PELITA Jurnal Penelitian dan Karya Ilmiah
Volume 25, Issue 02, December 2025, pp. 335-338
P-ISSN: 1907-5693 E-ISSN: 2684-8856
DOI Article: https://doi.org/10.33592/pelita.v25i2.5898

Peran Kebijakan Keamanan dalam Mengurangi Unauthorized Access pada Sistem Informasi

Rivki Saputra[1], Muhamad Rizky Icwan[2], Yuga Tama Wardani[3], Angjela Putri Asandi[4], Titin Agustina[5]
[1,2,3,4,5]Universitas Bina Sarana Informatika, Jakarta, Indonesia.

Article history:
Received July 12, 2025
Revised August 02, 2025
Accepted October 30, 2025
Available online December 30, 2025

Kata Kunci:
Unauthorized Access, Kebijakan Keamanan, Manajemen Risiko

Keywords:
Unauthorized Access, Security Policy, Risk Management

A B S T R A C T

Unauthorized access pada sistem informasi merupakan tantangan utama bagi organisasi di era digital. Jurnal ini membahas peran kebijakan keamanan dalam mengurangi risiko tersebut melalui tinjauan pustaka, analisis risiko, dan evaluasi implementasi. Penelitian menunjukkan bahwa kebijakan keamanan yang komprehensif, termasuk enkripsi data, autentikasi dua faktor, dan pemantauan sistem, efektif dalam melindungi aset digital. Manajemen risiko dan edukasi staf juga berperan penting dalam meningkatkan keamanan. Kesimpulannya, investasi dalam infrastruktur keamanan dan pelatihan staf sangat penting untuk menjaga integritas data dan mencegah kerugian akibat serangan cyber.

A B S T R A C T

Unauthorized access to information systems is a major challenge for organizations in the digital era. This journal discusses the role of security policies in mitigating such risks through literature review, risk analysis, and implementation evaluation. The research shows that comprehensive security policies, including data encryption, two-factor authentication, and system monitoring, are effective in protecting digital assets. Risk management and staff education also play an important role in improving security. In conclusion, investment in security infrastructure and staff training are essential to maintain data integrity and prevent

1. INTRODUCTION

Keamanan informasi adalah aspek penting untuk menjaga integritas dan kepercayaan dalam sistem informasi di berbagai industri. Dalam beberapa tahun terakhir, insiden keamanan seperti akses tidak sah (unauthorized access) meningkat seiring kemajuan teknologi. Akses tidak sah adalah pelanggaran di mana pihak yang tidak berwenang mendapatkan akses ke data yang seharusnya dilindungi, yang dapat menyebabkan kerugian finansial, hilangnya data, dan rusaknya reputasi organisasi. Oleh karena itu, kebijakan keamanan yang kuat sangat penting untuk mencegah akses tidak sah dan menjaga kerahasiaan data.

Kebijakan keamanan informasi mencakup aturan dan prosedur untuk mengatur penyimpanan, akses, dan perlindungan data. Penelitian pada PT. Indofood Sukses Makmur menunjukkan bahwa pengamanan objek vital dan sistem cyber dapat meminimalkan potensi akses tidak sah (Edy Susanto et al., 2023). Kesadaran individu juga berperan penting; pemahaman tentang keamanan informasi dapat mengurangi risiko dari teknik social engineering (Mahendra Adhi Nugroho et al., 2024).

Penerapan kecerdasan buatan (AI) dalam sistem informasi membantu mendeteksi dan mencegah akses tidak sah, meskipun juga menghadirkan tantangan baru terkait pengelolaan data kompleks. Optimalisasi AI dapat meningkatkan perlindungan data di kantor (Joy Phillip Nehemia & Muhammad Rifky Hendrayana, 2024). Selain AI, metode seperti Virtual Private Network (VPN) dan kriptografi juga penting untuk meningkatkan ketahanan sistem informasi (Berliana Syela Fajrin et al., 2024). Namun, tantangan utama adalah minimnya kepatuhan pengguna terhadap kebijakan yang ada.

Penelitian menunjukkan bahwa kepatuhan terhadap kebijakan keamanan dapat mengurangi risiko kebocoran data dan meningkatkan kontrol akses (Sitompul & Nasution, 2024). Penelitian ini bertujuan untuk mengidentifikasi peran kebijakan keamanan dalam mengurangi unauthorized access pada sistem informasi. Diharapkan penelitian ini memberikan wawasan mendalam tentang komponen kebijakan yang efektif serta strategi terbaru untuk meningkatkan keamanan sistem informasi. Selain itu, penelitian ini juga

*Corresponding author.
E-mail addresses: rizkyicwan84@gmail.com

mengulas strategi dan teknologi yang dapat diadopsi organisasi untuk meminimalkan risiko akses tidak sah serta pentingnya kesadaran dan kepatuhan terhadap kebijakan keamanan.

2. METHODS

Penelitian ini menggunakan pendekatan kualitatif dengan metode tinjauan pustaka untuk menganalisis peran kebijakan keamanan dalam mengurangi unauthorized access pada sistem informasi. Metode ini melibatkan pengumpulan dan analisis data dari berbagai sumber literatur yang relevan, termasuk artikel jurnal, buku, dan laporan penelitian terkait kebijakan keamanan dan manajemen risiko.

3. RESULT AND DISCUSSION Results and Discussion

Kebijakan keamanan informasi yang kuat terbukti mengurangi akses tidak sah (Unauthorized Access). Studi menunjukkan bahwa organisasi yang menerapkan kebijakan keamanan memiliki tingkat pelanggaran keamanan lebih rendah dibandingkan dengan organisasi yang tidak menerapkan.

Dalam Keputusan Presiden Nomor 63 Tahun 2004 disebutkan bahwa obyek vital nasional kawasan/lokasi/bangunan/instalasi adalah dan/atau usaha yang menyangkut hajat hidup orang banyak, kepentingan negara, dan/atau sumber pendapatan negara yang bersifat strategis. Mengingat peranannya yang cukup strategis, obyek vital nasional membutuhkan sistem pengamanan yang lebih kuat dan didasarkan atas standar sistem pengamanan yang ketat, sehingga mampu memperkecil risiko dan dampak keamanan yang ditimbulkan akibat adanya ancaman dan gangguan keamanan (Edy Susanto et al., 2023).

Untuk menerapkan sistem pengamanan yang lebih kuat serta sistem pengamanan yang ketat diperlukannya implementasi mekanisme otentifikasi (Password kuat dan two-factor terbuka untuk yang authentication) yang dapat memverifikasi identitas pengguna.

Menggunakan kata sandi atau kata sandi yang lemah adalah masalah yang sangat umum, keamanannya dapat ditingkatkan secara signifikan melalui pelatihan dan pengenalan berbagai aplikasi manajemen kata sandi. Sebagian besar pencurian data sensitif disebabkan oleh beberapa kesalahan keamanan dasar (Indri Widya Wulandari & Hwihanus Hwihanus, 2023).

Tidak hanya menggunakan kata sandi yang kuat, menggunakan autentifikasi dua faktor juga merupakan langkah strategis dalam kebijakan keamanan untuk mencegah akses tidak sah. Menurut (Ayedh M et al., 2023), keamanan BYOD yang ideal menekankan metode control akses identifikasi keamanan BYOD yang ideal menekankan metode kontrol akses identifikasi, seperti biometrik dan autentikasi dua faktor. Dengan menggunakan portal dan otentikasi dua faktor, pengguna diberikan sarana yang aman dan nyaman untuk memungkinkan akses ke aplikasi penting saja dan melarang permintaan yang tidak diautentikasi, sehingga membatasi layanan yang dapat diakses oleh perangkat yang berpotensi menyerang. Perubahan pada peralihan aturan streaming dapat diterapkan dengan cepat, memastikan bahwa pengguna selalu memiliki akses terbaru ke jaringan dengan prediksi serangan.

Dengan mengenkripsi data juga dapat melindungi sistem informasi dari Unauthorized Access atau akses tidak sah. Enkripsi data merupakan proses data khusus untuk menyembunyikan atau mengkhususkan data dalam bentuk pribadi maupun publik, kontrol akses merupakan verifikasi data pengguna yang melakukan akses komputer, artinya informasi hanya membutuhkan, pengguna sedangkan teknologi firewall adalah alat yang dapat mencegah orang lain menggunakan komputer pribadi, mencegah orang lain mendekati sistem pertahanan, dan memfilter situs yang dapat membahayakan komputer. SOP (Standar Operasional Prosedur) dan kebijakan privasi juga harus diterapkan oleh pengembang sistem karena administrator memiliki akses penuh pada data pengguna sehingga, mereka perlu membangun kepercayaan pengguna dan mencegah adanya keamanan informasi pengguna terjaga (Achmad Mukhlis et al., 2023). Meskipun data dicuri, namun tidak memiliki kunci enkripsi maka informasi atau data tetap terlindungi meskipun terjadi pelanggaran keamanan.

Untuk mendeteksi aktivitas mencurigakan, anomali, atau potensi ancaman keamanan, pemantauan sistem diperlukan untuk pengawasan secara real time dan analisis data aktivitas pada sistem informasi, jaringan, dan perangkat. Dengan mengidentifikasi aktivitas mencurigakan seperti Upaya login berulang (brute force), perubahan pada data, atau akses tidak sah. Akan meningkatkan peluang untuk mencegah insiden pelanggaran keamanan.

Salah satu teknologi pendeteksi ancaman keamanan untuk pemantauan sistem yaitu SIEM (Security Information and Event Management). SIEM (Security Information and Event Management) adalah solusi keamanan yang digunakan oleh organisasi untuk mendeteksi dan merespons ancaman keamanan pada sistem informasi . SIEM mengumpulkan dan menganalisis data dari berbagai sumber, termasuk log keamanan, aktivitas pengguna, dan lalu lintas jaringan, untuk mendeteksi aktivitas mencurigakan atau serangan yang terjadi. SIEM juga memungkinkan organisasi untuk mempercepat respons terhadap ancaman dan mengurangi risiko kerentanan keamanan pada sistem informasi (Anggara, 2023).

Manajemen risiko dalam keamanan informasi adalah upaya untuk mengidentifikasi potensi ancaman dan kerentanan, menilai dampak yang mungkin terjadi, dan merancang langkah-langkah untuk memitigasi risiko tersebut. Fokus utamanya adalah memastikan bahwa sumber daya informasi tetap terlindungi dari akses yang tidak sah.

Dalam mengelola risiko keamanan informasi dengan menggunakan salah satu framework standar keamanan yaitu ISO 27001. ISO/IEC 27001:2022 merupakan revisi terbaru yang memperbarui dan menyempurnakan standar sebelumnya, mencakup perubahan signifikan yang relevan dengan dinamika ancaman siber saat ini. Standar ini dirancang untuk memastikan bahwa keamanan informasi bukan hanya tanggung jawab departemen TI, tetapi juga menjadi bagian integral dari tata kelola organisasi secara keseluruhan. Dengan pendekatan berbasis risiko, ISO/IEC 27001:2022 membantu organisasi dalam mengidentifikasi risiko keamanan yang potensial dan menetapkan kontrol yang tepat untuk mengelola risiko tersebut (Sinaga & Taan, 2024).

Tidak hanya kebijakan keamanan informasi pada teknologi yang perlu dipelajari. Namun, kesadaran dan pelatihan staf juga sangat perlu untuk dipelajari. Edukasi staf merupakan komponen vital dalam kebijakan keamanan untuk memastikan semua karyawan memahami perannya dalam melindungi sistem informasi dari akses tidak sah (unauthorized access). Edukasi yang efektif menciptakan budaya keamanan yang kuat dan membantu mencegah insiden yang disebabkan oleh kesalahan manusia.

Kesadaran dan pelatihan karyawan adalah salah satu pertahanan pertama dan penting terhadap ancaman keamanan informasi. Karyawan yang terlatih dengan baik cenderung lebih waspada terhadap serangan siber, lebih mampu mengidentifikasi tanda- tanda insiden keamanan, dan lebih efektif dalam menjaga data organisasi tetap aman. Ini juga dapat membantu mengurangi risiko pelanggaran data yang disebabkan oleh tindakan atau kesalahan karyawan (Sitompul & Nasution, 2024).

Untuk mencegah kebocoran informasi, perusahaan dan organisasi harus mengambil langkahlangkah keamanan yang tepat, seperti menggunakan enkripsi data, memperkuat akses ke data rahasia, dan memastikan bahwa karyawan terlatih dan memahami pentingnya menjaga kerahasiaan data. Pada tingkat individu, penggunaan teknologi yang aman, seperti penggunaan password yang kuat dan tidak membagikan informasi pribadi secara sembarangan, juga dapat membantu mencegah kebocoran informasi. Untuk dapat mencegah kebocoran informasi maka dapat dilakukan dengan tindakan preventif seperti mengikuti standar keamanan informasi (Anggara, 2023).

Selain dari hasil - hasil studi diatas, ada beberapa langkah lagi yang dapat diterapkan untuk mengatasi akses tidak sah (Unauthorized access) diantaranya,

1. Melakukan backup data secara rutin, untuk memastikan agar data dapat dipulihkan jika suatu saat terjadi insiden keamanan seperti ransomware atau kehilangan data, melakukan pencadangan harus dilakukan secara berkala.
2. Audit keamanan berkala, dengan melakukan audit secara rutin, dapat membantu mengidentifikasi celah keamanan dan area yang perlu diperbaiki serta menilai efektivitas dan kontrol yang ada.
3. Pengelolaan akses berbasis peran, dengan menerapkan model ini, dapat memastikan pengguna mendapatkan informasi hanya yang diperlukan berdasarkan peran mereka.
4. Pemanfaatan teknologi blockchain, dengan menggunakan blockchain, transparansi dan integritas data dapat diperoleh. Karna blockchain juga dapat mengurangi resiko manipulasi data, keamanan data dan transaksi pun ikut meningkat.
5. Program respon insiden, mengembangkan dan menguji rencana respon insiden untuk memastikan organisasi dapat merespon dengan cepat dan efektif bila terjadi insiden keamanan.
6. Memperbarui firewall, karena firewall merupakan pertahanan yang berada pada jaringan, perlu untuk melakukan pembaruan firewall dan konfigurasinya untuk tetap menjaga jaringan pada kondisi yang prima

4. CONCLUSION

Keamanan informasi merupakan aspek penting dalam menjaga integritas dan kepercayaan dalam sistem informasi di berbagai industri. Akses tidak sah (unauthorized access) adalah tindakan yang dilakukan pihak yang tidak berwenang untuk mendapatkan akses ke data penting, yang dapat menyebabkan kerugian finansial, hilangnya data, atau rusaknya reputasi organisasi. Kecerdasan buatan (AI) dapat membantu mendeteksi dan mencegah akses tidak sah, dan optimalisasi (AI) dapat meningkatkan perlindungan data di kantor. Pelatihan karyawan tentang keamanan informasi sangat penting untuk

mengurangi risiko akses tidak sah (unauthorized access). Karyawan yang terlatih dapat lebih waspada terhadap serangan siber, lebih mampu mengidentifikasi tanda tanda insiden keamanan, dan lebih efektif dalam menjaga data organisasi tetap aman.

Selain itu, untuk mencegah kebocoran informasi, perusahaan dan organisasi harus mengambil langkah-langkah keamanan yang tepat, seperti menggunakan enkripsi data, memperkuat kontrol akses ke data rahasia, serta memastikan kesadaran dan kepatuhan karyawan terhadap kebijakan keamanan. Penelitian ini menegaskan bahwa kebijakan keamanan yang komprehensif, pengelolaan risiko yang baik, dan investasi dalam infrastruktur serta pelatihan staf merupakan langkah penting untuk mengurangi risiko akses tidak sah, menjaga integritas data, dan melindungi organisasi dari kerugian akibat serangan siber.

5. REFERENCES

Achmad Mukhlis, Baiq Laila Alfila, & Aliya Zhafira Wastuyana. (2023). Ancaman dan Langkah Pengamanan Sistem Informasi Menggunakan Metode Systematic Literature Review. Jurnal ilmiah Sistem Informasi dan Ilmu Komputer, 3(2), 143–152. https://doi.org/10.55606/juisik.v3i2.496

Anggara, T. R. (2023). Strategi Implementasi SIEM untuk Mengurangi Risiko terhadap Kebocoran Informasi. Jurnal Teknologi Terpadu, 9(2), 101–107. https://doi.org/10.54914/jtt.v9i2.756

Ayedh M, A. T., Wahab, A. W. A., & Idris, M. Y. I. (2023). Systematic Literature Review on Security Access Control Policies and Techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions. Applied Sciences, 13(14), 8048. https://doi.org/10.3390/app13148048

Berliana Syela Fajrin, Priatno, & Muhammad Ridwan Effendi. (2024). PENERAPAN SISTEM KEAMANAN JARINGAN MENGGUNAKAN VPN DENGAN METODE PPTP PADA PT HINOKA SINERGI TANYO. JURNAL SISTEM INFORMASI UNIVERSITAS SURYADARMA, 11(2). https://doi.org/10.35968/jsi.v11i2.1252

Edy Susanto, Alvionita Dairo Lende, Akmal Riza Firjatullah, & Reza Almasyah Pratama. (2023). Analisis Keamanan Informasi PT. Indofood Sukses Makmur, Tbk: Studi Kasus tentang Peran Objek Vital, Pengamanan File, dan Pengamanan Cyber. Jurnal Manajemen dan Ekonomi Kreatif, 1(3), 79–87. https://doi.org/10.59024/jumek.v1i3.116

Indri Widya Wulandari & Hwihanus Hwihanus. (2023). PERAN SISTEM INFORMASI AKUNTANSI DALAM PENGAPLIKASIAN ENKRIPSI TERHADAP PENINGKATAN KEAMANAN PERUSAHAAN. Jurnal Kajian dan Penalaran Ilmu Manajemen, 1(1), 11–25. https://doi.org/10.59031/jkpim.v1i1.46

Joy Phillip Nehemia & Muhammad Rifky Hendrayana. (2024). Tantangan Dan Manfaat AI Dalam Perlindungan Data Kantor: Mengoptimalkan Keamanan Informasi. Jurnal Transformasi Bisnis Digital, 1(3), 13–27. https://doi.org/10.61132/jutrabidi.v1i2.108

Mahendra Adhi Nugroho, Sri Wulan Asih, & Anisah Novi Karunia. (2024). PERAN KESADARAN MANUSIA DALAM KEAMANAN INFORMASI DAN SOCIAL ENGINEERING. Bureaucracy Journal : Indonesia Journal of Law and Social-Political Governance, 4.

Sinaga, R., & Taan, F. (2024). Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala. NUANSA INFORMATIKA, 18(2), 46–54. https://doi.org/10.25134/ilkom.v18i2.205

Sitompul, & Nasution. (2024). Pentingnya Kepatuhan Keamanan Informasi Dalam Mengurangi Risiko Data Breach. Maeswara : Jurnal Riset Ilmu Manajemen dan Kewirausahaan, 2(1), 99–107. https://doi.org/10.61132/maeswara.v2i1.587