DOI: https://doi.org/10.62017/wanargi

ANALISIS TINGKAT KEAMANAN DATA PERUSAHAAN YANG RENTAN TERHADAP SERANGAN CYBER DALAM SISTEM INFORMASI MANAJEMEN

Zahrani Fatni Hapsah *[1]
Muhammad Irwan Padli Nasution [2]

[1,2] Universitas Islam Negeri Sumatra Utara
*e-mail: zahranifatni@gmail.com[1], irwannst@uinsu.ac.id[2]

Abstrak

Ancaman terhadap aset penting dan keamanan file meningkat pesat. Penjahat dunia maya kini semakin canggih dan dapat mengeksploitasi kelemahan keamanan pada sistem digital. Untuk meningkatkan keamanan siber, diperlukan analisis mendalam terhadap ancaman yang dihadapi di lingkungan digital dan solusi praktis. Pada kali ini penulis akan membahas tentang analisis tingkat keamanan data perusahaan yang rentan terhadap serangan cyber dalam sistem informasi manajemen. Tujuan dari penelitian ini adalah untuk menganalisis faktor-faktor penting, mengidentifikasi isu-isu utama terkait perlindungan data perusahaan terhadap serangan siber, menganalisis dan menyarankan cara dan strategi untuk meningkatkan keamanan file dan melakukan studi tentang kasus dan ancaman serta solusi untuk dunia digital. pendekatan kualitatif yang menggunakan literatur. Peretasan, peretasan, sabotase dunia maya, dan spyware adalah beberapa ancaman kejahatan dunia maya yang paling umum di Indonesia. Mengidentifikasi, menganalisis, menangani dan mengendalikan risiko adalah seluruh aspek dari proses manajemen risiko. Untuk mengatasi ancaman ini, diperlukan tenaga ahli teknis yang dapat membantu membangun sistem keamanan nasional yang canggih dan membangun firma hukum keamanan siber. Artikel ini menawarkan pemahaman mendalam tentang kerentanan yang ada dan memberikan rekomendasi strategis untuk meningkatkan keamanan data perusahaan dalam sistem informasi manajemen, melindungi informasi rahasia, serta mencegah serangan siber potensial.

***Kata kunci** : Ancaman, keamanan data file, sistem informasi manajemen, serangan cyber, manajemen resiko*

Abstract

Threats to critical assets and file security have rapidly increased. Cybercriminals are becoming increasingly sophisticated and can exploit security vulnerabilities in digital systems. To enhance cybersecurity, a comprehensive analysis of threats within the digital environment and practical solutions is required. In this instance, the author will discuss an analysis of the level of corporate data security vulnerable to cyber-attacks in management information systems. The purpose of this research is to analyze critical factors, identify key issues related to protecting corporate data from cyber-attacks, analyze and suggest methods and strategies to enhance file security, and conduct a study on cases, threats, and solutions in the digital world using a qualitative approach supported by literature. Hacking, cyber espionage, cyber sabotage, and spyware are among the most common cybercrimes in Indonesia. Identifying, analyzing, addressing, and controlling risks are integral aspects of risk management processes. Addressing these threats necessitates technical experts to assist in building sophisticated national security systems and establishing cybersecurity legal frameworks. This article provides an in-depth understanding of existing vulnerabilities and offers strategic recommendations to improve corporate data security within management information systems, safeguarding confidential information, and preventing potential cyber-attacks.

***Keywords**: Threats, file data security, management information system, cyber attack, risk management*

PENDAHULUAN

Kejahatan *cyber* merujuk pada tindakan kriminal yang dilakukan menggunakan teknologi komputer atau jaringan internet. Ini termasuk serangan perangkat lunak berbahaya, pencurian data pribadi, penipuan daring, serangan DDoS, dan kegiatan ilegal lainnya yang terjadi di ranah digital.

Seiring dengan berkembangnya teknologi informasi dan komunikasi, sistem informasi sangatlah penting bagi operasional bisnis. Orang mengandalkan sistem informasi untuk berkomunikasi melalui berbagai perangkat fisik (perangkat keras), sistem kontrol dan

DOI: https://doi.org/10.62017/wanargi

pemrosesan informasi (perangkat lunak), jaringan, dan infrastruktur data. Oleh karena itu, banyak orang yang menganggap manfaat sistem informasi sangat penting dalam rencana bisnisnya. Sistem informasi dapat mengumpulkan, mengatur dan menyediakan informasi yang membantu manajemen perusahaan untuk mengambil keputusan dan rencana, untuk bekerja dan untuk meningkatkan penjualan barang yang di produksi.

Ancaman terhadap keamanan data dan file penting meningkat pesat. Penjahat dunia maya menjadi lebih pintar dan terampil dalam mengeksploitasi kerentanan keamanan dalam sistem digital, termasuk serangan malware, peretasan, dan serangan jaringan yang canggih. Selain itu, seiring dengan semakin banyaknya data yang dikirim dan disimpan secara elektronik, tantangan dalam melindungi file menjadi lebih kompleks. Oleh karena itu, diperlukan analisis mendalam terhadap ancaman yang dihadapi di lingkungan digital dan solusi yang dapat diterapkan untuk meningkatkan keamanan siber. Kajian terhadap serangan yang terjadi dan tindakan yang diambil untuk mengatasinya sangat penting untuk memahami kompleksitas dan tantangan yang dihadapi dalam melindungi hal dan file penting.

Dalam beberapa tahun terakhir, dunia telah mengalami beberapa kasus pelanggaran keamanan data yang cukup besar, seperti yang terjadi pada tahun 2022 lalu Indonesia juga baru saja mengalami peretasan akun data menkominfo RI, Marriott International dan kasus Facebook-Cambridge Analytica. Oleh karena itu, keamanan data dan privasi pengguna menjadi sangat penting untuk diperhatikan dan ditingkatkan kualitas keamanannya oleh perusahaan.

Berbicara mengenai sistem informasi dan penyimpanan file, kali ini saya akan membahas tentang keamanan data perusahaan yang rentan terhadap serangan cyber dalam sistem informasi manajemen. Menarik pembicaraan tentang bagaimana penerapan sistem informasi serta sistem keamanan pada perusahaannya.

METODE

Metode penelitian merupakan serangkaian prosedur dan teknik yang digunakan untuk mengumpulkan data, menganalisis informasi, dan menjawab pertanyaan penelitian dalam suatu studi atau penelitian ilmiah. Metode penelitian dapat meliputi pendekatan, teknik pengumpulan data, analisis data, serta langkah-langkah yang digunakan dalam suatu studi ilmiah.

Metode penelitian yang digunakan dalam penelitian ini yaitu metode kualitatif dan melibatkan studi literatur yang berfokus pada sistem informasi manajemen dan sistem manajemen keamanan pada perusahaan. mengkaji berbagai dokumen, buku, dan jurnal terkait. untuk mengetahui bagaimana perusahaan meningkatkan perlindungan data dan privasi pengguna melalui pengelolaan data yang efektif. Hasil peninjauan dokumen akan dianalisis untuk mengidentifikasi titik-titiik lemah dalam keamanan data perusahaan. Pendekatan ini memberikan pemahaman yang komprehensif tentang kerentanan yang mungkin terjadi dan solusi yang efektif.

HASIL DAN PEMBAHASAN

Analisis Tingkat Keamanan Data

Hasil analisis menunjukkan bahwa perusahaan-perusahaan tertentu memiliki kerentanan tertentu dalam Sistem Informasi Manajemen mereka. Diantaranya adalah kurangnya enkripsi data, kelemahan pada sistem otentikasi, dan kurangnya pembaruan perangkat lunak yang menyebabkan ketidakstabilan keamanan.

Hasil analisis juga menunjukkan bahwa beberapa area dalam Sistem Informasi Manajemen memiliki tingkat keamanan yang rendah, meningkatkan risiko terhadap serangan cyber. Faktor-faktor seperti kurangnya pelatihan keamanan bagi pengguna, kebijakan keamanan yang kurang jelas, dan pembaruan sistem yang tidak teratur menjadi penyebab utama.

Perusahaan yang sadar akan pentingnya keamanan informasi dan mengikuti pelatihan terkait menjadi parameter yang relevan.

Tabel 1

Parameter	Hasil Pengamatan	Evaluasi

DOI: https://doi.org/10.62017/wanargi

Pemahaman perusahaan mengenai signifikansi keamanan sistem informasi di lingkungan perusahaan	Perusahaan menyadari pentingnya keamanan informasi, tetapi kurang pemahaman menyeluruh terhadap program-program yang diimplementasikan	Pembaruan dan kembali menginformasikan mengenai kepentingan menjaga keamanan informasi
Kesadaran perusahaan dalam melindungi sistem dari resiko serangan cyber, virus dan malware	Perusahaan menyadari betapa pentingnya melindungi data perusahaan dari serangan cyber dan virus, namun masih terdapat tantangan dalam mendeteksi keberadaan virus dan serangan cyber	Pembaruan dan memberikan presentasi mengenai resiko serangan cyber dan virus yang bisa merusak sistem
Pelatihan terkait keamanan	Meskipun pelatihan telah dilaksanakan, belum semua bagian perusahaan menerima pelatihan tersebut	Pembaruan dan mengadakan pelatihan menyeluruh

Potensi bahaya kejahatan siber (cyber crime) bisa memiliki dampak terhadap pertempuran siber, dan berikut adalah beberapa kemungkinan ancaman kejahatan siber di perusahaan-perusahaan Indonesia:

a. Peretasan (*Hacking*)

Hacking merujuk pada proses atau kegiatan di mana seseorang, yang biasa disebut hacker, mencoba untuk memanipulasi, mengakses, atau mengubah informasi yang ada dalam suatu sistem komputer atau jaringan, seringkali tanpa izin atau pengetahuan pemiliknya. Aktivitas hacking dapat dilakukan dengan berbagai niat, mulai dari tujuan yang bersifat eksploratif dan peningkatan keamanan hingga tindakan yang merusak atau mencuri data.

Hacker dapat menggunakan berbagai metode untuk mencapai tujuan mereka. Ini bisa melibatkan penggunaan perangkat lunak atau teknik khusus, seperti mencari celah keamanan (*exploits*) dalam perangkat lunak atau sistem operasi, melakukan serangan phishing untuk mendapatkan informasi login, atau menggunakan serangan brute force untuk menebak kata sandi.

Pembobolan keamanan dapat disebabkan oleh berbagai faktor, termasuk keinginan iseng untuk menguji keamanan sistem hingga ketidaksetujuan terhadap pemerintah. Contoh kasus seperti yang terjadi pada perusahaan keuangan atau bank BSI Kebocoran data juga menimpa bank yang berstatus badan usaha milik negara (BUMN), yakni Bank Syariah Indonesia (BSI). Kasus hacker ini baru-baru ini terjadi dan berhasil membetot perhatian masyarakat. Total data yang bocor mencapai 1,5 TB dan dari seluruh data yang dicuri, 15 juta diantaranya adalah data pengguna dan password untuk akses internal dan layanan yang digunakan bank. Kebocoran data juga mencakup juga data karyawan, dokumen keuangan, dokumen legal, NDA, dan masih banyak lagi. Data pelanggan yang bocor diantranya nama, nomor hp, alamat, saldo rekening, histori transaksi, tanggal pembukaan rekening, informasi pekerjaan, dan lain-lain.

Pada tahun 2004 silam juga terjadi kasus dimana hacker bernama Xnuxer atau Dani Firmansyah berhasil membobol situs KPU seharga Rp 152 miliar. Kala itu Xnucer mengotak-atik halaman web dan informasi di dalamnya. Hacker asal Jogja tersebut mengubah nama partai menjadi Partai Si Yoyo, Partai Kolor Ijo, Partai Dibenerin Dulu Webnya, dan sebagainya. Ia juga sempat mencoba mengubah hasil perolehan suara, meskipun gagal.

Lalu adapun kasus lain seperti kasus kebocoran data SIM card. Kebocoran ini menyebabkan data pribadi para pendaftar nomor HP dengan NIK dan KK tersebar luas di forum hacker breached.to. Tersangkanya adalah Bjorka. Tak tanggung-tanggung, jumlah kebocoran

DOI: https://doi.org/10.62017/wanargi

mencapai lebih dari 1,3 miliar data yang mencakup NIK, No HP, provider, tgl registrasi, yang mana ukuran file utuhnya menyentuh 87 GB dengan format CSV.

Tidak hanya masyarakat biasa, kebocoran data juga dialami bahkan oleh sejumlah petinggi negara. Yang paling sering menjadi target adalah data milik Menkominfo, Johnny G. Plate yang sebelumnya juga sempat panas berselisih dengan hacker Bjorka.

b. Cracking

Cracking adalah istilah yang merujuk pada proses mengatasi atau mengeksploitasi sistem keamanan untuk memodifikasi atau melepas proteksi dari suatu perangkat lunak atau sistem. Tindakan cracking ini seringkali dilakukan tanpa izin dan bertujuan untuk mendapatkan akses atau fungsionalitas yang tidak sah, seperti menggunakan perangkat lunak tanpa membayar lisensinya. Berbeda dengan hacking yang dapat mencakup berbagai niat, cracking secara khusus terfokus pada melewati atau menghilangkan mekanisme perlindungan.

Ada beberapa metode yang digunakan dalam cracking, termasuk:

1. *Reverse Engineering* : Menganalisis perangkat lunak atau sistem untuk memahami cara kerjanya dan mencari cara untuk melewati proteksi yang diterapkan.
2. *Patching* : Mengidentifikasi dan mengubah bagian-bagian tertentu dari perangkat lunak atau sistem untuk menghilangkan atau menonaktifkan mekanisme perlindungan.
3. *Keygenning* : Menciptakan atau menghasilkan kunci lisensi palsu untuk mengakali sistem yang memerlukan kunci untuk mengaktifkan fungsi tertentu.

Cracking seringkali bertentangan dengan hukum hak cipta dan lisensi perangkat lunak. Aktivitas ini dapat merugikan pengembang perangkat lunak dengan mengurangi pendapatan yang seharusnya mereka terima dari penjualan lisensi. Oleh karena itu, cracking dianggap ilegal dalam banyak yurisdiksi.

Perusahaan sering mengambil langkah-langkah untuk meningkatkan keamanan dan mencegah cracking, seperti penggunaan teknik enkripsi yang kuat, perlindungan perangkat lunak dengan lisensi yang ketat, dan pemantauan keamanan yang aktif.

Di Indonesia, terdapat insiden peretasan yang dilakukan oleh seseorang yang dikenal sebagai "*carder*." Mereka menggunakan teknik ini untuk mencuri informasi kartu kredit dengan cara mengamati dan mengawasi data kartu kredit dari para nasabah. Setelah berhasil mengakses informasi tersebut, peretas-peretas ini berupaya untuk mendapatkan akses ke data sensitif dan kekayaan simpanan nasabah di bank guna mendapat keuntungan pribadi.

c. Cyber Sabotage

Cyber sabotage adalah bentuk serangan cyber yang dilakukan secara sengaja untuk merusak, mengganggu, atau menghancurkan data, sistem, atau infrastruktur jaringan komputer yang terhubung ke internet. Cyber sabotage ini juga merupakan tindakan paling ditakuti banyak perusahaan-perusahaan besar di seluruh dunia.

Tujuan utama dari serangan ini adalah menyebabkan kerusakan yang signifikan pada operasional organisasi atau individu yang menjadi target. Metode yang digunakan dalam cyber sabotage bisa bervariasi, mulai dari merusak data, mengganggu kinerja sistem, hingga menciptakan kekacauan dalam operasional suatu entitas.

Serangan cyber sabotage dapat menyasar berbagai sektor, termasuk perusahaan, pemerintahan, atau individu. Penyerang seringkali menggunakan berbagai teknik seperti malware, ransomware, serangan DDoS (Distributed Denial of Service), atau bahkan insiden pencurian data untuk mencapai tujuan mereka. Dampak dari cyber sabotage dapat mencakup kerugian finansial, reputasi yang rusak, atau bahkan potensi risiko keamanan nasional tergantung pada target yang dipilih.

Menghadapi ancaman ini, organisasi dan individu perlu mengimplementasikan langkah-langkah keamanan cyber yang kuat, termasuk pemantauan sistem yang efektif, perlindungan terhadap malware, dan kebijakan keamanan informasi yang ketat. Kesadaran akan potensi risiko

DOI: https://doi.org/10.62017/wanargi

dan langkah-langkah pencegahan menjadi kunci dalam melindungi diri dari serangan cyber sabotage.

d. Spyware

Spyware adalah jenis perangkat lunak berbahaya yang dirancang untuk mengumpulkan informasi dari perangkat atau komputer target tanpa sepengetahuan atau izin pengguna. seperti merekam data *cookies* atau registry. Setelah data tercatat, informasi tersebut dapat dikirim atau dijual kepada perusahaan atau individu tertentu. Kemudian, mereka dapat memanfaatkan informasi tersebut untuk mengirimkan iklan yang tidak diinginkan atau menyebarkan virus berbahaya. Sayangnya, di Indonesia telah banyak terjadi insiden infeksi *malware* terkait penggunaan layanan perbankan online oleh masyarakat. Berikut adalah beberapa karakteristik dan rincian terkait *spyware*:

1. Infiltrasi Diam-Diam : *Spyware* sering masuk ke dalam sistem tanpa sepengetahuan pengguna. Ini dapat terjadi melalui unduhan perangkat lunak yang meragukan, lampiran email berbahaya, atau eksploitasi kelemahan keamanan dalam perangkat lunak.
2. Aktivitas Pengawasan : Setelah terpasang, *spyware* memantau aktivitas pengguna tanpa sepengetahuan mereka. Ini dapat mencakup pemantauan penelusuran web, catatan ketikan, dan akses ke file atau data pribadi.
3. Pencurian Informasi : *Spyware* dirancang untuk mencuri informasi pribadi seperti kata sandi, nomor kartu kredit, data keuangan, dan informasi identitas lainnya. Informasi ini kemudian dapat digunakan untuk tujuan yang merugikan, seperti pencurian identitas atau penipuan keuangan.
4. Pengiriman Data ke Pihak Ketiga : Data yang dikumpulkan oleh *spyware* sering dikirimkan ke pihak ketiga yang menciptakan atau mengendalikan *spyware* tersebut. Hal ini dapat menyebabkan pelanggaran privasi serius dan potensi risiko keamanan.
5. Penyebaran Melalui Metode Tertentu : *Spyware* dapat menyebar melalui berbagai metode, termasuk unduhan tidak sah, perangkat lunak palsu, atau serangan melalui email. Pengguna yang tidak waspada terhadap sumber perangkat lunak yang mereka unduh atau tautan yang mereka buka dapat menjadi korban *spyware*.
6. Efek Terhadap Kinerja Sistem : Keberadaan spyware dapat merugikan kinerja sistem. Proses pengawasan dan pengumpulan data dapat menghabiskan sumber daya sistem, menyebabkan penurunan kecepatan, dan bahkan menyebabkan crash sistem.
7. Upaya Penghapusan Sulit : Spyware sering dirancang untuk menyembunyikan dirinya dan membuatnya sulit dihapus. Beberapa spyware dapat memodifikasi konfigurasi sistem atau menyembunyikan diri di lokasi yang sulit diakses.
8. Perlindungan Melalui Keamanan Perangkat Lunak : Untuk melawan spyware, pengguna seringkali perlu mengandalkan perangkat lunak keamanan seperti antivirus dan antispyware. Namun, penting untuk selalu memperbarui perangkat lunak keamanan agar dapat mendeteksi varian spyware terbaru.

Pengenalan kontrol keamanan

Adapun sejumlah kontrol keamanan yang dapat diterapkan perusahaan untuk meningkatkan tingkat keamanan data perusahaan termasuk di antaranya implementasi enkripsi yang kuat, pembaruan sistem teratur, dan peningkatan kesadaran keamanan bagi pengguna Sistem Informasi Manajemen. Dan untuk Untuk mengurangi risiko keamanan data, perusahaan dapat mengimplementasi strategi mitigasi yang melibatkan kombinasi kebijakan keamanan yang diperbarui, pelatihan keamanan bagi pengguna, dan penerapan sistem deteksi intrusi. Penggunaan teknologi keamanan terkini juga diperlukan untuk melindungi data perusahaan secara menyeluruh.

DOI: https://doi.org/10.62017/wanargi

KESIMPULAN

Pencurian informasi dan data rahasia merupakan ancaman serius dalam ranah kejahatan siber, yang ditujukan untuk menyerang individu, lembaga pemerintah, dan sektor militer, berpotensi mengancam keamanan nasional suatu negara. Oleh karena itu, penting untuk menerapkan manajemen risiko yang terfokus pada informasi dan komunikasi guna mengurangi potensi kerentanan terhadap penyalahgunaan data di dunia maya, yang dapat berdampak signifikan pada banyak warga negara dan informasi bersifat rahasia. Selain memperkuat pertahanan negara, dukungan hukum yang terintegrasi dan saling mendukung juga menjadi krusial dalam menghadapi ancaman kejahatan siber.

Penting bagi perusahaan untuk menerapkan langkah-langkah keamanan yang holistik dalam Sistem Informasi Manajemen untuk melindungi data perusahaan dari serangan cyber. Implementasi kebijakan yang jelas, pelatihan secara berkala, dan pembaruan teknologi keamanan dapat membantu mengurangi risiko secara signifikan.

DAFTAR PUSTAKA

Farizy, Salman & Emi Sita Eriana. (2022). Keamanan Sistem Informasi. Unpam press

Susanto, Edy. Achmad, Romadhon, dkk. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. Jurnal Penelitian Bisnis dan Manajemen (1),172-191.

Soesanto, Edy. Alfonso, Lande. Dkk. (2023). Analisis Sistem Manajemen Keamanan Di Perusahaan Tokopedia Dalam Menigkatkan Proteksi Data Dan Privasi Pengguna. Kewirausahaan dan Manajemen Bisnis (1), 21-29.

Soesanto, Edy. Vina, Damayanti. Dkk. (2023). Tinjauan Mengenai Sistem Informasi Dan Keamanan Informasi Pada PT Trinusa Travelindo. (6), 967-976.

Yudha, Tangguh. (2023, 7 Mei). 5 Kasus Hacker Paling Menggemparkan di Indonesia. Techno.Okezone.com. https://techno.okezone.com/amp/2023/05/17/54/2815549/5-kasus-hacker-paling-menggemparkan-di-indonesia?page=1

Zulkarnain. (2020). Analisis Implementasi Keamanan Sistem Informasi pada Perusahaan Perakitan Elektronik. Sistem informasi dan teknologi (01), 1-3.