HUMANITIS: Jurnal Humaniora, Sosial dan Bisnis
Vol. 2 No. 7 Juli 2024, hal. 711-718 e-ISSN: 2988-6287

ANALISIS TINGKAT KEAMANAN DATA PADA SALAH SATU KANTOR PERPAJAKAN DI BEKASI YANG RENTAN TERHADAP SERANGAN CYBER DALAM SISTEM KEUANGAN

Ahmad Septian*[1], Teuku Alfiansyah[2], Aji Dewa Abdulla[3], Hedi Sutiawan[4] , Dwi Ali Ega Fauzi[5], Dimas Hadi Saputra[6], Tubagus Hedi Saepudin[7]
Prodi Teknik Industri, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya
Email : *[1]202210215054@mhs.ubharajaya.ac.id, [2]202210215062@mhs.ubharajaya.ac.id, [3]202210215069@mhs.ubharajaya.ac.id, [4]202210215059@mhs.ubharajaya.ac.id, [5]202210215061@mhs.ubharajaya.ac.id, [6]202210215019@mhs.ubharajaya.ac.id, [7]tubagus.hedi@dsn.ubharajaya.ac.id

Abstract

Cybercrime refers to crimes committed using computer technology or the Internet. This includes malicious attacks, theft of personal data, online fraud, and other illegal activities in the digital world. Tax accounting is a financial recording activity in a business entity or institution to find out the amount of tax that must be paid, technically apart from functioning to find out the amount of tax that must be paid. taxpayers must pay, this accounting branch also has other functions such as annual tax documentation, financial reports, analytical materials to determine the amount of tax that must be paid. Threats to the security of financial data are growing rapidly. Cybercriminals are increasingly sophisticated and able to exploit security vulnerabilities in digital systems, including malicious attacks, hacking and sophisticated network attacks. In recent years, there have been quite large cases of data security breaches, such as what happened in 2021. hacking of financial system data at one of the tax offices. Therefore, data security is very important to pay attention to and improve the quality of security by the office. The research method used in this research is a qualitative method and involves a literature study that focuses on financial management systems and security management systems in offices. reviewing various related documents, books and journals to find out how pe.

Keywords : *Cyber Security,Finance,Taxation.*

Abstrak

Kejahatan Cyber mengacu pada kejahatan yang dilakukan dengan menggunakan teknologi komputer atau Internet. Ini termasuk serangan jahat, pencurian data pribadi, penipuan online,dan aktivitas ilegal lainnya di dunia digital,Akutansi perpajakan adalah sebuah aktivitas pencatatan keuangan pada sebuah badan usaha atau lembaga untuk mengetahui jumlah pajak yang harus dibayarkan,secara teknis selain berfungsi untuk mengetahui besaran pajak yang harus dibayar wajib pajak,cabang akutansi ini juga memiliki fungsi lain seperti sebagai dokumentasi perpajakan tahunan,laporan keuangan,bahan analisis untuk mengetahui besaran pajak yang hatrus dibayar, Ancaman terhadap keamanan data keuangan berkembang pesat. Penjahat dunia maya semakin canggih dan mampu mengeksploitasi kerentanan keamanan dalam sistem digital, termasuk serangan berbahaya, peretasan, dan serangan jaringan yang canggih, Dalam beberapa tahun terakhir, telah terjadi kasus pelanggaran keamanan data yang cukup besar, seperti yang terjadi pada tahun 2021 lalu telah terjadi peretasan data sistem keuangan di salah satu kantor pajak. Oleh karena itu, keamanan data menjadi sangat penting untuk diperhatikan dan ditingkatkan kualitas keamanannya oleh Kantor tersebut,

Metode penelitian yang digunakan dalam penelitian ini yaitu metode kualitatif dan melibatkan studi literatur yang berfokus pada sistem manajemen keuangan dan sistem manajemen keamanan pada perkantoran. mengkaji berbagai dokumen, buku, dan jurnal terkait untuk mengetahui bagaimana perkantoran meningkatkan perlindungan data keuangan melalui pengelolaan data yang efektif
Keywords : Keamanan Cyber,Keuangan,Perpajakan

PENDAHULUAN

Kejahatan Cyber mengacu pada kejahatan yang dilakukan dengan menggunakan teknologi komputer atau Internet. Ini termasuk serangan jahat, pencurian data pribadi, penipuan online,dan aktivitas ilegal lainnya di dunia digital.

Akutansi perpajakan adalah sebuah aktivitas pencatatan keuangan pada sebuah badan usaha atau lembaga untuk mengetahui jumlah pajak yang harus dibayarkan,secara teknis selain berfungsi untuk mengetahui besaran pajak yang harus dibayar wajib pajak,cabang akutansi ini juga memiliki fungsi lain seperti sebagai dokumentasi perpajakan tahunan,laporan keuangan,bahan analisis untuk mengetahui besaran pajak yang hatrus dibayar(Rahmawati & Kumalasari, 2021)

Sistem keuangan adalah sistem yang mencakup infrastruktur keuangan, termasuk lembaga jasa keuangan, pasar keuangan, dan sistem pembayaran, serta merupakan sistem yang mendukung kegiatan perekonomian suatu negara dengan mengelola pengumpulan dan distribusi dana masyarakat. Sistem keuangan memegang peranan penting dalam perekonomian nasional. Sebagai bagian dari sistem perekonomian, sistem keuangan berfungsi mendistribusikan uang dari pihak yang surplus kepada pihak yang bermasalah.(Malaha et al., 2020)

Ancaman terhadap keamanan data keuangan berkembang pesat. Penjahat dunia maya semakin canggih dan mampu mengeksploitasi kerentanan keamanan dalam sistem digital, termasuk serangan berbahaya, peretasan, dan serangan jaringan yang canggih. Selain itu, seiring dengan semakin banyaknya data yang dikirim dan disimpan secara elektronik, masalah penyimpanan file menjadi lebih mendesak. Oleh karena itu, diperlukan kajian mendalam mengenai ancaman yang dihadapi lingkungan digital dan solusi yang dapat diterapkan untuk meningkatkan internet. Untuk memahami kompleksitas dan tantanganyang terkait dengan perlindungan sumber daya dan file sensitif, penting untuk memeriksaserangan yang terjadi dan cara mengatasinya.

Dalam beberapa tahun terakhir, telah terjadi kasus pelanggaran keamanan data yang cukup besar, seperti yang terjadi pada tahun 2021 lalu telah terjadi peretasan data sistem keuangan di salah satu kantor pajak. Oleh karena itu, keamanan data menjadi sangat penting untuk diperhatikan dan ditingkatkan kualitas keamanannya oleh Kantor tersebut.

berbicara mengenai sistem keuangan, kali ini peneliti akan membahas tentang keamanan data salah satu kantor pajak yang rentan terhadap serangan cyber dalam sistem keuangan,Menarik pembicaraan tentang bagaimana penerapan sistem keuangan serta sistem keamanan pada kantor tersebut

METODE PENELITIAN

Metode penelitian adalah seperangkat metode dan teknik yang digunakan untuk mengumpulkan data, menganalisis informasi, dan menjawab pertanyaan penelitian dalam suatu penelitian atau penyelidikan ilmiah. Metode penelitian dapat mencakup metodologi, metode pengumpulan data, analisis data, dan metode yang digunakan dalam penelitian ilmiah(Adlini et al., 2022)

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

HASIL DAN PEMBAHASAN

No	Author (th)	Hasil riset	Persamaan	Perbedaan
1	(Herdiana et al., 2021)	Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid19	Membahas mengenai Siber	Membahas mengenai ancaman resiko keamanan siber
2	(Munte, 2021)	Analisis keamanan siber dan hukum pidana dari Perspektif gender dan filsafat politik alison M. Jaggar	Membahas mengenai siber	Metode yang digunakan yaitu metode kepustakaan dengan teknik analisa teori legal feminis dan filsafat politik Alison M. Jaggar
3.	(Ilhami, 2022)	Data Privasi dan Keamanan Siber pada Smart-City: Tinjauan Literatur	Membahas mengenai siber	Metodologi penelitian ini membahas mengenai bagaimana alur dalam tinjauan literatur untuk memperjelas arah penelitian dalam artikel
4.	(Makbull Rizki, 2022)	Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi	Membahas mengenai siber	Metode yang dipakai pada penelitian ini pendekatan penelitian kualitatif dengan metode studi kasus

5.	(Baidoi et al., 2023)	Implementasi algoritma advanced encryption Standard untuk pengamanan file pada smp negeri 189 jakarta barat	Membahas mengenai pengamanan file	Metode yang digunakan yaitu metode waterfal
6.	(Mauliza et al., 2022)	Pengaruh Perlindungan Data dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat di Surabaya	Membahas mengenai pengamanan cyber	Perlindungan data berdampak pada peningkatan kepercayaan masyarakat Surabaya terhadap penggunaan fintech.
7	(Vania et al., 2023)	Injauan yuridis terhadap perlindungan data pribadi dari aspek pengamanan data dan keamanan siber	Membahas mengenai perlindungan data	Dalam penelitian ini penulis menggunakan metode penelitian hukum normatif melalui penelitian kepustakaan, mengacu pada hukum tertulis, hukum baik dan sumber hukum lainnya.

Hasil Analisis tersebut mengungkapkan adanya kerentanan pada sistem pengelolaan keuangan departemen perpajakan. Hal ini mencakup kurangnya enkripsi data, kerentanan dalam sistem otentikasi, dan kurangnya pembaruan perangkat lunak yang mengakibatkan kurangnya keamanan.

Hasil analisis juga menunjukkan bahwa beberapa area dalam Sistem manajemen keuangan memiliki tingkat keamanan yang cukup 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

Parameter	Hasil Pengamatan	Evaluasi
Pemahaman kantor mengenai signifikansi keamanan sistem keuangani di lingkungan perusahaan	kantor menyadari pentingnya keamanan sistem keuangan, tetapi kurang pemahaman menyeluruh terhadap program-program yang diimplementasikan	Pembaruan dan kembali menginformasikan mengenai kepentingan menjaga keamanan sistem keuangan
Kesadaran kantor dalam melindungi sistem dari resiko serangan cyber, virus dan malware	kantor menyadari betapa pentingnya melindungi data sistem keuangan 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 perkantoran menerima	Pembaruan dan mengadakan pelatihan menyeluruh

	pelatihan tersebut	

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

1. *Hacking*

   Hacking (peretas) mengacu pada tindakan atau praktik di mana seseorang, yang dikenal sebagai hacker, berupaya memanipulasi, mengakses, atau mengubah informasi yang terkandung dalam sistem atau jaringan komputer, biasanya tanpa izin dan sepengetahuan pemiliknya. Aktivitas peretasan bisa memiliki banyak tujuan, mulai dari memata-matai, meningkatkan keamanan, membobol, atau mencuri data.

   Hacking dapat menggunakan berbagai metode untuk mencapai tujuannya. Hal ini dapat mencakup penggunaan perangkat lunak atau teknik khusus seperti eksploitasi pada perangkat lunak atau sistem operasi, melakukan serangan phishing untuk mendapatkan informasi login, 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,seperti contoh Pada tahun 2021 lalu terjadi kasus dimana hacker berinisial O berhasil mengubah sistemn keuangan dan meraup uang ratusan juta rupiah. Kala itu O mengotak-atik halaman web dan informasi di dalamnya. Hacker asal bekasi tersebut mengubahrekening kantor menjadi ekening pribadi yang seharusnya uang pembayaran pajak masuk ke rekening kantor tetapi ini malah masuk ke rekening pribadi O

2. *Cracking*

   Cracking adalah istilah yang mengacu pada proses mengatasi atau menggunakan sistem keamanan untuk mengubah atau menghapus fitur keamanan komputer atau sistem. Operasi peretasan ini dilakukan tanpa izin dan bertujuan untuk mendapatkan akses atau aktivitas tidak sah, seperti menggunakan perangkat lunak tanpa membayar lisensi. Berbeda dengan peretasan yang melibatkan berbagai tujuan, peretasan berfokus pada pelanggaran atau perusakan langkah-langkah keamanan.

   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 sering kali melanggar undang-undang hak cipta dan lisensi perangkat lunak. Praktik-praktik ini dapat merugikan pengembang perangkat lunak karena mengurangi pendapatan yang mereka peroleh dari penjualan lisensi. Oleh karena itu, crack dianggap ilegal di banyak yurisdiksi.

Perkantoran sering kali mengambil langkah untuk memperkuat keamanan dan mencegah pelanggaran, termasuk menggunakan teknologi enkripsi yang kuat, melindungi komputer dengan lisensi yang ketat, dan pemantauan keamanan.

Di Indonesia, seseorang yang dikenal sebagai "Carder" melakukan operasi peretasan. Mereka menggunakan teknologi ini untuk mencuri informasi kartu kredit dengan memindai dan memantau rincian kartu kredit pelanggan. Setelah berhasil mengakses informasi tersebut, peretas mencoba mengakses data rahasia bank dan simpanan nasabah untuk mendapatkan kekayaan pribadi.

3. *Cyber sabotage*

Merupakan jenis serangan siber yang dilakukan dengan tujuan untuk merusak, mengganggu, atau menghancurkan data, sistem, atau infrastruktur jaringan komputer yang terhubung ke Internet. Tujuan utama serangan ini adalah menyebabkan gangguan signifikan terhadap operasional dari suatu organisasi atau individu. Metode yang digunakan dalam sabotase dapat mengakibatkan rusaknya data, terganggunya kinerja sistem, atau terciptanya gangguan dalam operasional entitas.Serangan siber dapat menargetkan banyak sektor, termasuk perusahaan, pemerintah, dan individu. Penyerang menggunakan banyak metode untuk mencapai tujuannya, termasuk malware, ransomware, serangan penolakan layanan (DDoS), dan bahkan pencurian data. Dampak dari cyberbullying dapat mencakup hilangnya pendapatan, rusaknya reputasi, atau risiko terhadap keamanan nasional, tergantung pada targetnya.Organisasi dan individu yang menghadapi ancaman ini harus menerapkan langkah-langkah keamanan siber, termasuk pemantauan sistem, pencegahan malware, dan kebijakan keamanan informasi. Penting untuk memahami potensi risiko dan mengambil tindakan pencegahan untuk melindungi diri Anda dari serangan sabotase dunia maya.

4. *Spyware*

Spyware adalah jenis perangkat lunak berbahaya yang dirancang untuk mengumpulkan informasi dari perangkat atau komputer tanpa sepengetahuan atau persetujuan pengguna. Cookie, data pendaftaran, dll. Setelah data dicatat, informasi tersebut dapat ditransfer ke perusahaan swasta atau individu. Mereka mungkin menggunakan informasi tersebut untuk mengirimi iklan yang tidak diinginkan atau menyebarkan virus berbahaya. Namun, di Indonesia terdapat banyak 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

Ada sejumlah kontrol keamanan yang dapat diterapkan perkantoran untuk meningkatkan tingkat keamanan data dalam sistem keuangan, termasuk menerapkan enkripsi yang kuat, memperbarui sistem secara berkala, dan meningkatkan keamanan sistem manajemen keuangan. Dan untuk mengurangi risiko keamanan data, lembaga dapat menerapkan strategi mitigasi yang menggabungkan kebijakan keamanan yang diperbarui, pelatihan keamanan bagi karyawan, dan penerapan sistem deteksi intrusi. Penggunaan teknologi keamanan terbaru diperlukan untuk melindungi semua data kantor.

KESIMPULAN

Pencurian informasi dan data rahasia merupakan ancaman besar dalam dunia kejahatan cyber, yang bertujuan menyerang individu, lembaga pemerintah, dan sektor militer, serta dapat menimbulkan risiko bagi keamanan suatu negara. Oleh karena itu, penting untuk menerapkan manajemen risiko yang kuat dalam sistem keuangan untuk mengurangi potensi kerentanan terhadap penyalahgunaan data di dunia maya, yang dapat merugikan banyak orang dan informasi sensitif. Menanggapi ancaman dunia maya, penting untuk memperkuat pertahanan negara dan memberikan dukungan hukum terpadu dan saling mendukung.Penting bagi perusahaan untuk menerapkan semua langkah keamanan dalam sistem informasi manajemennya untuk melindungi data perusahaan dari serangan dunia maya. Menerapkan kebijakan yang jelas, pelatihan rutin, dan pembaruan teknologi keamanan dapat mengurangi risiko.

DAFTAR PUSTAKA

Adlini, M. N., Dinda, A. H., Yulinda, S., Chotimah, O., & Merliyana, S. J. (2022). Metode Penelitian Kualitatif Studi Pustaka. *Edumaspul: Jurnal Pendidikan*, *6*(1), 974–980. https://doi.org/10.33487/edumaspul.v6i1.3394

Baidoi, N. U., Hardjianto, M., & Wibowo, A. (2023). Implementasi Algoritma Advanced Encryption Standard Untuk Pengamanan File Pada Smp Negeri 189 Jakarta Barat. *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, *2*(1), 1–9. http://senafti.budiluhur.ac.id/index.php/senafti/article/view/570

Herdiana, Y., Munawar, Z., & Indah Putri, N. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT : Information Communication & Technology*, *20*(1), 42–52. https://doi.org/10.36054/jict-ikmi.v20i1.305

Ilhami, D. A. S. (2022). Data Privasi dan Keamanan Siber pada Smart-City: Tinjauan Literatur. *Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi*, *2*(1), 51–60. https://doi.org/10.20885/snati.v2i1.19

Makbull Rizki. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *Politeia: Jurnal Ilmu Politik*, *14*(1), 54–62. https://doi.org/10.32734/politeia.v14i1.6351

Malaha, A., Dunggio, T., & Suleman, J. (2020). , 2020 Accepted: Sept. 16. *Journal Of Health, Technology And Science (JHTS)*, *1*(1), 1–6.

Mauliza, A. Y. I., Machmudi, R. D. S., & Indrarini, R. (2022). Pengaruh Perlindungan Data Dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat Di Surabaya. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, *1*(11), 2497–2516. https://doi.org/10.54443/sibatik.v1i11.395

Munte, A. (2021). Analisis Keamanan Siber Dan Hukum Dari Perspektif Gender Dan Filsafat Politik Alison M. Jaggar. *Al-Adl : Jurnal Hukum*, *13*(2), 284. https://doi.org/10.31602/al-adl.v13i2.4396

Rahmawati, M., & Kumalasari, E. I. (2021). Sistem Akuntansi Keuangan Pada CV. Prosper Media Menggunakan Zahir Accounting Versi 6.0. *Moneter - Jurnal Akuntansi Dan Keuangan*, *8*(2), 122–128. https://doi.org/10.31294/moneter.v8i2.10754

Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber. *Jurnal Multidisiplin Indonesia*, *2*(3), 654–666. https://doi.org/10.58344/jmi.v2i3.157