TEKNOBIS : Jurnal Teknologi, Bisnis dan Pendidikan
Volume 1, No. 2 Agustus 2023
ISSN 3024-8256 (media online)
Hal

Keamanan Data dalam Sistem Informasi Manajemen: Risiko dan Strategi Perlindungan

Agung Wijoyo S.S.Kom.,M.Kom[1], Siti Fatimah[2],Toni[3], Yana Widianti[4], Mukhlis Fadillah[5]

Ekonomi dan bisnis, Manajemen SDM, UNIVERSITAS PAMULANG , Tangrang Selatan, Indonesia

Email : dosen01671@gmail.com , sitifatimah22siifat@gmail.com , yanawidianti6@gmail.com

Abstrak- Data merupakan salah satu aset penting dan berharga baik bagi individu maupun organisasi. Dalam Sistem Informasi Manajemen (SIM), data yang disimpan dapat berupa data keuangan, data pelanggan, data karyawan, dan data penting lainnya. Oleh karena itu, keamanan data dalam SIM sangat penting untuk melindungi informasi dari ancaman seperti pencurian data, kerusakan fisik terhadap sistem informasi, dan ancaman lainnya. Artikel ini bertujuan untuk membahas tentang keamanan data dalam SIM, risiko yang dapat terjadi pada keamanan data, dan strategi perlindungan yang dapat dilakukan untuk mengatasi risiko tersebut. Keamanan data dalam sistem informasi manajemen adalah upaya untuk melindungi, mengamankan aset informasi dari ancaman yang mungkin akan timbul yang dapat membahayakan kerahasiaan, ketersediaan, dan integritas semua aset informasi perusahaan, bukan hanya perangkat keras dan lunak, tetapi juga data sensitif yang disimpan di dalamnya Keamanan data dalam Sistem Informasi Manajemen adalah aspek yang kritis untuk setiap organisasi. Risiko keamanan data dapat berasal dari berbagai sumber, dan dampaknya bisa sangat serius. Saran-saran praktis untuk mengatasi risiko keamanan data dalam SIM yaitu Keamanan Siber Utama, Kesadaran Karyawan, Solusi Keamanan Jaringan, Rencana Pemulihan Data, Audit Kepatuhan, dan Evaluasi Berkala.

Kata Kunci : *Sistem Informasi Manajemen (SIM), Keamanan Data, Risiko dan Strategi Perlindungan.*

PENDAHULUAN

Data merupakan salah satu aset penting dan berharga baik bagi individu maupun organisasi. Dalam Sistem Informasi Manajemen (SIM), data yang disimpan dapat berupa data keuangan, data pelanggan, data karyawan, dan data penting lainnya. Oleh karena itu, keamanan data dalam SIM sangat penting untuk melindungi informasi dari ancaman seperti pencurian data, kerusakan fisik terhadap sistem informasi, dan ancaman lainnya.

Dalam era digital saat ini, ancaman terhadap keamanan data semakin meningkat. Pencurian data, serangan virus dan malware, serta kesalahan manusia dapat membahayakan keamanan data

dalam SIM. Oleh karena itu, perlu dilakukan strategi perlindungan yang tepat untuk mengatasi risiko tersebut.

Artikel ini bertujuan untuk membahas tentang keamanan data dalam SIM, risiko yang dapat terjadi pada keamanan data, dan strategi perlindungan yang dapat dilakukan untuk mengatasi risiko tersebut, juga membahas tentang pentingnya menjaga keamanan data dalam SIM dan hal-hal yang perlu diperhatikan dalam menjaga keamanan data.

TEKNOBIS : Jurnal Teknologi, Bisnis dan Pendidikan
Volume 1, No. 2 Agustus 2023
ISSN 3024-8256 (media online)
Hal

TINJAUAN PUSTAKA

Pengertian Sistem Informasi Manajemen

Menurut Slamet Hariyanto dalam (Hariyanto, 2016). Manajemen itu sendiri meliputi perencanaan, pengorganisasian, pemantauan, pengarahan, dan proses lainnya dalam organisasi. Informasi dalam suatu organisasi, di sisilain, adalah data yang diproses dengan cara yang berharga dan bermakna bagi organisasi. Menurut Miyarso Dwi Ajie dalam (Ajie, 1375). Sistem informasi manajemen bukanlah hal baru. Ruang lingkup SIM sebenarnya terkandung dalam tiga kata yang membentuk SIM: "sistem", "informasi", dan "manajemen".

Sistem adalah kumpulan dari elemen-elemen yang saling berhubungan. Elemen-elemen sistem adalah departemen internal seperti gudang bahan baku, gudang produk jadi, produksi, promosi dan penjualan, dan pihak eksternal seperti pemasok dan konsumen yang saling terkait. Informasi adalah hasil pengolahan data yang diperoleh dari setiap elemen sistem ke dalam format yang mudah dimengerti dan mewakili pengetahuan yang relevan yang dibutuhkan orang untuk meningkatkan pengetahuan mereka tentang fakta-fakta yang ada. Manajemen terdiri dari proses kegiatan yang dilakukan oleh para pemimpin bisnis, seperti: perencanaan, pengorganisasian koordinas, dan pengendalian operasi untuk mencapai tujuan yang telah ditetapkan.

Dari ruang lingkup di atas, beberapa definisi sistem informasi manajemen menurut para ahli adalah sebagai berikut:

1. Menurut Jogiyanto Hartono (2000:700), istilah sistem informasi terkelola adalah kumpulan sistem informasi yang saling berinteraksi yang bertanggung jawab untuk pemrosesan dan pengumpulan data, menyediakan informasi yang berguna untuk mengelola semua tingkat kegiatan perencanaan dan pengendalian.
2. Menurut Joel D. Aron (buku E.S. Margianti), Pengertian Sistem Informasi Manajemen adalah sistem informasi yang menyediakan

   informasi yang dibutuhkan manajer untuk mengambil keputusan.

Pengertian Keamanan Data dalam Sistem Informasi Manajemen

Keamanan data dalam sistem informasi manajemen adalah upaya untuk melindungi, mengamankan aset informasi dari ancaman yang mungkin akan timbul yang dapat membahayakan kerahasiaan, ketersediaan, dan integritas semua aset informasi perusahaan, bukan hanya perangkat keras dan lunak, tetapi juga data sensitif yang disimpan di dalamnya Keamanan data dalam sistem informasi manajemen meliputi kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman seperti pencurian data, penggunaan sistem secara ilegal, penghancuran data secara ilegal, modifikasi, akses tidak sah, dan kerusakan terhadap sistem.

Untuk meningkatkan keamanan data dalam sistem informasi manajemen, perusahaan dapat menerapkan strategi perlindungan seperti menggunakan langkah-langkah dan alat keamanan siber untuk melindungi data sensitif dari akses yang tidak sah, menerapkan kerangka kerja keamanan siber yang komprehensif, menerapkan enkripsi dan praktik keamanan lainnya untuk melindungi data pribadi, mengimplementasikan regulasi perlindungan data pribadi, dan menjaga

keberlangsungan bisnis dengan menjaga keamanan data.

Pentingnya Keamanan Sistem Informasi Manajemen

Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat essensial bagi suatu organisasi, baik yang berupa organisasi komersial

(perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Keamanan informasi menggambarkan usaha untuk melindungi komputer dan non peralatan komputer, fasilitas,data,dan informasi dari penyalahgunaan oleh orang yang tidak bertanggungjawab. Keamanan informasi dimaksudkan untuk mencapai kerahasiaan, ketersediaan, dan integritas di dalam sumber daya informasi dalam suatu perusahaan.

Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi. Keamanan informasi dimaksudkan untuk mencapai tiga sasaran utama yaitu:

1. Melindungi data dan informasi perusahaan dari penyingkapan orang- orang yang tidak berhak. Inti utama dari aspek kerahasiaan adalah usaha untuk menjaga informasi dari orang- orang yang tidak berhak mengakses. Privacy lebih kearah data-data yang sifatnya privat. Serangan terhadap

   aspek privacy misalnya usaha untuk melakukan penyadapan. Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy adalah dengan menggunakan teknologi kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentikasi data.

2. Ketersediaan. Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi benar-benar asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Masalah pertama untuk membuktikan keaslian dokumen dapat dilakukan dengan teknologi watermarking dan digital signature.Watermarking juga dapat digunakan untuk menjaga intelektual property, yaitu dengan menandatangani dokumen atau hasil karya pembuat. Masalah kedua biasanya berhubungan dengan akses control, yaitu berkaitan dengan pembatasan orang-orang yang dapat mengakses informasi. Dalam hal ini pengguna harus menunjukkan bahwa memang dia adalah pengguna yang sah atau yang berhak menggunakannya.

3. Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa izin. Sistem informasi perlu menyediakan representasi yang akurat dari sistem fisik yang direpresentasikan.

Sepuluh Cara Menjaga Keamanan Sistem IT, sebagai berikut ini:

1. Protect with passwords. Semua akses ke jaringan maupun data, sangat sensitif dan harus dijaga dengan nama pengguna dan kata kunci yang unik. Sandi yang kuat berisi angka, huruf dan simbol.

2. Design safe systems. Hilangkan akses yang tidak perlu ke hardware maupun software Anda, dan batasi hak akses pengguna hanya untuk peralatan dan program yang dibutuhkan saja.

3. Conduct screening and background checks. Melakukan skrining dan pemeriksaan latar belakang pada karyawan perlu dilakukan.

4. Provide basic training. Pelanggaran keamanan yang tak terhitung jumlahnya kerap terjadi sebagai akibat kesalahan dan kecerobohan manusia.

5. Avoid unknown email attachements. Jangan pernah mengklik lampiran email yang tidak dikenal, yang

   kemungkinan bisa berisi virus komputer.

6. Hang up and call back. Jika Anda menerima panggilan dari orang yang tidak dikenal yang tiba-tiba ingin memberikan hadiah dan berpura-pura hadiah itu diberikan oleh perwakilan dari bank atau mitra lainnya, segera akhiri panggilan yang tidak dikenal tersebut.

7. Think before clicking. Untuk menghindari penipuan yang terjadi melalui email yang

meminta informasi nama pengguna, kata sandi atau informasi pribadi, Anda harus mempertimbangkannya kembali agar Anda tidak terdorong ke sebuah situs web palsu yang mendorong calon korban untuk memasukkan data mereka sendiri.

8. Use a virus scanner, and keep all software up-to-date. Menjaga perangkat lunak agar terus up-to- datejuga mampu mencegah virus masuk dan membuat keamanan sistem IT terjaga.
9. Keep sensitive data out of the cloud. Cloud computingmenawarkan banyak manfaat dan penghematan biaya kepada bisnis.
10. Stay paranoid. Jangan pernah meninggalkan laporan yang bersifat penting dan sensitif di meja Anda.

Risiko Keamanan Data dalam Sistem Informasi Manajemen

1. Risiko Pelanggaran Data

   Salah satu risiko terbesar yang dihadapi organisasi dalam SIM adalah pelanggaran data. Pelanggaran data terjadi ketika data sensitif seperti informasi pelanggan, informasi keuangan, atau data pribadi dicuri atau diakses oleh pihak yang tidak berwenang. Pelanggaran data dapat memiliki dampak serius, termasuk hilangnya kepercayaan pelanggan, kerugian finansial, dan bahkan tindakan hukum.

2. Risiko Serangan Perangkat Lunak Jahat

   Serangan perangkat lunak jahat, seperti virus, worm, ransomware, dan trojan horse, dapat merusak atau mencuri data dalam SIM. Serangan ini dapat terjadi melalui email phishing, situs web yang tidak aman, atau perangkat USB yang terinfeksi. Serangan perangkat lunak jahat merupakan ancaman konstan bagi keamanan data.

3. Risiko Serangan DDoS

   Serangan Denial of Service (DDoS) adalah serangan di mana penyerang mencoba membuat layanan SIM menjadi tidak tersedia dengan membanjiri sistem dengan lalu lintas internet palsu. Ini dapat

mengakibatkan gangguan serius dalam operasional perusahaan, terutama jika bisnis sangat bergantung pada SIM untuk operasi sehari-hari.

4. Risiko Ancaman Insider

   Ancaman dari dalam organisasi, baik itu disengaja atau tidak, merupakan risiko lain yang signifikan. Karyawan yang tidak jujur atau kurangnya pelatihan keamanan data dapat menyebabkan pelanggaran data atau kerusakan sistem dari dalam.

5. Risiko Ketidakpatuhan Regulasi

   Organisasi sering kali harus mematuhi berbagai regulasi dan kebijakan yang berkaitan dengan keamanan data, seperti GDPR di Eropa atau HIPAA di Amerika Serikat. Pelanggaran regulasi ini dapat mengakibatkan sanksi hukum dan denda yang signifikan.

Strategi Perlindungan Data

1. Enkripsi Data

   Salah satu langkah pertama dalam melindungi data dalam SIM adalah dengan menggunakan enkripsi. Data sensitif harus dienkripsi saat disimpan dan dalam perjalanan antara sistem. Enkripsi mengubah data menjadi format yang

tidak dapat dibaca tanpa kunci enkripsi yang benar.

2. Firewall dan Keamanan Jaringan

   Penggunaan firewall dan perangkat keamanan jaringan lainnya adalah langkah penting dalam mengamankan SIM. Firewall dapat membantu melindungi sistem dari serangan luar dan memantau lalu lintas yang mencurigakan.

3. Pembaruan Rutin

   Sistem SIM harus selalu diperbarui dengan patch keamanan terbaru. Serangan sering kali terjadi karena sistem yang tidak diperbarui memiliki kerentanan yang dapat dieksploitasi.

4. Manajemen Akses

   Manajemen akses adalah praktik penting dalam melindungi data. Organisasi harus memastikan bahwa hanya individu yang membutuhkan akses yang memiliki izin untuk mengakses data tersebut. Autentikasi yang kuat dan penggunaan kata sandi yang aman juga diperlukan.

5. Pelatihan Karyawan

   Karyawan harus dilatih dalam praktik keamanan data yang baik. Mereka harus menyadari risiko insider dan tahu cara menghindarinya, seperti dengan mengidentifikasi email phishing

   atau melaporkan perilaku mencurigakan.

6. Pemantauan Aktivitas

   Pemantauan dan deteksi ancaman adalah komponen penting dalam strategi perlindungan data. Sistem pemantauan dapat membantu organisasi mengidentifikasi serangan atau aktivitas mencurigakan dengan cepat, memungkinkan tindakan yang lebih cepat.

7. Pengelolaan Risiko

   Organisasi harus secara teratur melakukan evaluasi risiko dan mengembangkan rencana respons terhadap risiko yang diidentifikasi. Ini membantu dalam mengelola risiko dengan lebih efektif.

Jenis-jenis Keamanan Sistem Informasi Manajemen

Berikut adalah beberapa jenis keamanan sistem informasi yang perlu diperhatikan:

1. Application security: mencakup kerentanan software di aplikasi web dan mobile serta programming interfaces (APIs). Kerentanan ini biasa ditemukan di otentikasi atau otorisasi pengguna. Selain itu, bisa pula ditemukan di integritas kode dan konfigurasi, serta kebijakan dan prosedur
2. Cloud security: Sebuah sistem yang dibuat untuk meningkatkan keamanan dari sebuah data, aplikasi, atau infrastruktur komputasi lainnya yang terhubung dengan cloud.
3. Kriptografi: teknik penyandian data sehingga informasi rahasia seperti nomor kartu kredit atau kontrol autentikasinya tidak dapat dibaca oleh orang yang tidak berwenang
4. Keamanan Infrastruktur: mencakup perlindungan terhadap perangkat keras dan lunak, jaringan, dan sistem operasi
5. Respons insiden: mencakup proses dan kebijakan untuk menangani insiden keamanan siber yang terjadi
6. Manajemen kerentanan: mencakup proses untuk mengidentifikasi, mengevaluasi, dan mengurangi kerentanan yang ada di dalam sistem.

7. Firewall: merupakan sistem keamanan jaringan yang digunakan untuk membatasi akses ke jaringan dan mengontrol lalu lintas data
8. Pencegahan Kehilangan Data (DLP): alat untuk melindungi data sensitif dari insiden kehilangan atau pencurian oleh orang yang tidak berwenang
9. Analisis Perilaku: jenis keamanan jaringan yang dirancang untuk mencegah perangkat yang tidak dikenal mengakses jaringan

Dalam menjaga keamanan sistem informasi, perusahaan perlu memperhatikan jenis-jenis keamanan sistem informasi yang ada dan menerapkan strategi perlindungan yang sesuai untuk mencegah terjadinya ancaman keamanan siber dan melindungi data sensitif dari akses yang tidak sah.

KESIMPULAN

Keamanan data dalam Sistem Informasi Manajemen adalah aspek yang kritis untuk setiap organisasi. Risiko keamanan data dapat berasal dari berbagai sumber, dan dampaknya bisa sangat serius. Oleh karena itu, organisasi perlu mengidentifikasi risiko-risiko ini dan mengimplementasikan strategi perlindungan yang sesuai. Dengan demikian, organisasi dapat melindungi data berharga mereka, menjaga kepercayaan pemangku kepentingan, dan menghindari kerugian finansial yang tidak perlu. Keamanan data dalam SIM adalah investasi yang penting untuk masa depan yang sukses.

Saran-saran praktis untuk mengatasi risiko keamanan data dalam SIM:

1. Keamanan Siber Utama: Prioritaskan perlindungan dari serangan siber dengan investasi dalam perangkatlunak keamanan dan pelatihan karyawan.
2. Kesadaran Karyawan: Tingkatkan kesadaran karyawan tentang risiko keamanan melalui pelatihan berkala.
3. Solusi Keamanan Jaringan: Aktifkan perlindungan jaringan seperti firewall, enkripsi, dan pemantauan untuk mencegah serangan siber.
4. Rencana Pemulihan Data: Buat dan uji rencana pemulihan data yang kuat serta lakukan backup data secara berkala.
5. Audit Kepatuhan: Lakukan audit rutin untuk memastikan kepatuhan dengan regulasi privasi data yang berlaku.
6. Evaluasi Berkala: Selalu tinjau dan perbarui strategi keamanan sesuai dengan perkembangan risiko dan teknologi.

DAFTAR PUSTAKA

Hariyanto, S. (2016). Sistem Informasi Manajemen. Publiciana, 9(1), 80-85.

Jakaria, D. A., & Dirgahayu, R. T. (2013, June). Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro. In Seminar Nasional Aplikasi Teknologi Informasi (SNATI).

Baali, Y., Sasewa, D. R., Sjioen, A. E., Rejeki, S., Wahyuarini, T., Saputra, Y. M. D., ... & Sudirjo, F. (2023). SISTEM INFORMASI MANAJEMEN: KONSEP DAN APLIKASI

BISNIS. Get Press ndonesia.

Zen Munawar, S. T., Kom, S., Kom, M.,Putri, N. I., Kharisma, I. L., Kom,M., ... & MM, M. (2023). KEAMANAN SISTEM INFORMASI: Prinsip Dasar, Teori, dan Rekayasa Penerapan Konsep. Kaizen Media Publishing.Ardhiansyah, M., Rahayu, S., & Rahmawati, R. (2022). KEAMANAN KOMPUTER.

Nasution, D. S., Aminy, M. M., & Ramadani, L. A. (2019). Ekonomi Digital. Sanabil.

Ardana, P. D. H. (2023). SISTEM INFORMASI REHABILITASI DAN REKONSTRUKSI PASCA BENCANA BERBASIS WEB.

Wahyuni, S. (2022). Bab V Literasi Digital dan Media Sosial dalam Pembelajaran. Literasi Digital Berbasis Pendidikan, 59.