjaga keabsahan informasi keuangan dan mencegah potensi risiko yang merugikan (Husna et al., 2024). Dalam konteks bisnis dan akuntansi, penerapan strategi keamanan yang efektif menjadi kunci dalam memitigasi ancaman siber serta memastikan sistem tetap berfungsi dengan optimal (Safitri & Firdaus, 2024). Berikut ini akan dibahas implementasi keamanan informasi di perusahaan, diikuti dengan analisis efektivitas strategi pengamanan yang diterapkan berdasarkan penelitian yang relevan.

Penelitian oleh Husna et al. (2024) mengidentifikasi dan mengevaluasi berbagai risiko keamanan informasi di PT Astra Internasional, termasuk ancaman eksternal seperti serangan siber dan peretasan, serta ancaman internal seperti kebocoran atau penyalahgunaan data oleh karyawan. Selain itu, kerentanan sistem dapat meningkatkan risiko kehilangan atau penyalahgunaan data pelanggan dan karyawan. Untuk mengatasi risiko ini, PT Astra Internasional menerapkan beberapa strategi utama. Pertama, perusahaan menerapkan kebijakan keamanan informasi yang mengatur akses dan perlindungan data guna meminimalkan risiko kebocoran. Kedua, karyawan mendapatkan pelatihan keamanan informasi untuk meningkatkan kesadaran terhadap ancaman siber dan mengurangi resiko akibat kesalahan manusia (Setiawan & Kusuma, 2019). Ketiga, perusahaan berinvestasi dalam teknologi keamanan seperti firewall, enkripsi data, dan sistem deteksi ancaman untuk

memperkuat infrastruktur IT mereka. Analisis efektivitas strategi ini menunjukkan bahwa kebijakan keamanan yang diterapkan berhasil mengurangi ancaman internal, sementara evaluasi kerentanan sistem membantu perusahaan mengidentifikasi dan memperbaiki titik-titik lemah dalam infrastrukturnya. Selain itu, manajemen risiko cyber security yang diterapkan memungkinkan PT Astra Internasional untuk lebih siap dalam menghadapi ancaman digital yang terus berkembang dalam penelitian Pratama & Yulianto (2017). Namun, tantangan masih ada, termasuk meningkatnya ancaman siber yang semakin kompleks, perlunya peningkatan kesadaran karyawan mengenai keamanan informasi, serta kepatuhan terhadap regulasi yang terus berubah. Oleh karena itu, PT Astra Internasional perlu terus mengembangkan strategi keamanan yang lebih adaptif untuk memastikan perlindungan data yang lebih baik di masa depan.

Kemudian kasus kedua oleh Junillah et al. (2024) menganalisis implementasi keamanan sistem informasi di PT. Herald Sulsel. Implementasi keamanan sistem informasi di Perusahaan Herald Sulsel dilakukan untuk melindungi data sensitif perusahaan dari berbagai ancaman. Perusahaan menghadapi risiko keamanan seperti kerentanan jaringan yang rentan terhadap serangan eksternal, potensi kebocoran data yang dapat merugikan secara finansial maupun reputasi, serta kurangnya kesadaran karyawan terhadap ancaman keamanan. Untuk mengatasi risiko ini, perusahaan menerapkan beberapa strategi utama, yaitu perusahaan menggunakan kombinasi server internal dan pihak ketiga untuk menghindari akses tidak sah, menggunakan sistem enkripsi dan otentikasi guna melindungi data sensitif yang dikirim melalui jaringan maupun klasifikasi informasi dengan membagi data menjadi kategori rahasia, internal, dan publik agar lebih mudah dikelola dan diamankan. Selain itu, perusahaan menerapkan kontrol akses yang ketat melalui autentikasi dua faktor (2FA) serta penggunaan berbagai tools keamanan untuk mendeteksi ancaman secara dini.

Analisis efektivitas strategi ini menunjukkan bahwa langkah-langkah yang diterapkan berhasil meningkatkan keamanan sistem informasi. Kesadaran karyawan terhadap keamanan informasi meningkat, tetapi masih perlu pelatihan lebih lanjut agar mereka dapat mengenali dan mencegah ancaman dengan lebih baik. Klasifikasi informasi yang dilakukan terbukti efektif dalam mengurangi risiko kebocoran data, sementara sistem enkripsi dan otentikasi meningkatkan perlindungan akses ke informasi penting. Namun, ada beberapa tantangan yang masih harus dihadapi, seperti meningkatnya serangan siber yang semakin canggih sehingga perusahaan harus selalu memperbarui sistem keamanannya. Selain itu, kurangnya pelatihan khusus bagi karyawan masih menjadi kendala, sehingga perlu adanya program edukasi yang lebih terstruktur. Perusahaan juga harus memastikan kepatuhan terhadap regulasi keamanan

informasi yang terus berkembang agar tidak menghadapi risiko hukum di masa depan. Secara keseluruhan, Perusahaan Herald Sulsel telah menerapkan langkah-langkah yang cukup baik dalam mengamankan sistem informasinya. Namun, mereka perlu terus meningkatkan kesadaran karyawan, melakukan evaluasi berkala terhadap kebijakan keamanan, serta mengadaptasi strategi keamanan agar tetap efektif menghadapi ancaman baru di era digital.

DISKUSI

Keterbatasan anggaran adalah salah satu tantangan paling signifikan yang dihadapi oleh banyak perusahaan, terutama perusahaan kecil dan menengah. Investasi dalam keamanan siber sering kali dianggap sebagai biaya tambahan, bukan sebagai kebutuhan yang mendesak. Banyak perusahaan tidak memiliki tim IT yang cukup besar atau terlatih untuk menangani ancaman siber yang kompleks. Sebagai contoh kasus Herald Sulsel seperti yang disebutkan dalam studi oleh Junillah, Rahma, dan Oktaviyah (2024), perusahaan ini telah menerapkan langkah-langkah keamanan seperti penggunaan server internal dan pihak ketiga, enkripsi data, serta kontrol akses yang ketat. Namun, tidak disebutkan adanya tim IT yang besar atau anggaran khusus yang dialokasikan untuk keamanan siber. Sejalan dengan laporan dari Ponemon Institute (2019), lebih dari 60% perusahaan mengalami keterbatasan anggaran dalam melindungi data mereka. Tantangan yang sama tampaknya dihadapi oleh Herald Sulsel. Tanpa anggaran yang cukup, perusahaan mungkin kesulitan untuk memperbarui infrastruktur keamanan mereka secara berkala atau mengadopsi teknologi terbaru untuk mendeteksi ancaman lebih awal.

Karyawan sering kali menjadi titik lemah dalam pertahanan keamanan informasi perusahaan. Meskipun teknologi dapat memberikan perlindungan, kesadaran dan perilaku karyawan sangat penting dalam menjaga keamanan data. Kasus Herald Sulsel juga menyoroti pentingnya kesadaran karyawan terhadap keamanan informasi. Hasil analisis menunjukkan bahwa meskipun karyawan memahami pentingnya keamanan sistem informasi, mereka tidak selalu dapat mencegah serangan keamanan secara efektif (Junillah et al., 2024). Hal ini menunjukkan bahwa kesadaran karyawan masih perlu ditingkatkan, sebagaimana ditemukan dalam penelitian IBM Security (2020), bahwa 90% pelanggaran data disebabkan oleh kesalahan manusia. Selain itu, studi oleh KnowBe4 (2021) menekankan bahwa perusahaan yang melakukan pelatihan keamanan secara rutin dapat mengurangi risiko pelanggaran data hingga 70%. Dalam kasus Herald Sulsel, tidak adanya pelatihan keamanan yang rutin menjadi kelemahan yang dapat dieksploitasi oleh penyerang siber. Oleh karena itu, perusahaan perlu

mengembangkan program edukasi dan pelatihan berkala untuk meningkatkan kesadaran karyawan terhadap ancaman siber.

Ancaman siber terus berkembang dan menjadi semakin kompleks. Serangan seperti ransomware, phishing, dan malware tidak hanya semakin canggih, tetapi juga lebih terorganisir. Demikian juga, ancaman siber menjadi tantangan pada kasus Herald Sulsel. Perusahaan telah menerapkan berbagai sistem keamanan, seperti enkripsi data dan autentikasi dua faktor (2FA), yang merupakan langkah positif dalam menghadapi ancaman (Junillah et al., 2024). Namun, laporan Verizon (2021) menunjukkan bahwa serangan phishing meningkat 220% pada tahun 2020, yang berarti perusahaan harus terus memperbarui strategi keamanan mereka. Jika Herald Sulsel tidak secara berkala meninjau dan meningkatkan sistem keamanan mereka, maka mereka akan rentan terhadap serangan siber yang semakin canggih. Untuk mengatasi ini, mereka perlu menerapkan teknologi keamanan terbaru seperti kecerdasan buatan (AI) dan pembelajaran mesin (machine learning) untuk mendeteksi ancaman secara proaktif. Selain itu, penilaian risiko secara berkala juga harus dilakukan untuk memastikan bahwa sistem tetap aman terhadap serangan baru.

KESIMPULAN

Untuk meningkatkan keamanan sistem informasi di perusahaan seperti PT Astra Internasional dan Perusahaan Herald Sulsel diperlukan strategi berbasis prinsip CIA (Confidentiality, Integrity, Availability). Perusahaan meningkatkan pelatihan keamanan bagi karyawan dikarenakan kesadaran mereka terhadap ancaman siber masih rendah. Pelatihan harus dilakukan secara rutin dan berkelanjutan, seperti simulasi serangan phishing dan uji keamanan berkala. Selain itu, perusahaan perlu menerapkan kebijakan penggunaan kata sandi yang kuat, autentikasi dua faktor (2FA), serta pembatasan akses data sesuai peran karyawan untuk mengurangi risiko kebocoran informasi. Kemudian mengadopsi teknologi keamanan yang lebih canggih diperlukan untuk menangani ancaman yang terus berkembang. Perusahaan harus mengimplementasikan Sistem Deteksi dan Pencegahan Intrusi (IDPS) berbasis AI, serta menggunakan enkripsi tingkat lanjut seperti AES-256 untuk melindungi data. Selain itu, penerapan Zero Trust Architecture, firewall tingkat lanjut, VPN terenkripsi, dan pemantauan berbasis cloud akan memperkuat sistem keamanan perusahaan.

REKOMENDASI

Pengembangan kebijakan dan regulasi internal yang lebih ketat harus dilakukan agar sistem keamanan lebih terstruktur. Perusahaan perlu mengadopsi standar keamanan internasional seperti ISO 27001 yang menerapkan prinsip least privilege dalam manajemen akses, serta melakukan audit keamanan berkala dan simulasi serangan siber untuk menguji kesiapan tim dalam menangani insiden. Dengan menerapkan strategi ini, kedua perusahaan dapat meningkatkan ketahanan terhadap serangan siber, melindungi data mereka, dan memastikan keamanan informasi tetap terjaga di era digital.

REFERENSI

Azhar, Susanto. 2017. Sistem Informasi Akuntansi. Cetakan pertama. Bandung: Lingga Jaya.

Bodnar dan Hopwood. (2006). Sistem Informasi dan Akuntans. diterjemahkan oleh Amir Abadi Jusuf. Edisi 10. Andi. Yogyakarta.

Damayanti, A. T., Pradana, B. E., Putri, B. P., & Laila, H. N. (2023). Literature Review:

Fairuzabadi, M., Pangaribuan, J. J., Moedjahedy, J. H., Simarmata, J., Andryanto, A., Jaya, A. K., ... & Pungus, S. R. (2023). Keamanan Sistem Informasi dan Kriptografi. Yayasan Kita Menulis.

Fitriyah, R. (2024). *Keamanan sistem informasi dalam era digital: Tantangan dan solusi*. Jurnal Teknologi Informasi, 10(2), 45-60.

Gold, S. (2004) 'Threats looming beyond the perimeter', Information Security Technical Report, 9(4), pp. 12–14. Available at: https://doi.org/10.1016/S1363-4127(04)00047-0.

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis. Jurnal Konstituen, 5(1), 1-17.

Hilia Anriva, D. (2024). Tantangan Dan Solusi Penerapan Sistem Informasi Akuntansi Di Indonesia: Sebuah Analisis Tematik. Jurnal Akuntansi, 13(2), 97–109.

Husna, H., Afriliani, I., & Fitriana, N. (2024). Manajemen Risiko Keamanan Sistem Informasi Akuntansi Pada Perusahaan Otomotif Pt. Astra Internasional. Jurnal Akuntansi Keuangan Dan Bisnis, 2(2), 296-299.

Ibm Security. (2020). *Cost Of a Data Breach Report 2020*. Ponemon Institute. https://www.ibm.com/security/data-breach

Internasional. Jurnal Manajemen Informasi, 4(2), 15-30. Jakarta: PT Gramedia.

Junillah, A. L., Rahma, F., & Oktaviyah, N. (2024). Analisis Implementasi Keamanan Sistem Informasi pada Perusahaan Herald Sulsel. Journal of Accounting, Economics, and Business Education, 150-156.

Kartiningsih, S., & Zed, M. (2023). Metode Penelitian Studi Literatur: Teori dan Aplikasi.

KnowBe4. (2021). *The 2021 Phishing by Industry Benchmarking Report*. https://www.knowbe4.com/phishing-report

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & security, 25(4), 289-296.

Mark Rodhes-Ousley (2013) The Complete Refference: Information Security. 2nd ed. New York: McGraw-Hill Companies.

Moscove, Stephen A and Mark G. Simkin, Accounting Information System : Consepts and Practise, John Willey and Son, 1981.

Mubarak, T. Z., & Firdaus, R. (2024). Peran Sistem Informasi Akuntansi dalam Pengaplikasian Enkripsi terhadap Peningkatan Keamanan Perusahaan. Jurnal Intelek Insan Cendikia (JIIC), 1(9), 5910-5911

Muttaqin et al. (2023) Pengantar Teknologi Digital. Medan: Yayasan Kita Menulis.

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). Jurnal Ekonomi Manajemen Sistem Informasi, 3(5), 564-573.

Paryati (2008) 'Keamanan Sistem Informasi', Seminar Nasional Informatika 2008, 2008(semnasIF), pp. 379–386.

Pratama, D., & Yulianto, A. (2017). Manajemen Risiko Cybersecurity dalam Industri Otomotif: Perspektif PT Astra Internasional. Jurnal Problematika Kesiapan Guru terhadap Penerapan Kurikulum Merdeka. In SNHRP-5

Ponemon Institute. (2019). *Global State of Cybersecurity in Small and Medium-Sized Businesses*. https://www.ponemon.org/local/upload/file/SMB_Cybersecurity_Report_2019.pdf

Puspitawati, L. (2021). Sistem Informasi Akuntansi: Kualitas dan Faktor Lingkungan Organisasi yang Mempengaruhi.

Romney, Marshall B. dan Paul John Steinbart, 2017. Sistem Informasi Akuntansi, Edisi 13, Cetakan keenam, Penerbit Salemba Empat, Jakarta Selatan

Safitri, D., & Firdaus, R. (2024). PENERAPAN SISTEM INFORMASI AKUNTANSI DALAM BISNIS MODERN MENGHADAPI TANTANGAN DIGITALISASI. Jurnal Intelek Dan Cendikiawan Nusantara, 1(6), 9511-9514.

Saputri, H., Kusnaedi, U., & Asmana, Y. (2023). Pengaruh Sistem Informasi Akuntansi Terhadap Kualitas Laporan Keuangan Perusahaan Jasa di Jakarta Utara. Madani: Jurnal Ilmiah Multidisiplin, 1(4), 102-109.

Sari, A. K., & Hwihanus. (2023). Peranan Sistem Informasi Akuntansi dan Implementasi Menghadapi Pemalsuan Data di Era Digital pada Masyarakat Desa. MRI: Jurnal Manajemen Riset Inovasi, 1(1), 186-196.

Seminar Nasional Hasil Riset dan Pengabdian.

Setiawan, R., & Kusuma, A. (2019). Analisis Kebijakan Perlindungan Data Karyawan dan Pelanggan di Perusahaan Otomotif: Kasus PT Astra

Stallings, W. (2017) Cryptography and Network Security: Principles and Practice 7th Global Edition. Pearson.

Sugiyono. (2018). Metode Penelitian Kuantitatif. Bandung: Alfabeta.

Susanto, A. (2017). Sistem Informasi Akuntansi (Pemahaman Konsep Secara Terpadu). Bandung: Linga Jaya

Teknologi Informasi dan Komunikasi Bisnis, 1(2), 30-45

Verizon. (2021). *Data Breach Investigations Report (DBIR) 2021*. https://www.verizon.com/business/resources/reports/dbir/

Whitman, M. E., & Mattord, H. J. (2011). Roadmap to information security: For IT and infosec managers. Delmar Learning.