Evaluasi Keamanan Sistem Informasi Manajemen Di Lingkungan Bisnis Digital

**Gading Islami¹, Alnayla Earthza Wilansky², Alifia Jurien Wilansky³, Sandra Lesmana⁴,
Muhamad Ihsan Fauzi⁵, Samsoni⁷, Aprinia Handayani⁸**

¹Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
Email: 1Gadingislami12@gmail.com, 2naylawilansky@gmail.com, 3alifiajurienwilansky@gmail.com, 4sandralesmana0201@gmail.com, 5muhammadihsanfauzi11@gmail.com, 6dosen00388@gmail.com, 7dossen02719@gmail.com

Abstrak—Evaluasi keamanan sistem merupakan proses yang krusial dalam mengidentifikasi, menganalisis, dan mengatasi potensi kerentanan dalam suatu sistem informasi. Tujuan utama dari evaluasi ini adalah untuk memastikan bahwa sistem mampu melindungi data dan sumber daya dari ancaman yang mungkin muncul, baik dari dalam maupun luar organisasi. Proses evaluasi keamanan mencakup penilaian risiko, pengujian penetrasi, audit keamanan, dan analisis kepatuhan terhadap standar keamanan yang berlaku. Hasil dari evaluasi ini memberikan dasar yang kuat untuk pengembangan strategi mitigasi risiko dan peningkatan keamanan yang berkelanjutan. Penelitian ini mengeksplorasi metode dan alat yang digunakan dalam evaluasi keamanan sistem serta dampaknya terhadap keseluruhan postur keamanan organisasi.

Kata Kunci: Evaluasi Keamanan Sistem, Penilaian Risiko, Pengujian Penetrasi, Audit Keamanan, Analisis Kepatuhan, Mitigasi Risiko, Keamanan Informasi, Postur Keamanan

Abstract—*System security evaluation is a crucial process in identifying, analyzing, and addressing potential vulnerabilities in an information system. The main objective of this evaluation is to ensure that the system can protect data and resources from possible threats, both internal and external to the organization. The security evaluation process includes risk assessment, penetration testing, security audits, and compliance analysis with applicable security standards. The results of this evaluation provide a solid foundation for developing risk mitigation strategies and continuous security improvements. This research explores the methods and tools used in system security evaluation and their impact on the overall security posture of the organization.*

Keywords: *System Security Evaluation, Risk Assessment, Penetration Testing, Security Audit, Compliance Analysis, Risk Mitigation, Information Security, Security Posture*

1. PENDAHULUAN

1.1 Latar Belakang

Evaluasi keamanan sistem informasi manajemen (SIM) di lingkungan bisnis digital merupakan proses kritis untuk memastikan perlindungan data dan keberlanjutan operasional perusahaan.

ISO 27001 adalah standar internasional yang paling dikenal untuk sistem manajemen keamanan informasi (ISMS). (Titus Kristanto, Mohammad Sholik, Dewi Rahmawati, 2019) Standar ini memberikan panduan untuk menetapkan, mengimplementasikan, memelihara, dan terus meningkatkan ISMS. Penerapan ISO 27001 membantu perusahaan melakukan penilaian risiko yang menyeluruh dan menciptakan rencana penanganan risiko yang praktis, sehingga perusahaan lebih siap mengidentifikasi dan mencegah risiko kebocoran sebelum terjadi. (Hoffman, 2018)

Proses evaluasi melibatkan penilaian risiko yang komprehensif, di mana perusahaan mengidentifikasi potensi ancaman dan kerentanan dalam sistem informasi mereka. Selain itu, audit keamanan secara berkala diperlukan untuk memastikan kepatuhan terhadap kebijakan keamanan dan standar industri. Audit ini juga membantu mengidentifikasi area yang memerlukan peningkatan dalam strategi keamanan siber perusahaan. (Mokodompit & Nurlaela, 2017)

Evaluasi keamanan yang efektif tidak hanya meningkatkan postur keamanan perusahaan tetapi juga membangun kepercayaan pelanggan. Pelanggan yang merasa datanya aman cenderung lebih loyal dan memiliki hubungan jangka panjang dengan perusahaan. Selain itu, reputasi perusahaan juga mendapat dorongan positif ketika berhasil mempertahankan catatan keamanan yang kuat. (Amirinnisa¹ & Bisma², 2023)

2. METODE

A. Metode Penelitian

Penelitian ini menggunakan beberapa metode untuk mengumpulkan dan menganalisis data, termasuk studi literatur, survei, pengujian penetrasi, dan audit keamanan. Berikut adalah penjelasan singkat untuk setiap metode:

1. Studi Literatur

Mengkaji berbagai sumber literatur untuk mengidentifikasi tren, tantangan, dan solusi dalam evaluasi keamanan SIM.

2. Survei

Mengumpulkan data dari manajer IT dan profesional keamanan di berbagai perusahaan untuk memahami praktik dan persepsi terkait keamanan SIM.

3. Pengujian Penetrasi

Melakukan simulasi serangan siber untuk mengidentifikasi kerentanan dalam sistem informasi.

4. Audit Keamanan

Evaluasi sistematis terhadap kebijakan, prosedur, dan kontrol keamanan yang diterapkan dalam SIM perusahaan.

B. Metode Pengumpulan Data

Dalam penelitian ini, metode pengumpulan data terdiri dari observasi, wawancara, dan dokumentasi. (Adi Saputra et al., 2023) Data dikumpulkan melalui dokumen yang berkaitan dengan penerapan sistem manajemen keamanan aset informasi perusahaan berbasis ISO 27001, sedangkan wawancara mengumpulkan informasi dari persepsi dan pendapat responden tentang implementasi sistem tersebut. Observasi dilakukan secara partisipatif dengan mengikuti aktivitas yang berkaitan dengan implementasi sistem. (Sofianda et al., 2023)

3. ANALISA DAN PEMBAHASAN

1. Metode dan Alat dalam Evaluasi Keamanan SIM

- ISO 27001: Standar ini menawarkan kerangka kerja menyeluruh untuk mengelola keamanan informasi. Implementasi ISO 27001 melibatkan penilaian risiko, pengembangan kebijakan keamanan, dan audit berkala untuk memastikan kepatuhan terhadap standar. (Alim et al., 2024)
- Pengujian Penetrasi: Teknik ini penting untuk mengidentifikasi kerentanan yang tidak terlihat dalam penilaian risiko biasa. Pengujian penetrasi memberikan gambaran nyata tentang seberapa efektif langkah-langkah keamanan yang ada.
- Audit Keamanan: Evaluasi berkala terhadap kebijakan dan kontrol keamanan membantu memastikan bahwa langkah-langkah keamanan tetap efektif dan sesuai dengan perkembangan ancaman siber.

2. Dampak Evaluasi Keamanan terhadap Postur Keamanan dan Kepercayaan Pelanggan

- Postur Keamanan: Evaluasi keamanan yang menyeluruh meningkatkan kemampuan perusahaan untuk mendeteksi dan merespons ancaman siber. Ini termasuk penguatan kontrol akses, enkripsi data, dan pemantauan terus-menerus terhadap aktivitas jaringan.
- Kepercayaan Pelanggan: Pelanggan cenderung lebih percaya pada perusahaan yang transparan tentang langkah-langkah keamanan mereka dan yang menunjukkan

kepatuhan terhadap standar industri. Kepercayaan ini penting untuk membangun loyalitas pelanggan dan hubungan jangka panjang.

3. Rekomendasi untuk Meningkatkan Keamanan SIM

- Implementasi ISO 27001: Mengadopsi standar ini untuk membangun dan memelihara sistem manajemen keamanan informasi yang komprehensif.
- Peningkatan Keamanan Jaringan: Menggunakan firewall, sistem deteksi intrusi, dan enkripsi data untuk melindungi jaringan dari akses yang tidak sah.
- Pelatihan Kesadaran Keamanan: Memberikan pelatihan reguler kepada karyawan tentang praktik terbaik keamanan siber.
- Pengujian dan Audit Berkala: Melakukan pengujian penetrasi dan audit keamanan secara berkala untuk memastikan bahwa langkah-langkah keamanan tetap efektif.

Hasil Penelitian

1. Identifikasi Kerentanan

Pengujian penetrasi mengungkapkan beberapa kerentanan dalam sistem yang dapat dieksploitasi oleh penyerang, seperti kelemahan dalam konfigurasi jaringan dan perangkat lunak yang tidak diperbarui. (Wijaya, 2021)

2. Analisis Risiko

Analisis risiko menunjukkan bahwa data pelanggan dan informasi keuangan adalah aset yang paling rentan terhadap serangan siber. Kepatuhan terhadap regulasi seperti GDPR dan ISO 27001 sangat penting untuk mengurangi risiko ini.

3. Dampak Evaluasi Keamanan

Evaluasi keamanan yang efektif meningkatkan postur keamanan perusahaan dan membangun kepercayaan pelanggan. Pelanggan yang merasa datanya aman cenderung lebih loyal dan memiliki hubungan jangka panjang dengan perusahaan.

4. KESIMPULAN

Evaluasi keamanan sistem informasi manajemen di lingkungan bisnis digital adalah proses yang berkelanjutan dan memerlukan pendekatan yang komprehensif. Dengan mengadopsi standar industri, mengimplementasikan kontrol keamanan yang kuat, dan melakukan evaluasi berkala, perusahaan dapat melindungi data mereka dari ancaman siber dan membangun kepercayaan pelanggan. Implementasi rekomendasi yang diberikan dalam laporan ini diharapkan dapat membantu perusahaan meningkatkan keamanan SIM mereka dan mencapai keberhasilan jangka panjang dalam lingkungan bisnis digital.

REFERENCES

- Adi Saputra, L., Muhammad Akbar, F., Cahyaningtias, F., Puspa Ningrum, M., & Fauzi, A. (2023). Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan. *Jurnal Pendidikan Siber Nusantara*, 1(2), 58–66. <https://doi.org/10.38035/jpsn.v1i2.48>
- Alim, M., Rasyid Munthe, I., & Putra Juledi, A. (2024). Evaluasi Keamanan Sistem Informasi dalam Lingkungan Bisnis Digital. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, 7(1), 328–332. <https://doi.org/10.55338/jikomsi.v7i1.3088>
- Amirinnisa¹, M., & Bisma², R. (2023). Analisis Penilaian Risiko Keamanan Informasi Berdasarkan Iso 27005 Untuk Persiapan Sertifikasi Iso 27001 pada Pemerintah Kota Madiun. *Jeisbi*, 04(04), 47–58.
- Hoffman, D. W. (2018). *EVALUASI KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE INDEKS KEAMANAN INFORMASI (KAMI VERSI 3.1) (STUDI KASUS: DINAS KOMUNIKASI DAN INFORMATIKA PEMERINTAH DAERAH XYZ)*.
- Mokodompit, M. P., & Nurlaela, N. (2017). Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000 (Studi Kasus Pada Peguruan Tinggi X). *Jurnal Sistem Informasi Bisnis*, 6(2), 97. <https://doi.org/10.21456/vol6iss2pp97-104>

- Sofianda, W., Habibi Ritonga, S., & Buyung Nasution, A. (2023). Evaluasi Manajemen Keamanan Sistem Informasi Pada Perusahaan PT.Wook Tecnology. *JurnalJurnal Sains Dan Teknologi (JSIT)*, 3(1), 101–108.
- Titus Kristanto, Mohammad Sholik, Dewi Rahmawati, M. N. (2019). Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ. *Jurnal Informatika Dan Sains*.
https://www.researchgate.net/publication/339068517_Analisis_Manajemen_Keamanan_Informasi_Menggunakan_Standard_ISO_270012005_Pada_Staff_IT_Support_Di_Instansi_XYZ
- Wijaya, Y. D. (2021). Evaluasi Kemananan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) Iso/Iec 27001:2013. *Jurnal Sistem Informasi Dan Informatika (Simika)*, 4(2), 115–130.
<https://doi.org/10.47080/simika.v4i2.1178>