

IMPLEMENTASI PENGAMANAN FILE DI PT. XYZ (STUDI PUSTAKA MANAJEMEN SEKURITI)

Achmad Mahardika Dwi Anda Putra Prasetio¹, Aldy Putra Puji Siswoko², Bagus Oktavian³, Andre Satrio Trihantono⁴, Muhammad Naufal Ramadhan⁵, Sahrul Juniar Arfan⁶, Tubagus Hedi Saepudin^{7*}

Universitas Bhayangkara Jakarta Raya, Teknik Industri

Email: ¹202210215082@mhs.ubharajaya.ac.id, ²202210215086@mhs.ubharajaya.ac.id,
³202210215104@mhs.ubharajaya.ac.id, ⁴202210215081@mhs.ubharajaya.ac.id,
⁵202210215188@mhs.ubharajaya.ac.id, ⁶202110215098@mhs.ubharajaya.ac.id,
⁷tubagus.hedi@dsn.ubharajaya.ac.id

Abstract

This research analyzes the implementation of file security at PT. XYZ, is Indonesia's national energy industry which operates in the field of exploration, creation and distribution of energy resources. In facing cyber security threats such as hacker attacks, data theft and sabotage, PT. XYZ must guarantee the security of information and the integrity of files stored in their systems. This research uses qualitative methods and a literature review to evaluate the steps taken by PT. XYZ in protecting sensitive information and maintaining the trust of customers and business partners. The analysis results show that PT. XYZ has implemented several file security practices, including access control, data encryption, backup and recovery, activity monitoring, security policy settings, and security training and awareness. This implementation is expected to provide guidelines and recommendations for improving information security in the oil and gas industry sector.

Keywords: File Security, Information Security, PT. XYZ.

Abstrak

Penelitian ini menganalisis implementasi pengamanan file di PT. XYZ, sebuah industri energi nasional Indonesia yang bergerak dalam eksplorasi, penciptaan, dan distribusi sumber daya energi. Dalam menghadapi ancaman keamanan cyber seperti serangan hacker, pencurian data, dan sabotase, PT. XYZ harus memastikan keamanan informasi dan integritas file yang disimpan dalam sistem mereka. Penelitian ini menggunakan metode kualitatif dan kajian literatur untuk mengevaluasi langkah-langkah yang diambil PT. XYZ dalam melindungi informasi sensitif dan menjaga kepercayaan pelanggan serta mitra bisnis. Hasil analisis menunjukkan bahwa PT. XYZ telah menerapkan beberapa praktik pengamanan file, termasuk pengendalian akses, enkripsi data, backup dan pemulihan, monitoring aktivitas, pengaturan kebijakan keamanan, serta pelatihan dan kesadaran keamanan. Implementasi ini diharapkan dapat memberikan panduan dan rekomendasi bagi peningkatan keamanan informasi di sektor industri minyak dan gas bumi.

Kata Kunci : Pengamanan File, Keamanan Informasi, PT. XYZ.

PENDAHULUAN

PT XYZ merupakan perusahaan energi Indonesia yang bergerak di bidang eksplorasi, produksi, dan distribusi sumber daya energi. Sebagai salah satu industri terkemuka di Indonesia, PT XYZ memiliki pengalaman luas dalam memastikan keberlangsungan operasional, menjaga informasi sensitif, dan mengatasi tantangan keamanan siber yang terus berubah di era digital. (Akbulut 2010). PT. XYZ memiliki risiko keamanan siber yang signifikan, termasuk serangan peretas, pencurian data, dan sabotase. Keamanan informasi data elektronik sangat penting bagi industri yang menggunakan fasilitas IT dan menerapkannya dalam infrastruktur (Studi et al. 2020). Tanpa sistem keamanan, informasi yang terdapat dalam sistem sangat rentan untuk dieksploitasi oleh pihak yang tidak berkepentingan (The 2021). Akibatnya, hal ini meningkatkan risiko pelanggaran data dan kejahatan digital lainnya. Ketentuan Penggunaan dan Batasan Tanggung Jawab Penggunaan

PT. XYZ juga mengalami masalah keamanan file, termasuk menjaga integritas file yang disimpan dalam sistem mereka dan melindunginya dari akses yang tidak sah. Mengingat volume dan jenis data yang dikelola oleh PT. XYZ, memastikan keamanan file sangat penting untuk melindungi informasi sensitif serta menjaga kepercayaan pelanggan dan mitra bisnis. (The 2021)

Oleh karena itu, penelitian ini bertujuan untuk menyelidiki secara mendalam implementasi keamanan informasi di PT XYZ, dengan fokus khusus pada aspek keamanan file. Dengan meninjau prosedur yang diterapkan oleh PT XYZ untuk melindungi informasi, penelitian ini diharapkan dapat memberikan wawasan berharga mengenai praktik terbaik di industri minyak dan gas. Penelitian ini diharapkan mampu mengevaluasi sejauh mana PT XYZ berhasil melindungi data penting dan infrastruktur teknologi informasinya dari berbagai ancaman. Hasil penelitian ini juga diharapkan dapat membantu PT XYZ dalam meningkatkan keamanan informasinya di masa mendatang. (Soesanto et al. 2023).

METODE PENELITIAN

Metode penulisan artikel ilmiah ini menggunakan metode kualitatif dan telaah pustaka. Penelitian ini mengkaji hipotesis serta hubungan atau perbedaan antar variabel dalam buku dan jurnal, baik offline maupun online, dengan menggunakan Mendeley, Google Scholar, media daring lainnya. Teori-teori yang relevan dipilih berdasarkan hasil dan temuan penelitian

HASIL DAN PEMBAHASAN

Pengamanan File

Menurut G.J. Simons, keamanan informasi adalah upaya untuk menghindari penipuan atau, setidaknya, mendeteksi adanya penipuan dalam sistem berbasis data, di mana data itu sendiri tidak memiliki makna fisik. (Gollmann, 1999).

Implementasi Pengaman File Pada PT. XYZ

Keamanan berkas merupakan upaya berkelanjutan untuk memastikan integritas dan keamanan berkas yang disimpan dalam sistem PT. XYZ. Langkah-langkah ini meliputi penyediaan akses yang tepat, enkripsi data, dan penggunaan tanda tangan digital untuk memvalidasi keaslian berkas. Tujuan penyimpanan berkas-berkas ini adalah untuk mencegah akses dan perubahan informasi yang tidak sah. Di PT. XYZ, Keamanan berkas merupakan strategi jangka panjang untuk memastikan integritas, kerahasiaan, dan ketersediaan berkas perusahaan. Berikut ini adalah beberapa praktik umum yang digunakan untuk manajemen file :

1. **Pengendalian Akses:** Sistem kontrol akses yang ketat diterapkan untuk memastikan bahwa hanya pengguna dengan kredensial valid yang dapat mengakses berkas. Hal ini memerlukan penerapan kontrol akses berdasarkan peran, di mana akses diberikan berdasarkan peran atau jabatan pengguna di dalam struktur organisasi.
2. **Enkripsi Data:** PT. XYZ menggunakan teknologi enkripsi untuk mengelola penyimpanan file .Enkripsi mengubah file ke dalam bentuk yang tidak dapat dibaca, kecuali menggunakan kunci enkripsi yang benar. Ini melindungi berkas dari akses tidak sah , terutama jika terjadi pelanggaran keamanan atau akses tidak sah ke data.
3. **Backup dan Pemulihan:** Perusahaan mengimplementasikan kebijakan pencadangan secara teratur untuk file-file yang krusial. Prosedur ini mencakup pembuatan cadangan secara terjadwal dan menyimpan file-file tersebut di tempat yang aman. Dalam situasi kehilangan data atau serangan, file-file tersebut dapat dipulihkan dari salinan cadangan.
4. **Monitoring Aktivitas:** PT. XYZ memantau aktivitas berkas menggunakan alat pemantauan khusus. Praktik ini berperan dalam mengidentifikasi dan mengawasi upaya akses tidak sah atau perilaku mencurigakan terhadap berkas-berkas sensitif. Pemantauan tersebut memungkinkan tanggapan yang cepat terhadap ancaman atau insiden keamanan yang muncul.
5. **Pengaturan Kebijakan Keamanan:** Perusahaan mungkin telah menerapkan pedoman keamanan untuk penggunaan dan manajemen file. Pedoman tersebut mungkin meliputi ketentuan tentang cara penyimpanan file, berbagi file, penggunaan perangkat penyimpanan eksternal, serta langkah-langkah keamanan lain yang harus diikuti oleh para karyawan.
6. **Pelatihan dan Kesadaran Keamanan:** Secara berkala , PT. XYZ dapat memberikan pelatihan kepada karyawan tentang pentingnya keamanan berkas serta rekomendasi praktik terbaik. Hal ini akan meningkatkan kesadaran karyawan mengenai isu-isu keamanan file dan mengajarkan mereka metode yang sesuai untuk melindungi file.

7. Tanda Tangan Digital: Menggunakan tanda tangan digital untuk memastikan keaslian dan integritas file, sehingga menjamin file tidak diubah oleh pihak yang tidak berwenang.

Implementasi keamanan file merupakan proses yang berkelanjutan, mengikuti perkembangan teknologi dan evolusi ancaman keamanan yang baru. Oleh karena itu, penting untuk secara konsisten memonitor tren keamanan terbaru dan mengupdate langkah-langkah keamanan sesuai kebutuhan, sehingga file-file perusahaan tetap aman. (Soesanto et al. 2023)

KESIMPULAN

Dalam konteks ini, tujuan penelitian ini adalah untuk menganalisis dan menyelidiki implementasi keamanan file di PT. XYZ. Penerapan pengamanan file pada PT. XYZ sangat penting untuk menjaga kelangsungan operasional dan keamanan perusahaan. Langkah-langkah keamanan yang efektif, serta perlindungan file dan data yang tepat, akan memungkinkan PT. XYZ melindungi dirinya dari bahaya eksternal yang dapat mempengaruhi perusahaan dan konsumennya.

DAFTAR PUSTAKA

Akbulut, Hasan Hüseyin. 2010. "No Title Μελέτη Της Μεταβολής Της Σχετιζόμενης Με Την Υγεια Ποιότητας Ζωής Ασθενών Με Καρκίνο Του Μαστού Αρχικών Σταδίων, Ένα Έτος Μετά Τη Διάγνωση." *Το Βήμα Του Ασκληπιου* 9(1):76–99.

Soesanto, Edy, Lidia Margareta Purba, Bunga Aprilia, Dwi Renaldy Putra, and Sela Dwi Putri. 2023. "Implementasi Objek Vital, Pengamanan File Dan Pengamanan Cyber Di PT Pertamina." *IJM: Indonesian Journal of Multidisciplinary* 1(1):96–105.

Studi, Program, Magister Manajemen, Sekolah Tinggi, Manajemen Ppm, Sekolah Tinggi, Manajemen Ppm, and J. W. Marriott. 2020. "PERTAMINA HULU ENERGI NUNUKAN COMPANY Muhammad Roy Urich Kusumawardhana Ningky Sasanti Munir Ancaman Terorisme Di Indonesia Menjadi Kadiv Humas Mabes Polri , Irjen Pol Nanan Pengontrol Pelaksanaan Pengeboman Di Hotel Adanya Fenomena Bahwa Beberapa Pelaku ." 17(2):166–95.

The, B. Y. 2021. "REPORT OF THE GAS , OIL , AND LIQUIDS STEERING." 1–42.