Maeswara: Jurnal Riset Ilmu Manajemen dan Kewirausahaan
Vol. 2 No. 1 Februari 2024
e-ISSN: 2988-5000; p-ISSN: 2988-4101, Hal 99-107
DOI: https://doi.org/10.61132/maeswara.v2i1.587

Pentingnya Kepatuhan Keamanan Informasi Dalam Mengurangi Risiko Data Breach

Ripa Sabila Usni Sitompul
Program Studi Manajemen, Fakultas Ekonomi Dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara

Muhammad Irwan Padli Nasution
Program Studi Manajemen, Fakultas Ekonomi Dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara

Korespondensi penulis: rifasabila03@gmail.com

Abstract. *This research aims to find out how vital information security compliance is in reducing the risk of Data Breach. The method used in this research is Library Research (Library) which is the method used in this writing, and in its use, this method uses books, and journals both in written form and online. Based on the results obtained from this research, it can be concluded that a Data Breach is an incident where sensitive data or important information becomes vulnerable or is accessed by unauthorized parties. To prevent a Data Breach, organizations need to take various security measures, policies, and practices, such as encryption, access management, physical security, network security, security training and awareness, security policies, and monitoring and auditing. Sensitive data protection helps maintain the confidentiality, integrity, and availability of data and protects the reputation and trust of customers and business partners. By implementing good sensitive data protection, organizations can reduce the risk of data breaches which can be financially detrimental and damage the company's image.*

Keywords*: Data Breach, Information Security, Information Systems*

Abstrak. Penelitian ini bertujuan untuk mengetahui betapa vitalnya kepatuhan keamanan informasi dalam mengurangi risiko Data Breach. Metode yang digunakan dalam penelitian ini adalah Library Research (Kepustakaan) menjadi metode yang digunakan dalam penulisan ini, dan dalam penggunaannya metode ini menggunakan buku-buku, jurnal baik berbentuk tulisan maupun online. Berdasarkan hasil yang didapatkan dari penelitian ini dapat disimpulkan kalau Data Breach merupakan insiden di mana data sensitif atau informasi penting menjadi rentan atau diakses oleh pihak yang tidak berwenang. Untuk mencegah Data Breach, organisasi perlu mengambil berbagai tindakan, kebijakan, dan praktik keamanan, seperti enkripsi, manajemen akses, keamanan fisik, keamanan jaringan, pelatihan dan kesadaran keamanan, kebijakan keamanan, serta pemantauan dan audit. Perlindungan data sensitif membantu menjaga kerahasiaan, integritas, dan ketersediaan data serta melindungi reputasi dan kepercayaan pelanggan dan mitra bisnis. Dengan menerapkan perlindungan data sensitif yang baik, organisasi dapat mengurangi risiko data breach yang dapat merugikan secara finansial dan merusak citra perusahaan.

Kata kunci: Data Breach, Keamanan Informasi, Sistem Informasi

Received November 19, 2023; Accepted Desember 19, 2023; Published Februari 29, 2024
* Ripa Sabila Usni Sitompul, *rifasabila03@gmail.com*

LATAR BELAKANG

Dalam era digital yang semakin maju, perusahaan dan organisasi di seluruh dunia semakin tergantung pada teknologi informasi untuk menyimpan, mengelola, dan mengakses data sensitif. Namun, kebergantungan ini juga membawa risiko yang signifikan, terutama dalam bentuk serangan siber yang dapat mengakibatkan data breach. Data breach adalah insiden di mana data rahasia atau pribadi yang disimpan oleh sebuah organisasi diakses, diungkapkan, atau dicuri oleh pihak yang tidak berwenang.

Ancaman siber telah berkembang sangat pesat beberapa tahun belakangan ini, dengan penjahat siber semakin terampil dalam mencari celah keamanan dan memanfaatkannya untuk keuntungan mereka sendiri. Serangan siber yang berhasil dapat menyebabkan kerugian besar, seperti pencurian data pribadi pengguna, kehilangan reputasi, dan dampak finansial yang serius. Ini menjadi salah satu tantangan terbesar dalam dunia digital saat ini.

Selain risiko finansial dan reputasi, ada juga tekanan hukum yang semakin meningkat. Banyak yurisdiksi sekarang memiliki regulasi ketat yang mengharuskan perusahaan untuk menjaga keamanan data pelanggan dan pengguna. Ketidakpatuhan dapat mengakibatkan denda yang substansial dan tuntutan hukum yang merugikan.

Dalam beberapa tahun terakhir, kita telah melihat beberapa data breach besar dan terkenal yang telah mengguncang perusahaan besar dan bahkan negara. Sebagai contoh, pada tahun 2017, perusahaan kredit Equifax mengalami data breach yang mengungkapkan informasi pribadi dari lebih dari 143 juta individu. Kasus serupa terjadi pada perusahaan besar lainnya seperti Target dan Facebook.

Namun, tidak semua harapan hilang. Kepatuhan keamanan informasi telah muncul sebagai strategi utama dalam mengurangi risiko data breach. Ini mencakup penerapan langkah-langkah keamanan yang ketat, pelatihan karyawan, dan penggunaan teknologi keamanan informasi terkini. Kesadaran karyawan juga menjadi sangat penting, karena seringkali serangan dimulai dengan tindakan kelalaian atau tindakan tidak bijak dari anggota tim internal.

METODE PENELITIAN

Library Research (Kepustakaan) menjadi metode yang digunakan dalam penulisan ini, dan dalam penggunaannya metode ini menggunakan buku-buku, jurnal baik berbentuk tulisan maupun online. Menurut sugiyono dalam buku penelitiannya dijelaskan bahwa Library Research adalah cara yang dilakukan dalam mengumpulkan data penelitian dari berbagai

informasi kepustakaan melalui analisis hasil penelitian, buku refrensi, artikel lainnya, dan sumber-sumber yang mendukung.

HASIL DAN PEMBAHASAN

Kepatuhan keamanan informasi sangat penting dalam mengurangi risiko data breach (pelanggaran data) dan menjaga integritas, kerahasiaan, dan ketersediaan data organisasi. Berikut adalah beberapa alasan mengapa kepatuhan keamanan informasi penting dalam mengurangi risiko data breach:

1. Perlindungan Data Sensitif

Kepatuhan keamanan informasi membantu organisasi untuk mengidentifikasi dan melindungi data yang sensitif. Ini termasuk data pelanggan, data keuangan, informasi pribadi, dan lainnya karena jika jatuh ke tangan yang salah bisa digunakan untuk tujuan yang tidak baik. Kepatuhan data sensitif merujuk pada praktik dan kebijakan yang harus diikuti untuk menjaga ketersediaan data, integritas, dan kerahasiaan yang dianggap sensitif. Data sensitif adalah data yang, jika jatuh ke tangan yang salah atau diakses oleh individu atau entitas yang tidak berhak, dapat menimbulkan dampak yang merugikan.

Data sensitif dapat mencakup informasi pribadi, informasi keuangan, rahasia bisnis, dan informasi lain yang memiliki nilai strategis atau potensi bahaya jika dicuri, diubah, atau disalahgunakan. Kepatuhan data sensitif sangat penting untuk melindungi data berharga dan mengurangi risiko pelanggaran data. Kehilangan atau pengungkapan data sensitif dapat memiliki konsekuensi serius, termasuk dampak hukum, kerugian finansial, dan kerusakan reputasi. Oleh karena itu, organisasi harus berinvestasi dalam kebijakan, praktik, dan teknologi yang mendukung kepatuhan data sensitif. Perlindungan data sensitif mencakup berbagai kebijakan, tindakan, dan praktik keamanan yang dirancang untuk menjaga kerahasiaan, integritas, dan ketersediaan data. Mengenkripsi data sensitif untuk melindungi data saat berpindah melalui jaringan atau disimpan dalam penyimpanan fisik.

Memberikan akses hanya kepada individu yang memerlukan data tersebut untuk tugas mereka. Ini melibatkan manajemen akses dan penggunaan izin akses. Melindungi perangkat keras dan penyimpanan fisik yang mengandung data sensitif dari akses yang tidak sah. Melindungi jaringan komputer dari serangan dengan menggunakan firewall, deteksi intrusi, dan tindakan keamanan jaringan lainnya. Melibatkan pelatihan karyawan untuk mengidentifikasi ancaman keamanan, tindakan keamanan yang diperlukan, dan tindakan pencegahan. Menerapkan kebijakan keamanan yang jelas dan prosedur yang harus diikuti oleh seluruh organisasi.

Melakukan pemantauan aktif terhadap kegiatan yang mencurigakan dan melakukan audit keamanan secara berkala.Data breach adalah insiden yang harus dihindari. Perlindungan data sensitif adalah serangkaian langkah yang diambil untuk mencegah terjadinya data breach dan menjaga keamanan data sensitif dari ancaman.

2. Pencegahan Akses Tidak Sah

Kepatuhan memerlukan praktik pengendalian akses yang ketat, seperti autentikasi ganda, manajemen hak akses, dan enkripsi data. Ini membantu mencegah akses tidak sah ke sistem dan data yang dapat menyebabkan data breach. Pencegahan akses tidak sah adalah tindakan untuk mencegah individu atau entitas yang tidak berhak dari mengakses data, sistem, atau sumber daya yang dilindungi. Ini merupakan langkah penting dalam menjaga keamanan informasi dan mengurangi risiko pelanggaran data. Pencegahan akses tidak sah adalah prasyarat penting dalam memastikan keamanan informasi dan melindungi data sensitif dari pelanggaran atau pencurian.

Organisasi perlu mengimplementasikan praktik keamanan yang ketat dan mengikuti standar keamanan informasi yang relevan untuk mengurangi risiko akses tidak sah yang dapat mengancam integritas dan kerahasiaan data mereka.

3. Deteksi Dini dan Respons Cepat

Kepatuhan biasanya mencakup prosedur deteksi dini dan respons cepat terhadap insiden keamanan. Dengan ini, organisasi dapat mengidentifikasi serangan atau pelanggaran data dengan cepat dan mengambil tindakan untuk menghentikan kerugian lebih lanjut. Deteksi dini dan respons cepat adalah elemen penting dalam mengurangi risiko pelanggaran data dan kehilangan informasi berharga. Hal ini mencakup proses dan teknologi yang digunakan untuk mendeteksi tanda-tanda aktivitas yang mencurigakan atau insiden keamanan, serta langkah-langkah yang diambil untuk menghadapinya dengan cepat.

Deteksi dini dan respons cepat merupakan komponen penting dalam siklus keamanan informasi yang kuat. Dengan pendekatan proaktif ini, organisasi dapat mengidentifikasi insiden keamanan lebih awal, mengurangi dampaknya, dan mencegah kerusakan yang lebih parah.

4. Kesadaran dan Pelatihan Karyawan

Kepatuhan keamanan informasi mendorong kesadaran keamanan di antara karyawan. Pelatihan dan kesadaran yang baik dapat membantu mencegah serangan phishing dan insiden terkait manusia lainnya, yang sering menjadi pintu masuk bagi pelanggaran data. Kesadaran

dan pelatihan karyawan dalam hal keamanan informasi sangat penting untuk menjaga keamanan data dan sistem organisasi. Kesadaran dan pelatihan karyawan adalah langkah-langkah yang bertujuan untuk membekali karyawan dengan pengetahuan dan pemahaman yang diperlukan untuk mengidentifikasi, menghindari, dan merespons ancaman keamanan informasi.

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.

5. Pemantauan dan Audit

Kepatuhan melibatkan pemantauan dan audit sistem dan praktik keamanan. Ini membantu organisasi untuk secara teratur mengevaluasi dan memperbarui kebijakan dan prosedur mereka, serta menemukan dan mengatasi potensi kerentanan sebelum mereka dieksploitasi oleh penyerang. Pemantauan dan audit adalah dua aspek penting dalam menjaga keamanan informasi dan sistem komputer. Keduanya bertujuan untuk memantau aktivitas, menganalisis data, dan mengevaluasi kepatuhan terhadap kebijakan dan standar keamanan. Pemantauan aktif sistem dan jaringan komputer dapat membantu mengidentifikasi aktivitas yang mencurigakan atau anormal. Ini termasuk memantau log, lalu lintas jaringan, dan perilaku pengguna. Audit keamanan melibatkan pemeriksaan sistem, aplikasi, dan infrastruktur untuk memastikan kepatuhan terhadap kebijakan keamanan dan standar. Ini dapat membantu mengidentifikasi kerentanan dan masalah keamanan yang memerlukan perbaikan.

Kombinasi antara pemantauan dan audit membantu organisasi mengidentifikasi ancaman, mencegah insiden keamanan, dan memastikan kepatuhan terhadap praktik keamanan yang benar. Ini juga membantu organisasi merespons dengan cepat terhadap insiden keamanan jika terjadi, dan menyelidiki penyebabnya untuk memastikan perbaikan keamanan yang sesuai dilakukan.

6. Kerugian Finansial dan Reputasi

Pelanggaran data dapat menyebabkan kerugian finansial yang signifikan, termasuk biaya perbaikan, sanksi hukum, dan kerugian pelanggan. Selain itu, dampak reputasi yang negatif dapat memengaruhi kepercayaan pelanggan dan mitra bisnis. Kerugian finansial dan

reputasi adalah dua dampak serius yang dapat terjadi sebagai akibat dari pelanggaran data atau insiden keamanan informasi. Ini adalah dua dari banyak alasan mengapa organisasi harus sangat peduli dengan keamanan informasi dan melindungi data mereka dengan baik. Insiden keamanan, seperti data breach atau serangan siber, dapat mengakibatkan biaya perbaikan yang signifikan.

Ini mencakup biaya untuk mengidentifikasi, mengatasi, dan memulihkan dari serangan, termasuk pemulihan data, perbaikan sistem, dan perbaikan kerentanan yang mungkin telah dieksploitasi oleh penyerang. Kehilangan reputasi yang buruk dapat mengakibatkan penurunan bisnis. Konsumen dan mitra bisnis yang mendengar tentang pelanggaran data dapat memilih untuk tidak lagi berhubungan dengan organisasi yang terlibat. Kerugian finansial dan reputasi yang disebabkan oleh pelanggaran data dapat sangat merugikan bagi organisasi.

Oleh karena itu, upaya untuk mencegah insiden keamanan, meresponsnya dengan cepat dan efektif, dan menjaga kepatuhan terhadap peraturan keamanan dan privasi data adalah sangat penting. Kesadaran akan risiko ini dan investasi dalam perlindungan data adalah langkah yang sangat bijak untuk menjaga kesehatan finansial dan reputasi organisasi.

7. Kepatuhan Hukum

Di banyak yurisdiksi, ada peraturan dan undang-undang yang mengharuskan organisasi untuk mematuhi standar keamanan tertentu dan melaporkan pelanggaran data kepada otoritas terkait dan individu yang terkena dampak. Kepatuhan hukum dalam konteks keamanan informasi mengacu pada kewajiban organisasi untuk mematuhi peraturan dan undang-undang yang berkaitan dengan perlindungan data dan keamanan informasi. Ada banyak peraturan yang berlaku di berbagai yurisdiksi, dan organisasi harus mematuhi aturan-aturan ini untuk menghindari sanksi hukum dan menjaga data dan sistem mereka tetap aman.

Kepatuhan hukum juga melibatkan kewajiban untuk melindungi data pelanggan atau klien, termasuk data pribadi dan keuangan yang mungkin disimpan atau diproses oleh organisasi. Kepatuhan hukum dalam keamanan informasi adalah krusial untuk menghindari masalah hukum dan memastikan perlindungan data yang tepat. Organisasi harus aktif memantau peraturan dan undang-undang yang berlaku dan mengimplementasikan praktik dan kebijakan yang sesuai untuk mematuhi ketentuan tersebut. Kesadaran akan persyaratan kepatuhan hukum dan komitmen untuk mematuhinya adalah langkah penting dalam menjaga integritas dan reputasi organisasi.

8. Mitigasi Ancaman Internal

Kepatuhan juga membantu mengurangi risiko ancaman internal, seperti pekerja yang tidak jujur atau mantan karyawan yang memiliki akses yang tidak sah ke data. Mitigasi ancaman internal merujuk pada langkah-langkah yang diambil oleh organisasi untuk mengurangi risiko yang berasal dari dalam organisasi itu sendiri. Ancaman internal dapat berasal dari karyawan, mantan karyawan, atau individu lain yang memiliki akses ke sistem dan data organisasi. Mitigasi ancaman internal adalah aspek penting dari strategi keamanan informasi. Ancaman internal dapat menjadi risiko serius bagi organisasi, dan dengan langkah-langkah yang tepat, risiko ini dapat diminimalkan. Dengan pendekatan yang komprehensif yang mencakup manajemen hak akses, pemantauan, pelatihan, dan kebijakan yang ketat, organisasi dapat melindungi data dan sistem mereka dari ancaman internal.

Dalam rangka mengurangi risiko data breach, organisasi perlu mengimplementasikan prosedur dan kebijakan yang sesuai dengan standar keamanan informasi yang relevan, seperti ISO 27001, dan terus memantau dan memperbarui praktik keamanan mereka. Dengan demikian, mereka dapat mengurangi risiko data breach dan melindungi aset informasi mereka serta reputasi mereka.

Kesimpulan singkat dari semua penjelasan di atas adalah bahwa keamanan informasi adalah kunci untuk melindungi data, menghindari kerugian finansial dan reputasi, dan mematuhi peraturan hukum. Ini melibatkan praktik dan kebijakan seperti kepatuhan, pencegahan akses tidak sah, deteksi dini, pelatihan karyawan, pemantauan, audit, mitigasi ancaman internal, dan perhatian terhadap kerugian finansial dan reputasi. Keseluruhan, keamanan informasi adalah tanggung jawab bersama dan esensial dalam dunia bisnis dan teknologi.

KESIMPULAN DAN SARAN

Perlindungan data sensitif adalah suatu tindakan yang sangat penting dalam mengurangi risiko data breach. Data breach merupakan insiden di mana data sensitif atau informasi penting menjadi rentan atau diakses oleh pihak yang tidak berwenang. Untuk mencegah data breach, organisasi perlu mengambil berbagai tindakan, kebijakan, dan praktik keamanan, seperti enkripsi, manajemen akses, keamanan fisik, keamanan jaringan, pelatihan dan kesadaran keamanan, kebijakan keamanan, serta pemantauan dan audit. Perlindungan data sensitif membantu menjaga kerahasiaan, integritas, dan ketersediaan data serta melindungi reputasi dan kepercayaan pelanggan dan mitra bisnis. Dengan menerapkan

perlindungan data sensitif yang baik, organisasi dapat mengurangi risiko data breach yang dapat merugikan secara finansial dan merusak citra perusahaan.

DAFTAR REFERENSI

Ailin, T. (2020, November 09). Indonesia Butuh Aturan Khusus Perlindungan Data Pribadi. DipetikNovember 18, 2020, dari merdeka.com: https://www.merdeka.com/uang/indonesia-butuh-aturan-khusus-perlindungan- data-pribadi.html

Califa chazar (2015).”Standar manajemen keamanan sistem informasi berbasis iso/iec 27001:2005”

Cinda septilia kusumaningrum, budi widjajanto (2016) “kelengkapan dan kematangan sistem keamanan informasi berdasarkan indeks kami pada divisi sampling dan pengujian bbpom kota semarang” fakultas ilmu komputer, universitas dian nuswantoro semarang.

H. Affandi and a. Darmawan, "audit kemanan informasi menggunakan iso 27002 pada data center pt.gigipatra multimedia," jurnal tim darmajaya, vol. I, no. 2, 2015.

Hadjon Philipus, M., & Hukum, A. (2017). Gadjah, Mada University Press. Karo, R. P. (2019, Oktober 08). Perlindungan Hukum atas Privasi dan Data Pribadi Masyarakat. Dipetik November 18,2020, dari hukumonline.com: https://www.hukumonline.com/klinik/detail/ulasan/lt5d588c1cc649e/perlindung an-hukum-atas-privasi-dan-data-pribadi-masyarakat/

https://www.liputan6.com/tekno/read/4300393/ramai-data-pribadi-bocor- pengamat-belum-tentu-dari-operator-telko

Kusnadi, S. A. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. AL WASATH Jurnal Ilmu Hukum, 2(1), 9–16. https://doi.org/10.47776/alwasath.v2i1.127

Lahur, M. F. (2022). 1,3 Miliar Kartu SIM Bocor, Vaksincom: Data Pribadi Otentik dan Masih Aktif. Www.Tempo.Co. https://tekno.tempo.co/read/1630939/13-miliar-kartu-sim- bocor-vaksincom-data-pribadi-otentik-dan-masih-aktif

M. Amin, "pengukuran tingkat kesadaran keamanan informasi menggunakan multiple criteria decision analysis (mcda)," jurnal penelitian dan pengembangan komunikasi dan informatika, vol. V, no. 1, 2014.

Newswire. (2021). Ini Bahaya Yang Bisa Terjadi Bila DataPribadi Kita Bocor. Www.Solopos.Com. https://www.solopos.com/ini-bahaya-yang-bisa- terjadi-bila-data-pribadi-kita-bocor-1126609

Niffari, H. (2020). PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI Suatu

Oktavira, B. A. (2020, Agustus 04). Dasar Hukum Perlindungan Data Pribadi Pengguna Internet. Dipetik November 18, 2020, dari hukumonline.com: https://www.hukumonline.com/klinik/detail/ulasan/lt4f235fec78736/dasar- hukum-perlindungan-data-pribadi-pengguna-internet/

R. E. Indrajit, konsep dan strategi keamanan informasi di dunia cyber, yogyakarta: graha ilmu.

R. Papang and e. N. Sancoyo, "penyusunan tata kelola audit e-procurement instansi pemerintah," jnteti, vol. Ii, no. 3, 2013.

Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain. Jurnal Hukum Dan Bisnis (Selisik), 6(1), 1–14. https://doi.org/10.35814/selisik.v6i1.1699

Unian dani (2008). “pengembangan kebijakan keamanan”, fasilkom ui, 2018 [10] (kominfo, 2017). Tim direktorat keamanan informasi kementrian komunikasi dan informatika ri. 2017. “panduan penerapan sistem manajemen keamanan”

Wardani, A. S. (2020, Juli 09). Ramai Data Pribadi Bocor, Pengamat: Belum Tentu dari Operator Telko. Dipetik November 18, 2020, dari liputan6.com:

Winarsih, W., & Irwansyah, I. (2020). Proteksi Privasi Big Data Dalam Media Sosial. Jurnal Audience, 3(1), 1–33. https://doi.org/10.33633/ja.v3i1.3722