E-ISSN : 3025-1311
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 3 No 7 Tahun 2024

CARA MENGIDENTIFIKASI DAN MENGHINDARI KEBOCORAN DATA

Ripa Sabila Usni Sitompul[1], Muhammad Irwan Padli Nasution[2]
Program Studi Manajemem Fakultas Ekonomi Dan Bisnis Islam Universitas Islam Negeri Sumatera Utara
[1]Email: rifasabila03@gmail.com [2]Email: irwannst@uinsu.ac.id

Abstract
Data leaks are a serious threat in the business environment that can cause financial losses and reputation damage. This research aims to provide practical guidance for companies in identifying, preventing, and dealing with data leaks. The Library Research method explains steps such as creating security policies, controlling email content, implementing EDR solutions, employee training, and updating IT equipment to increase company data security.
Keywords: data leaks, information security, data protection, EDR solutions, employee training.

Abstrak
Kebocoran data merupakan ancaman serius dalam lingkungan bisnis yang dapat menyebabkan kerugian finansial dan kerusakan reputasi. Penelitian ini bertujuan untuk memberikan panduan praktis bagi perusahaan dalam mengidentifikasi, mencegah dan menangani kebocoran data. Melalui metode Library Research dijelaskan langkah-langkah seperti membuat kebijakan keamanan, pengendalian konten email, penerapan solusi EDR, pelatihan karyawan, dan pemutakhiran peralatan IT untuk meningkatkan keamanan data perusahaan.
Kata Kunci: Kebocoran Data, Keamanan Informasi, Perlindungan Data, Solusi EDR, Pelatihan Karyawan

Latar Belakang

Kebocoran data merupakan isu yang sangat penting dalam dunia bisnis dan teknologi informasi saat ini. Kebocoran data dapat menyebabkan dampak serius bagi perusahaan, termasuk kerugian finansial, kerusakan reputasi, dan pelanggaran privasi pelanggan. Oleh karena itu, penting bagi perusahaan untuk memahami risiko kebocoran data dan mengambil langkah-langkah proaktif untuk mencegahnya. Dalam konteks yang semakin kompleks dan terhubung secara digital, peretas selalu mencari cara baru untuk mendapatkan akses ke sistem, mencuri informasi sensitif, dan memanipulasi karyawan untuk mendapatkan informasi yang mereka butuhkan. Hal ini menunjukkan perlunya perlindungan endpoint dan keamanan data yang kuat untuk melindungi perusahaan dari ancaman kebocoran data.

Dengan demikian, penelitian ini bertujuan untuk memberikan pemahaman yang lebih dalam tentang cara mengidentifikasi, mencegah, dan mengatasi kebocoran data dalam lingkungan bisnis. Melalui metode Library Research, penelitian ini menggali berbagai sumber informasi untuk menyusun langkah-langkah praktis yang dapat diterapkan oleh perusahaan untuk meningkatkan keamanan data mereka. Dengan adanya pemahaman yang lebih baik tentang risiko kebocoran data dan langkah-langkah yang dapat diambil untuk mengatasinya, diharapkan perusahaan dapat meningkatkan ketahanan mereka terhadap ancaman keamanan informasi dan melindungi data sensitif mereka dengan lebih efektif.

Tujuan

Tujuan dari penelitian ini adalah untuk mengetahui cara agar perusahaan dapat menghindari dan mengidentifikasi kebocoran data, yang bisa menyebabkan dampak buruk bagi perusahaan. Ini mencakup langkah-langkah yang dapat dilakukan untuk mengidentifikasi dan menangani kebocoran data, serta mengurangi risiko kebocoran data.

Metode

Penelitian perpustakaan adalah metode yang digunakan dalam artikel ini, dan metode ini mencakup penggunaan buku, jurnal, teks, dan internet. Menurut karya penelitian Sugiyono, penelitian kepustakaan diartikan sebagai suatu metode pengumpulan data penelitian dari berbagai informasi perpustakaan dengan cara menganalisis hasil penelitian, referensi buku, dokumen lain, dan sumber pendukung lainnya

Hasil Penelitian

Data security atau keamanan data merupakan sebuah sistem keamanan yang memang dibutuhkan untuk melindungi data yang terdapat di dalam jaringan, sistem atau komponen digital lainnya. Keamanan ini bisa melindungi data agar terhindar dari kejahatan siber (cyber crime) yang saat ini juga semakin marak dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Bagi pemilik usaha atau bisnis ritel, paham tentang keamanan data ini sangat penting untuk menjaga keberlangsungan bisnis yang dijalankan. Dengan begitu, data yang dimiliki bisa tetap aman dari kerusakan maupun akses yang tidak sah dari pihak yang tidak berkepentingan yang mungkin ingin mengubah data tersebut.

Jenis-Jenis Data Security

Bagi perusahaan, data adalah aset yang sangat berharga. Operasional hingga finansial perusahaan bisa kacau apabila data milik bisnis maupun konsumen mengalami kebocoran atau dicuri. Tentu hal ini sangat merugikan karena bisa mengancam keberlangsungan bisnis. Oleh sebab itu, perusahaan harus menerapkan keamanan data ini dengan benar. Dalam praktiknya, keamanan data ini terbagi menjadi beberapa jenis yang masing-masing memiliki metode kerja yang berbeda yaitu:

1. Enkripsi (Encryption)

   Enkripsi atau data encryption merupakan metode pengamanan data melalui algoritma yang mengubah data menjadi sebuah format yang tidak akan terbaca oleh yang tidak memiliki wewenang. Hanya pengguna yang berwenang dengan kata kunci sesuai saja yang bisa membuka maupun mengakses informasi tersebut. Teknik ini bisa dibilang cukup efektif melindungi data penting selama pengiriman maupun penyimpanan.
2. Autentikasi (Authentication)

   Teknik keamanan data ini digunakan untuk memastikan bahwa pihak yang mengakses data atau sistem adalah yang memiliki wewenang dan kredensialnya memang telah tercatat dalam database sistem tersebut. Praktik dari teknik ini mencakup beberapa hal seperti wajib memasukkan nomor PIN, sandi, biometrik, kartu gesek dan token keamanan.
3. Kontrol Akses (Access Control)

   Cara kerja jenis pengamanan data ini adalah dengan membatasi akses baik secara fisik maupun digital yang menuju ke sistem, jaringan hingga data penting. Proses ini hanya akan memberi izin akses kepada pihak yang berwenang saja. Dengan kontrol

akses, anda bisa menentukan siapa saja yang bisa mengakses data dan sistem sekaligus membatasi akses yang mereka inginkan.

4. Pencadangan dan Pemulihan (Backup and Recovery)
   Ini merupakan jenis pengamanan yang wajib dilakukan. Sebab jika terjadi kegagalan sistem, kerusakan, bencana atau kebocoran data, anda masih bisa memulihkan data dan mengakses sekaligus menggunakan data secara normal. Oleh sebab itu, sangat penting bagi anda untuk membuat pencadangan serta pemulihan data secara berkala di tempat yang terpisah seperti halnya cloud.
5. Firewall
   Pertahanan utama dalam melawan cyber crime adalah firewall yang merupakan sistem pengamanan yang biasanya digunakan untuk memantau sekaligus melindungi jaringan komputer dari serangan dari luar. Cara kerja pengamanan data firewall ini adalah dengan memblokir akses yang mencurigakan yang sudah melalui proses analisa data yang masuk sekaligus mengidentifikasi aktivitas yang dilakukan.
6. Endpoint Protection
   Endpoint protection ini umum digunakan untuk melindungi perangkat akhir seperti smartphone dan komputer dari cyber crime. Pengamanan data jenis ini berupa perangkat lunak antivirus sekaligus perlindungan terhadap malware yang akan memantau dan mendeteksi tanda-tanda serangan siber. Dengan memastikan keamanan pada perangkat akhir ini, maka semua titik akses menuju jaringan anda bisa dikatakan aman dari ancaman cyber crime yang berbahaya.
7. Penghapusan Data
   Menghapus data yang sudah tidak dibutuhkan harus dilakukan dengan benar dan teratur. Penghapusan data (data eraser) merupakan jenis pengamanan data yang dilakukan dengan menggunakan perangkat lunak dalam melakukan overwrite di perangkat penyimpanan supaya tidak bisa dipulihkan lagi.

Kegunaan Menggunakan Keamanan Data

Kegunaan utama menerapkan pengamanan data ini tentu untuk melindungi data, baik itu data milik perusahaan dan konsumen. Selain itu, ternyata masih ada beberapa kegunaan lain yang bisa dirasakan dampak baiknya bagi pelaku usaha. Berikut adalah diantaranya:

1. Mencegah Serangan Siber
   Seperti yang sudah banyak disinggung di atas, pengamanan data digunakan untuk melindungi data dari serangan siber yang bisa mengganggu aktivitas operasional perusahaan. Dengan menerapkan pengamanan yang benar, maka berbagai risiko bisa ditanggulangi dengan baik.
2. Melindungi Data
   Kegunaan paling utama dari pengamanan data ini data milik perusahaan maupun konsumen bisa terlindung dari serangan siber maupun jenis kejahatan lain. Dengan adanya keamanan data ini, maka berbagai ancaman serta risiko digital lainnya yang mengintai bisa diatasi ataupun dihindari dengan baik.
3. Menjaga Produktivitas Perusahaan
   Saat serangan siber menyerang, aktivitas operasional perusahaan biasanya juga ikut terganggu. Tapi jika perusahaan sudah menerapkan pengamanan data dengan benar, maka risiko ini bisa ditangani dengan baik. Anda menjadi mengerti hal apa yang perlu dilakukan saat terjadi serangan siber, sehingga aktivitas perusahaan bisa tetap berjalan normal.
4. Meningkatkan Kepercayaan Pelanggan
   Tentu saja pelanggan akan lebih percaya terhadap perusahaan yang bisa menjaga data konsumen dengan baik. Dengan begitu, citra perusahaan serta kepercayaan

konsumen pada perusahaan bisa meningkat dan dapat melanjutkan bisnis jangka panjang dengan anda.
Strategi data security yang baik harus menentukan beberapa hal. Diantaranya, data apa saja yang perlu dicadangkan, bagaimana data dipulihkan saat terjadi kegagalan serta media penyimpanan seperti apa yang perlu digunakan.

Cara Menghindari Kebocoran Data:

1. Perusahaan harus menetapkan kebijakan keamanan
   Perusahaan harus mulai membuat aturan untuk diikuti oleh semua karyawan. Contohnya penerapan kebijakan untuk memastikan karyawan tidak membiarkan komputer mereka hidup/unlocked dan tidak berbagi akun dengan rekan kerja lainnya.
2. Pengendalian Kebocoran data melalui email
   Karena terkadang karyawan mengirimkan informasi atau dokumen rahasia lewat email. Untuk mencegah hal ini terjadi, perusahaan bisa menggunakan email content filtering.
3. Endpoint protection
   Peretas memiliki cara baru untuk dapat mengakses sistem, mencuri informasi, dan memanipulasi karyawan untuk memberikan informasi rahasia. Maka dari itu perusahaan butuh endpoint protection.
4. Meningkatkan keamanan data
   Hilangnya data biasanya disebabkan oleh kelalaian pengguna atau adanya kelemahan pada sistem yang digunakan. kelemahan keamanan yang tidak segera diperbaiki bisa memungkinkan peretas mendapatkan akses ke data internal yang lebih sensitif

Cara Mengantisipasi Kebocoran Data:

1. Memberikan akses intelijen kepada tim Operasi Keamanan (SOC)
   Beri tim Operasi Keamanan (SOC) perusahaan akses terhadap intelijen terkini dan terus mendapatkan informasi terkini tentang alat dan perlengkapan, metode, dan teknik terbaru yang digunakan oleh penjahat dunia maya (siber)
2. Menerapkan solusi *Endpoint Detection and Response* (EDR)
   Untuk mencegah pelanggaran data, perusahaan harus bisa menerapkan solusi deteksi dan respons titik akhir (EDR) karena memungkinkan perusahaan mendeteksi dan menyelesaikan insiden secara real time.
3. Solusi keamanan tingkat perusahaan
   Untuk mencegah atau mengantisipasi kebocoran pada data, perusahaan harus bisa meningkatkan sistem keamanan datanya. Solusi keamanan data perusahaan untuk mencegah penyalahgunaan data karena kebocoran pada data.
4. Memberikan pelatihan kepada karyawan tentang keamanan siber
   Banyak kebocoran data yang terjadi biasanya diakibatkan dari kelalaian manusia. Oleh sebab itu, perusahaan dapat menggunakan metode ini untuk menghindari kebocoran data. caranya dengan melatih karyawannya tentang dasar-dasar keamanan siber. Contohnya, tidak menyimpan ataupun membuka email dan file dari situs web yang tidak dikenal yang bisa membahayakan seluruh perusahaan.
5. Mengingatkan karyawan untuk menangani data sensitif
   Ini adalah sesuatu yang dapat Anda harapkan ketika karyawan Anda menangani data sensitif perusahaan. Contohnya, simpan data perusahaan hanya di layanan cloud tepercaya dengan autentikasi diaktifkan dan jangan membaginya dengan pihak ketiga yang tidak dipercaya.
6. Implementasikan menggunakan perangkat lunak yang disetujui

Perusahaan dapat menerapkan cara ini untuk mencegah kebocoran data perusahaan. Hal ini karena data dikompromikan ketika perusahaan menggunakan perangkat lunak yang diunduh dari sumber tidak sah atau ilegal.

7. Backup data penting dan perbarui perangkat keras dan aplikasi IT
   Mencadangkan big data suatu perusahaan merupakan salah satu cara untuk mengantisipasi kebocoran data. Bahkan jika pelanggaran data terjadi, bisnis masih dapat mengakses data sensitif perusahaan mereka di cloud tempat data tersebut dicadangkan. Bisnis perlu memperbarui perangkat keras dan aplikasi TI mereka untuk menghindari kelemahan yang tidak dapat dipecahkan.

Kesimpulan

Berdasarkan hasil penelitian dari metode literatur review yang telah dilakukan, dapat disimpulkan bahwa dari cara mengidentifikasi dan menghindari kebocoran data adalah dengan perlindungan data pribadi memerlukan tindakan preventif yang kuat, sistem keamanan yang handal, serta kesadaran akan risiko dan ancaman kebocoran data yang dapat terjadi lewat berbagai sumber. Dengan menjaga keamanan data/data security dengan baik, kita dapat mengelola untuk meminimalisir kerugian yang diakibatkan oleh kebocoran pada data. Cara dengan, pertama perhatikan hal-hal kecil yang biasanya dilakukan, mulai dari nomor hp, hingga alamat kamu tinggal. Kedua, batasi akses pada perangkat. Hapus akses untuk pihak yang tidak dikenal. Dan yang terakhir, pilihlah rekan yang baik/tepat. Jangan sampai ada rekan kita yang menyalahgunakan informasi/data untuk kepentingan mereka sendiri dan merugikan bagi kita atau perusahaan kita. Dan yang lebih baik lagi bisa dengan langkah-langkah seperti membuat kebijakan keamanan, pengendalian konten email, penerapan solusi EDR, pelatihan karyawan, dan pemutakhiran peralatan IT untuk meningkatkan keamanan data perusahaan.

DAFTAR PUSTAKA

Satria, Muhammad Hatta. *"Perlindungan Kerahasiaan Data Investor untuk Pencegahan Kebocoran Data Investor pada Perusahaan Inovasi Keuangan Digital Goolive."* Jurisdictie: Jurnal Hukum Dan Syariah 10.1 (2019): 1-17.

Shachar Kaufman, Saharon Rosset, Claudia Perlich, dan Ori Stitelman. 2012. *"Kebocoran dalam data mining: Formulasi, deteksi, dan penghindaran."* ACM Trans. Tahu. Penemuan. Data 6, 4, Pasal 15 (Desember 2012)

Zhao, Q., Zuo, C., Pellegrino, G., & Zhiqiang, L. (2019). *"Geolocating Drivers: A Study of Sensitive Data Leakage in Ride-Hailing Services. Annual Network and Distributed System Security Symposium"* February 2019 (NDSS 2019)

CTI CONTENT WRITER, *"Cara Mengantisipasi dan Menyikapi Kebocoran Data Perusahaan."* Helios informatika nusantara 25 juni 2021