JoSES: Journal of Sharia Economics Scholar
Volume 2, Nomor 2, June 2023, Halaman 113-121

ISSN: 2302-6219
DOI: https://doi.org/10.5281/zenodo.12608875

Taktik Canggih untuk Memastikan Keamanan Data Perusahaan dan Mengatasi Ancaman Kebocoran Data di Masa Depan

Muhd. Aidil Fitri[1], Muhammad Irwan Padli Nasution[2]
[12]Universitas Islam Negeri Sumatera Utara[1], Universitas Islam Negeri Sumatera Utara[2]
Email: Aidilfitry1474@gmail.com[1], irwannst@uinsu.ac.id[2]

Abstract

In an increasingly sophisticated digital era, data protection has become an important issue, especially considering the increasing amount of personal and sensitive information that is stored and processed in digital format. Global cyber threats continue to grow rapidly, and the number of data breaches continues to increase every year. Data leaks are a hot topic not only abroad but also in Indonesia. One hacker who has attracted the attention of many people is Bjorka. No joke, the suspect Bjorka collected 26 million search history data and information on users of communications service providers, 1.3 billion SIM card registration data, 105 million Indonesian National Election Commission data, allegedly stole various types of data, including confidential information. From public officials to 34 million Indonesian citizens. Researchers will discuss issues regarding what must be prevented so that data security remains controlled? What steps can companies take to ensure data remains safe? What is the strategy for data protection? The purpose of this discussion is to understand readers and researchers how to improve the quality of data security, to prevent data leaks which are currently occurring, especially in companies in Indonesia. As well as linking the discussion in this research to previous research. In this article, we use the Literature Review technique, several researchers have discussed the context being discussed by the researcher, then the researcher draws conclusions. Based on the results of research conducted, there are several steps that companies can implement to maintain security based on several previous studies.

Abstrak

Di era digital yang semakin canggih, perlindungan data telah menjadi isu penting, terutama mengingat semakin banyaknya informasi pribadi dan sensitif yang disimpan dan diproses dalam format digital. Ancaman dunia maya global terus berkembang pesat, dan jumlah pelanggaran data terus meningkat setiap tahunnya. Kebocoran data menjadi topik hangat tidak hanya di luar negeri tapi juga di Indonesia. Salah satu hacker yang menarik perhatian banyak orang adalah Bjorka. Tak main-main, tersangka Bjorka mengumpulkan 26 juta data riwayat pencarian dan informasi pengguna penyedia jasa komunikasi, 1,3 miliar data registrasi kartu SIM, data KPU RI sebanyak 105 juta data nasional Indonesia, Diduga mencuri berbagai jenis data, termasuk informasi rahasia. Dari pejabat publik hingga 34 juta WNI. Peneliti akan membahas permasalahan mengenai Apa yang harus dicegah agar keamanan data tetap terkontrol?, Bagaimana Langkah-Langkah yang dapat dilakukan perusahaan agar data tetap aman?, Bagaimana strategi dalam perlindungan data?. Tujuan dari pembahasan ini adalah memahami pembaca dan peneliti bagaimana dapat meningkatkan kualitas keamanan data, dapat mencegah kebocoran data yang sedang marak terjadi, terkhusus pada perusahaan di Indonesia. Serta mengaitkan pembahasan pada penelitian ini pada penelitian terdahulu. Dalam artikel ini menggunakan teknik *Literature Review*, pada beberapa peneliti yang telah membahas konteks yang sedang dibahas oleh peneliti, kemudian peneliti mengambil berapa kesimpulan.Berdasarkan hasil penelitian yang dilakukan bahwa terdapat beberapa langkah yang dpat diimplementasikan perusahaan untuk menjaga kemanan berdasarkan beberapa penelitian terdahulu.

Article Info
Received date: 08 June 2024 Revised date: 18 June 2024 Accepted date: 22 June 2024

PENDAHULUAN

Di era digital yang semakin canggih, perlindungan data telah menjadi isu utama, terutama mengingat semakin banyaknya informasi pribadi dan sensitif yang disimpan dan diproses dalam format digital. Ancaman dunia maya global terus berkembang pesat, dan jumlah pelanggaran data terus meningkat setiap tahunnya. Menurut laporan RiskBased Security, dalam sembilan bulan pertama tahun

2022 saja, pelanggaran data mengungkap 7,9 miliar catatan. Jumlah ini lebih dari dua kali lipat (112%) dibandingkan jumlah rekaman yang diterbitkan pada periode yang sama pada tahun 2021.

Jumlah pelanggaran tertinggi terjadi di layanan kesehatan, toko ritel, dan fasilitas umum, dengan mayoritas dilakukan oleh penjahat. Beberapa sektor ini lebih menarik bagi penjahat dunia maya karena mereka mengumpulkan data keuangan atau medis, namun perusahaan yang menggunakan jaringan mereka lebih rentan terhadap data pelanggan, spionase perusahaan, dan serangan pelanggan. Ketika skala ancaman siber terus meningkat, International Data Corporation memperkirakan pengeluaran global untuk solusi keamanan siber akan mencapai $133,7 miliar pada tahun 2020 (Carell dan Zuhriyah 2021). Pemerintah di seluruh dunia telah menanggapi meningkatnya ancaman siber dengan memberikan panduan untuk membantu organisasi menerapkan praktik keamanan siber yang efektif.

Kebocoran data menjadi topik hangat tidak hanya di luar negeri tapi juga di Indonesia. Salah satu hacker yang menarik perhatian banyak orang adalah Bjorka. Tak main-main, Bjorka mengumpulkan 26 juta data riwayat pencarian dan informasi pengguna penyedia layanan komunikasi, 1,3 miliar data registrasi kartu SIM, 105 juta data KPU RI, dan data nasional Indonesia, serta merahasiakannya . Dari PNS hingga 34 juta WNI.

Keamanan data masih menjadi perhatian utama dunia bisnis, meski insiden pencurian data terus meningkat. Faktanya, keamanan data seringkali menjadi hal terakhir yang dipertimbangkan perusahaan ketika membangun sistem atau memilih penyedia. Biasanya, perusahaan paling mementingkan fungsionalitas dan biaya.

Ketika sebuah perusahaan mengalami pelanggaran data atau masalah keamanan lainnya, dampaknya bisa signifikan, baik berwujud maupun tidak berwujud. Oleh karena itu, penting bagi perusahaan untuk menjadikan keamanan data sebagai prioritas bisnis. Hal ini harus dilakukan agar perusahaan terhindar dari ancaman serius yang dapat mengganggu proses bisnis dan melemahkan peluang yang ada.

Tabel 1. Daftar Negara dengan Jumlah Kebocoran Data Terbanyak

Rusia	14.788.574 Akun
Perancis	12.949.968 Akun
Indonesia	12.742.013 Akun
Amerika Serikat	4.827.286 Akun
Tiongkok	2.782.843 Akun
Taiwan	1.230.939 Akun
Brasil	1.164.531 Akun
India	1.041.887 Akun
Kolombia	826.628 Akun
Nigeria	558.647 Akun

Sumber: https://databoks.katadata.co.id/

Menurut perusahaan keamanan siber Surfshark, Indonesia adalah negara dengan jumlah pelanggaran data tertinggi ketiga di dunia. Pada kuartal ketiga tahun 2022, 12,74 juta akun di Tanah Air ditemukan mengalami pelanggaran data. Direkam hingga 13 September 2022. Daftar 21. 000 perusahaan telah dibagikan oleh peretas. Daftar perusahaan tersebut paling sedikit meliputi perusahaan asuransi, perusahaan pertambangan, konsultan hukum, koperasi, perkebunan, farmasi, logistik, real estate, impor/ekspor, sandang, kerajinan tangan, transportasi, dan konstruksi.

Ada beberapa praktik terbaik yang dapat membantu organisasi memerangi serangan kejahatan dunia maya. Kembangkan strategi dan ambil tindakan proaktif. Pertama, lindungi jaringan Internet Anda dengan menggunakan enkripsi dan kata sandi yang kuat. Buat juga kebijakan penggunaan jaringan yang jelas untuk memastikan akses jaringan dibatasi hanya pada mereka yang benar-benar membutuhkan (Ni Putu Ria Dewi Marhaeni 2013). Kemudian, selalu buat cadangan data Anda dan simpan serta salin data penting Anda di tempat yang aman untuk memastikannya berfungsi saat Anda membutuhkannya. Hal ini memfasilitasi pemulihan data jika terjadi serangan kejahatan dunia maya atau kehilangan data lainnya.

Ketiga, kami memberikan pelatihan kepada karyawan kami mengenai praktik keamanan siber yang baik. Hal ini termasuk mengajari mereka cara membedakan serangan phishing, cara menjaga keamanan kata sandi, dan cara menghindari mengklik tautan atau lampiran yang mencurigakan. Karyawan yang terlatih dapat melindungi bisnis dengan lebih baik dari serangan kejahatan dunia maya (Kashyap dan Chaudhary 2023).

Oleh karena itu, penelitian ini didasarkan pada tinjauan beberapa penelitian sebelumnya sebagai referensi. Salah satunya adalah penelitian yang dilakukan oleh Tri Ginanjar Laksana yang menggambarkan temuan awal dalam mendeteksi serangan kriminal keamanan data untuk mencegah pelanggaran data di masa depan dalam organisasi. Selain itu, artikel ini menjelaskan cara mengembangkan strategi keamanan siber yang efektif untuk digunakan dalam bisnis Anda. Tujuan dari pembahasan ini adalah memahami pembaca dan peneliti bagaimana dapat meningkatkan kualitas keamanan data, dapat mencegah kebocoran data yang sedang marak terjadi, terkhusus pada perusahaan di Indonesia. Serta mengaitkan pembahasan pada penelitian ini pada penelitian terdahulu.

KAJIAN TEORI

Data dan Informasi

Pengertian data menurut (Gunadi & Widianto, 2020) adalah informasi yang bersifat kualitatif dan kuantitatif, atau fakta-fakta yang membuktikan, sehingga dapat memberi manfaat bagi peneliti atau memberikan gambaran kepada peneliti tentang suatu kondisi atau situasi, yang merupakan bahan baku yang harus diolah untuk menghasilkan informasi. situasi. Sedangkan informasi adalah kumpulan data yang telah diolah untuk dijadikan suatu analisis yang dapat digunakan oleh pihak-pihak yang diperlukan.

Keamanan Data Informasi

Keamanan sistem informasi adalah perlindungan sistem informasi dari ancaman yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan data yang disimpan dan diproses dalam sistem. Keamanan sistem informasi mencakup berbagai teknologi, prosedur, kebijakan, dan praktik yang dirancang untuk mengidentifikasi, mencegah, memitigasi, dan mengatasi potensi risiko keamanan pada sistem informasi.

Sistem keamanan informasi memiliki tiga tujuan dasar yaitu :

Gambar 1. Aspek Keamanan Informasi

a. *Confidentially* (Kerahasiaan), Informasi dalam sistem komputer dijamin kerahasiaannya, hanya dapat diakses oleh pihak yang berwenang, dan integritas serta konsistensi data dalam sistem tetap terjaga. Oleh karena itu, usaha mereka yang mencoba mencuri informasi tersebut akan sia-sia.
b. *Integrity* (Integritas), Dalam keamanan informasi, integritas mengacu pada metode atau prosedur untuk memastikan bahwa data atau informasi tidak dapat dimanipulasi, dimodifikasi, atau diedit oleh pihak-pihak tanpa izin. Langkah-langkah ini memastikan keakuratan dan kelengkapan informasi. Sama seperti Anda melindungi informasi sensitif, Anda juga perlu melindungi integritasnya.
c. *Confidentiality* (Ketersediaan), Dari perspektif keamanan informasi, penting untuk mengambil langkah-langkah untuk memastikan bahwa sistem dapat terus digunakan.Perlindungan ketersediaan harus diberikan untuk memastikan bahwa sistem dan data dapat diakses oleh pengguna yang berwenang ketika informasi tersebut dibutuhkan.

Pembobolan Data

Pelanggaran data pribadi adalah kejahatan dunia maya. *Cybercrime* merupakan kejahatan yang dilakukan melalui media komputer atau jaringan , seperti pencurian data (phishing) yang terjadi pada industri perbankan.Harus ada undang-undang kejahatan dunia maya yang relevan. *Cyber Law* merupakan undang-undang khusus kejahatan di bidang Internet dan jaringan , yang mengatur bentuk-bentuk perlindungan hukum terhadap perdagangan elektronik, pembelajaran elektronik, pemegang hak cipta, rahasia dagang, paten, dan tanda tangan elektronik. 6 Undang-undang perlindungan terkait kejahatan dunia maya sangat dibutuhkan untuk mencegah semua kejahatan di dunia maya. Di industri perbankan, terjadi pelanggaran data pribadi perusahaan.

PENELITIAN

Pada artikel ini peneliti menggunakan metode kualitatif dengan mengumpulkan beberapa bahan review. Seperti buku, website, penelitian terdahulu, jurnal nasional ataupun jurnal internasional yang disesuaikan dengan konteks yang sedang diteliti. Dalam artikel ini menggunakan teknik *Literature Review*, pada beberapa peneliti yang telah membahas konteks yang sedang dibahas oleh peneliti, kemudian peneliti mengambil berapa kesimpulan.

Tinjauan pustaka adalah metode perolehan data dengan menggunakan penelitian kualitatif. Metode tinjauan pustaka adalah suatu metode yang melibatkan serangkaian kegiatan yang berkaitan dengan pengumpulan data dari sumber perpustakaan, membaca dan mencatat informasi, serta melakukan analisis terhadap bahan penelitian yang dikumpulkan. Tujuan dari metode ini adalah untuk memperoleh pemahaman mendalam mengenai topik penelitian yang sedang dibahas.

Tinjauan literatur memerlukan banyak keputusan untuk memastikan bahwa data, analisis data, dan kesimpulan yang dihasilkan konsisten dengan tujuan yang dimaksudkan. Hal ini memerlukan persiapan dan pelaksanaan yang optimal. Tinjauan literatur memerlukan analisis yang cermat dan terperinci untuk mendapatkan hasil, namun tidak memberikan privasi.

Pencarian artikel jurnal dilakukan salah satu website Google Scholar, database jurnal yang dipilih terindex sinta ataupun garuda dengan kata kunci keamanan data dan kebocoran data. Kriteria data yang dipilih untuk digunakan dalam penelitian adalah:

a. Jurnal terbit pada rentang waktu 3 atau 6 tahun.
b. Data jurnal dipilih baik terindex sinta maupun garuda.
c. Data artikel yang dipilih berkaitan dengan topik yang sedang dibahas oleh penelitian.

HASIL DAN PEMBAHASAN

Tabel 2. Literature Review

No.	Penulis	Judul Penelitian	Hasil Penelitian
1.	Dewi Riskita Yuniarti, dkk	Analisis Potensi dan Strategi Pencegahan *Cyber Craim* Dalam Sistem Logistik di Era Digital	Studi tersebut menemukan bahwa ancaman serangan kejahatan dunia maya terhadap sistem logistik dapat berasal dari berbagai sumber, termasuk peretas, kelompok kejahatan terorganisir, dan bahkan karyawan internal yang memiliki akses ke sistem logistik perusahaan.Selain itu, terdapat strategi untuk mencegah kejahatan dunia maya dalam sistem logistik. Ini berarti mengubah kata sandi perusahaan Anda secara berkala, melakukan uji penetrasi, memperbarui perangkat lunak yang Anda gunakan, melatih karyawan Anda, menggunakan kombinasi kata sandi yang rumit, menggunakan layanan hosting yang

			aman dan membuat sistem perencanaan keamanan, serta melindungi data sensitif WAF, dan aplikasi blockchain.
2.	Tri Ginanjar & Sri Mulyani	Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan.	Hasil survei yang dilakukan adalah sebagai berikut: Untuk meningkatkan keamanan siber dan melindungi bisnis Anda dari serangan kejahatan siber, memahami jenis serangan kejahatan siber yang terjadi saat ini, mengembangkan strategi keamanan yang efektif, dan mengambil tindakan proaktif untuk meningkatkan upaya keamanan siber Anda harus dilakukan. Dunia usaha dapat memperoleh keterampilan dan pengetahuan keamanan siber yang diperlukan dengan mendapatkan sertifikasi dan berpartisipasi dalam program pelatihan keamanan siber. Oleh karena itu, segera ambil langkah untuk melindungi bisnis Anda dari serangan jahat.
3.	Risqiana, Jessenia Hayfa, Rizky Rani, dkk	Implementation of Data Protection Authoritory (DPA) in Indonesia: The Urgency of Legal Protection of Customor's Personal Data in E- Bangking Service Transactions	Berdasarkan hasil analisis yang dilakukan, pengenalan Data Protection Authority (DPA) merupakan langkah penting dan komprehensif untuk menjamin keamanan dan perlindungan data pribadi nasabah dalam transaksi perbankan berbasis digital. DPA mengatur dan menjamin keamanan dan privasi informasi pribadi nasabah, mendorong bank untuk bertanggung jawab atas tindakannya dan mematuhi peraturan dan ketentuan, serta melindungi nasabah dari tuntutan pelanggaran. Keberadaan Otoritas Perlindungan Data (DPA) akan membuat penegakan hukum terhadap pelanggaran perbankan digital menjadi lebih efektif sehingga menciptakan sistem hukum yang kuat dan memperkuat sektor perbankan digital. Secara keseluruhan, penerapan DPA merupakan langkah penting dalam menjamin keamanan data pribadi nasabah, membangun kepercayaan dan mendukung perkembangan sektor perbankan digital di era teknologi yang terus berkembang.
4.	Jan Domnik & Alexander Holland	On Data Leakage Prevention Maturity: Adapting the C2M2 Framework	Hasil penelitian ini mencakup pengembangan Model Kematangan DLP yang disesuaikan berdasarkan Kerangka Kerja Kemampuan Keamanan Siber (C2M2) untuk mengevaluasi kematangan DLP. Model ini telah diaplikasikan dalam

			konteks perbankan dan berhasil mengidentifikasi kemampuan dan kesenjangan DLP, serta efektif dalam melindungi data sensitif pelanggan dan memastikan kepatuhan terhadap standar regulasi . Selain itu, penelitian ini menyoroti pentingnya pemahaman mendalam tentang DLP dan identifikasi kerangka kerja yang dapat menilai kematangan infrastruktur DLP . Model ini diharapkan dapat membantu organisasi dalam meningkatkan tingkat kematangan DLP dengan biaya yang lebih efisien
5.	Long Cheng, Fang Liu, Danfeng Yao	Enterprise Data Breach: Causes, Chalanges, Prevention, and Future Directions	Hasil penelitian yang dilakukan adalah Teknik-teknik deteksi ancaman insider seperti analisis perilaku, watermarking, dan honeypots memiliki kelemahan masing-masing yang dapat mempengaruhi tingkat deteksi dan tingkat positif palsu. Penggunaan honeypots untuk deteksi dini ancaman insider telah diusulkan sebagai metode yang efektif. Machine learning dan data mining digunakan untuk deteksi anomali keamanan siber, namun salah satu tantangannya adalah kurangnya data pelatihan .

Dari beberapa hasil review jurnal diatas ditemukan bahwa strategi menghindari kejahatan *cyber* sangatlah signifikan dilakukan oleh setiap perusahaan untuk menjaga data tetap aman dalam era digital saat ini. Dari hasil review diatas dapat kita pahami ada beberapa taktik atau cara agar data tidak dapat di bobol.

Jurnal 1 bahwa perusahaan dapat mencegah serangan *Cyber criem* 1. Mengganti *password* secara berkala, 2. Penetration Testing, 3. Memperbarui *Softwere* yang digunakan untuk mencegah *cyber criem*, 3. Menggunakan WAF (Web Application Firewall) ini mmerupakan salah satu keaman dari *cyber criem* akan mendeteksi berbagai ancaman terhadap *website* perusahaan, 4. Menggunakan Aplikasi Blockchain dapat digunakan untuk mengamankan dan melacak keamana berbagai barang dan terhindar dari berbagai kecurangan.

Jurnal 2 dalam penelitian tersebut ada beberapa praktik yang dapat digunakan untuk menghindari *cyber criem,* Malware merupakan program menyalinkan program ke dokumen yang lain. Sosial Engineering: Penggunaan rekayasa sosial untuk membujuk individu atau organisasi agar mengungkapkan informasi sensitif. Kejahatan Identitas (Identity Theft): Penggunaan informasi pribadi tanpa izin untuk melakukan kejahatan.

Jurnal 3 dalam mengatasi permasalahan keamanan data Kementrian Komunikasi (KOMINFO) menerapkan metode DPA (*Data Protection Authority*) ini merupakan badan pengawas dengan kompetensi untuk mencegah kejahatan dunia maya, khususnya penyalahgunaan data dan informasi pribadi. Fitur ini memastikan data pribadi seseorang tersimpan aman di pusat pendataan yang dikelola Kominfo.

Jurnal 4 dalam mengatasi kesenjangan spesifik dalam penelitian DLP, terutama kurangnya kerangka kerja holistik untuk menilai dan meningkatkan strategi DLP di seluruh organisasi. Hal ini membekali para praktisi dengan alat dasar untuk menentukan kematangan DLP saat ini dan merancang

strategi untuk memitigasi risiko pelanggaran data yang didorong oleh orang dalam, sehingga memperkuat ketahanan keamanan siber organisasi.

Jurnal 5 salah satu cara atau solusi yang dapat dilakukan ketika terjadi kesalahan atau kejahatan di dalam sistem data. Beberapa solusi DLPD merupakan pendekatan hibrid yang menganalisis konten dan konteks.36 Karena tujuan utama DLPD adalah untuk mengidentifikasi konten sebagai sesuatu yang sensitif, metode berbasis konten biasanya mencapai akurasi deteksi yang lebih tinggi daripada analisis berbasis konteks murni, dan oleh karena itu sebagian besar upaya penelitian di bidang ini berfokus pada analisis konten untuk mendeteksi data sensitif.

Dalam uraian pembahasan pada 5 jurnal diatas yang telah diuraikan mengenai tindakan atau solusi yang dapat dilakukan perusahaan atau suatu organisasi agar dapat terhindar dari suatu ancaman digital saat ini yakni *cyber criem* yang merupakan tindakan kejahatan yang paling sering terjadi di Indonesai maupun diluar negeri. Dan hal ini sangat menjadi referensi bagi perusahaan agar terhindar dari ancaman global tersebut.

Adapun beberapa hal yang dapat menjadi referensi atau pelengkap penelitian ini dengan menambahkan sumber bacaan oleh penulis : Miftahul Huda mengenai keamanan informasi. Dalam buku tersebut terdapat beberapa hal yang dapat dilakukan suatu perusahaan atau organisasi agar dapat menjadi strategi atau taktik untuk menghindari kebocoran data di masa depan.

1. **SSL (Secure Socket Layer)**
   Situs web ini menggunakan SSL (Secure Socket Layer) untuk membuat koneksi aman dengan browser web Anda. Ketika seseorang mengunjungi situs web yang menggunakan teknologi SSL, saluran aman dibuat antara browser pengguna dan server web selama sesi browser. SSL adalah standar industri untuk komunikasi web yang aman dan digunakan untuk mengamankan jutaan transaksi online setiap hari. Sertifikat SSL adalah sertifikat digital yang memverifikasi identitas situs web dan mengenkripsi informasi yang dikirim ke server menggunakan teknologi SSL. Sertifikat berfungsi sebagai tanda pengenal elektronik yang diakui oleh pihak lain.
2. **HTTPS (Hypertext Transfer Protocol Secure)**
   HTTPS adalah protokol komunikasi jaringan Internet. HTTPS melindungi integritas dan kerahasiaan antara situs Anda dan komputer pengguna Anda.Penggunaan HTTPS memastikan bahwa data yang dikirim dari website Anda ke pengunjung Anda aman dan tidak dapat dilihat oleh pihak lain. Protokol HTTPS juga mempersulit orang lain untuk membajak konten data dan dokumen yang dikirimkan website Anda kepada pengunjung. Artinya, tidak ada apa pun yang diperoleh pengunjung dari situs web Anda yang dapat dibajak atau dicuri oleh orang lain.
3. **VPN (Virtual Private Network)**
   Jaringan pribadi virtual adalah teknologi transfer data yang memungkinkan pengguna terhubung ke jaringan publik dan menggunakannya sebagai koneksi ke jaringan lokal mereka. Ini memberi izin dan pengaturan yang sama seperti pada LAN. Salah satu permasalahan jaringan internet adalah kurangnya dukungan keamanan yang memadai.
   IP sekarang menjadi kebutuhan dasar untuk pertukaran data antara beberapa LAN yang terpisah secara spasial. VPN membantu mencegah intrusi selama transmisi data. VPN digunakan untuk menjaga kerahasiaan data, integritas data, dan validitas sumber.VPN membantu melindungi data dan informasi Anda agar tidak digunakan oleh orang lain. Jaringan publik bisa sangat berbahaya karena VPN memungkinkan mengirim dan menerima data dengan aman.
4. **Chiper**
   Chiper adalah algoritma untuk melakukan enkripsi dan inversi enkripsi. Enkripsi adalah proses melindungi informasi dengan membuatnya tidak dapat dibaca tanpa pengetahuan khusus. Karena banyak negara menggunakan enkripsi untuk melindungi komunikasi, enkripsi digunakan oleh organisasi dan individu tertentu yang sangat berkepentingan dengan kerahasiaan.
5. **Kecerdasan Buatan (Artificial Intelegent)**
   Contoh penggunaan kecerdasan buatan dalam keamanan siber adalah sistem deteksi intrusi. Sistem ini menggunakan teknik pembelajaran mesin untuk mempelajari pola serangan dan mengambil keputusan berdasarkan data dari jaringan komputer. Ketika terjadi aktivitas mencurigakan, seperti login tidak sah

atau distribusi malware, administrator dapat diperingatkan dan segera mengambil tindakan. Pembelajaran mesin juga memainkan peran penting dalam keamanan siber. Teknologi ini memungkinkan sistem komputer belajar secara otomatis dari data dan pengalaman sebelumnya.

Dengan kata lain, kecerdasan buatan dan pembelajaran mesin memainkan peran penting dalam menjaga keamanan siber. Sistem keamanan dapat mendeteksi, menganalisis, dan merespons serangan dalam menghadapi ancaman dunia maya yang semakin kompleks.

SIMPULAN

Permasalahn utama di dalam setiap lembaga ataupun perusahaan adalah sistem datanya. Dimana kemanan data merupakan salah satu komponen yang paling penting agar data yang diamankan dari perusahaan maupun data pelanggan dapat terjaga dengan baik. Berdasarkan hasil penelitian yang dilakukan bahwa terdapat beberapa langkah yang dpat diimplementasikan perusahaan untuk menjaga kemanan berdasarkan beberapa penelitian terdahulu. Salah satunya adalah melakukan pengamana dan evaluasi kerja, menggantikan *password* secara berkala, menggunakan WAF merupakan langkah yang tepat dan bijak agar dapat mendeteksi permasalahan utama dalam kemanan data yakni *cyber criem* baik di Indonesia maupun di dunia.

REFERENSI

Wulandari, I. W., & Hwihanus, H. (2023). Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan. *Jurnal Kajian dan Penalaran Ilmu Manajemen*, *1*(1), 11-25.

Sayuthi, S. (2021). Konsep Pengendalian Intern Untuk Keamanan Sistem Informasi. *Al-Buhuts*, *17*(2), 290-308.

Azis, M. S., & Safitri, J. E. (2023). Implementasi Form Log In pada Aplikasi Excel untuk Meningkatkan Keamanan Data. *PRAWARA Jurnal ABDIMAS*, *2*(03 JULI), 67-72.

Wijoyo, A., Fatimah, S., & Widianti, Y. (2023). Keamanan Data dalam Sistem Informasi Manajemen: Risiko dan Strategi Perlindungan. *TEKNOBIS: Jurnal Teknologi, Bisnis dan Pendidikan*, *1*(2).

Ramadhani, N., & Sutabri, T. (2024). ANALISIS JARINGAN 5G TERHADAP E-COMMERCE DI INDONESIA. *Scientica: Jurnal Ilmiah Sains dan Teknologi*, *2*(6), 79-83.

Hilmy, M. I., & Azmi, R. H. N. (2021). Konstruksi Pertahanan Dan Keamanan Negara Terhadap Perlindungan Data Dalam Cyberspace Untuk Menghadapi Pola Kebiasaan Baru. *Jurnal Lemhannas RI*, *9*(1), 114-124.

Laksana, T. G., & Mulyani, S. (2024). Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan. *Jurnal Ilmiah Multidisiplin*, *3*(01), 109-122.

Risqiana, R., Hayfa, J., Rani, R., & Wungkana, S. R. (2024). Implementation of Data Protection Authority (DPA) in Indonesia: The Urgency of Legal Protection of Customer's Personal Data in E-Banking Service Transactions. *Jurnal Penelitian Ilmu-Ilmu Sosial*, *5*(1), 19-33.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1211.

Huda, M. (2020). *Keamanan Informasi*. Nulisbuku. https://books.google.com/books/about/Keamanan_Informasi.html?id=CcjZDwAAQBAJ#v=onepage&q&f=false

"Indonesia Masuk 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak di Dunia", Databoks.com, pada 13 September 2022, di akses pada 23 April 2024 https://databoks.katadata.co.id/datapublish/2022/09/13/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia

"Opini: Kemanan Data di Era Transformasi Digital Bisnis", Bisnis.com, pada 07 Desember 2023, di akses pada 23 April 2024 https://m.bisnis.com/amp/read/20231207/84/1721642/opini-keamanan-data-di-era-transformasi-digital-bisnis

"Dokumen Rahasia dari 21.000 Perusahaan di Indonesa Dilaporkan bocor, ini bisa jadi alat Penipuan", News Indonesia, pada 19 Agustus 2022, di akses pada 23 April 2024 https://www.bbc.com/indonesia/majalah-62603873