Jumek : Jurnal Manajemen dan Ekonomi Kreatif
Vol.1, No.3 Juli 2023
e-ISSN: 2964-1241; p-ISSN: 2964-1632, Hal 79-87
DOI: https://doi.org/10.59024/jumek.v1i3.116

Analisis Keamanan Informasi PT. Indofood Sukses Makmur, Tbk : Studi Kasus tentang Peran Objek Vital, Pengamanan File, dan Pengamanan Cyber

Edy Susanto[1], Alvionita Dairo Lende[2], Akmal Riza Firjatullah[3], Reza Almasyah Pratama[4]
[1,2,3,4]Ekonomi dan Bisnis, Universitas Bhayangkara Jakarta Raya
Email: edy.soesanto@dsn.ubharajaya.ac.id[1], alvionita.dairo.lende19@mhs.ubharajaya.ac.id[2], 20211025066@mhs.ubharajaya.ac.id[3], 202010325045@mhs.ubharajaya.ac.id[4]

Abstract. *Information security analysis of PT. Indofood is a case study that discusses the role of vital objects, file security, and cyber security in the company. PT. Indofood is a large company in the food and beverage industry, which faces significant information security challenges. In terms of vital objects, PT. Indofood identifies critical systems and infrastructure that must be strictly protected. A risk evaluation may have been carried out to identify potential threats and take appropriate steps to protect these vital objects. Access controls, physical safeguards, and security training may have been put in place to keep vital objects safe. File security is an important focus for PT. Indofood. Security measures implemented include access control, data encryption, regular backup and restore, and monitoring of file activity. Strict access control policies and security awareness training provide additional protection for critical company files. In cyber security, PT. Indofood uses various measures to protect their systems and networks from cyberthreats. Implementation of firewalls, network protection systems, and regular software updates helps prevent unauthorized access and keeps systems secure. Email security solutions, identity and access management, and data encryption provide an additional layer of protection against cyberattacks. High security awareness and security awareness training provided to employees helps reduce attack risk and improve response to security incidents. PT. Indofood also conducts periodic security tests to identify vulnerabilities in their systems and take necessary remedial actions. Overall, PT. Indofood has implemented strong measures in securing vital objects, file security, and cyber security. However, it is important to remember that information security is an ongoing endeavor that must be continuously updated according to the latest developments in security and technological threats.*

Keywords: *Vital Objects, File Security, Cyber Security*

Abstrak. Analisis keamanan informasi PT. Indofood merupakan studi kasus yang membahas peran objek vital, pengamanan file, dan pengamanan cyber di perusahaan tersebut. PT. Indofoodadalah perusahaan besar di sektor industri makanan dan minuman, yang menghadapi tantangan keamanan informasi yang signifikan. Dalam hal objek vital, PT. Indofoodmengidentifikasi sistem dan infrastruktur kritis yang harus dilindungi dengan ketat. Evaluasi risiko mungkin telah dilakukan untuk mengidentifikasi ancaman potensial dan mengambil langkah-langkah yang sesuai untuk melindungi objek vital tersebut. Pengendalian akses, pengamanan fisik, dan pelatihan keamanan mungkin telah diterapkan untuk menjaga keamanan objek vital. Pengamanan file menjadi fokus penting bagi PT. Indofood. Langkah-langkah keamanan yang diimplementasikan meliputi pengendalian akses, enkripsi data, backup dan pemulihan rutin, serta pemantauan aktivitas file. Kebijakan pengaturan akses yang ketat

Received April 07, 2023; Revised Mei 02, 2023; Accepted Juni 07, 2023
* Edy Susanto, edy.soesanto@dsn.ubharajaya.ac.id

dan pelatihan kesadaran keamanan memberikan perlindungan tambahan terhadap file-file penting perusahaan. Dalam pengamanan cyber, PT. Indofood menggunakan berbagai langkah-langkah untuk melindungi sistem dan jaringan mereka dari ancaman siber. Implementasi firewall, sistem proteksi jaringan, dan pembaruan perangkat lunak secara teratur membantu mencegah akses yang tidak sah dan menjaga keamanan sistem. Solusi keamanan email, manajemen identitas dan akses, serta enkripsi data memberikan lapisan perlindungan tambahan terhadap serangan siber. Kesadaran keamanan yang tinggi dan pelatihan kesadaran keamanan yang diberikan kepada karyawan membantu mengurangi risiko serangan dan meningkatkan respons terhadap insiden keamanan. PT. Indofood juga melakukan pengujian keamanan secara berkala untuk mengidentifikasi kerentanan dalam sistem mereka dan mengambil tindakan perbaikan yang diperlukan. Secara keseluruhan, PT. Indofood telah mengimplementasikan langkah-langkah yang kuat dalam mengamankan objek vital, pengamanan file, dan pengamanan cyber. Namun, penting untuk diingat bahwa keamanan informasi adalah upaya berkelanjutan yang harus terus diperbarui sesuai dengan perkembangan terkini dalam ancaman keamanan dan teknologi.

Kata kunci : Objek Vital, Pengamanan File, Pengamanan Cyber

PENDAHULUAN

Pada era digital yang semakin berkembang, keamanan informasi telah menjadi salah satu aspek yang sangat penting bagi perusahaan dalam menjaga integritas, kerahasiaan, dan ketersediaan data mereka. Dalam konteks ini, PT. Indofood, sebagai salah satu perusahaan makanan dan minuman terbesar di Indonesia, menghadapi tantangan yang sama dalam menjaga keamanan informasi mereka.

Dalam menjalankan operasionalnya, PT. Indofood mengelola berbagai aset dan komponen penting dalam infrastruktur teknologi informasi mereka. Objek vital seperti server pusat, sistem jaringan, dan basis data menjadi bagian integral dalam menyimpan dan mengelola data kritis perusahaan. Oleh karena itu, perlindungan dan pengamanan objek vital ini menjadi prioritas utama bagi PT. Indofood guna memastikan kelangsungan operasional yang stabil dan terhindar dari risiko keamanan informasi.

Selain itu, PT. Indofood juga dihadapkan pada tantangan pengamanan file, di mana file-file yang disimpan dalam sistem mereka harus terjaga integritasnya dan terhindar dari akses yang tidak sah. Mengingat jumlah dan jenis data yang dikelola oleh PT. Indofood, pengamanan file menjadi langkah penting untuk melindungi informasi sensitif dan menjaga kepercayaan pelanggan serta mitra bisnis.

Di tengah meningkatnya ancaman siber, PT. Indofood juga harus menghadapi risiko serangan cyber yang dapat mengganggu kegiatan operasional dan mencuri informasi berharga. Perlindungan terhadap serangan malware, peretasan, dan serangan siber lainnya menjadi

elemen kunci dalam upaya PT. Indofood untuk menjaga keamanan sistem komputer dan jaringan mereka.

Maka dari itu, penelitian ini bertujuan untuk melakukan analisis mendalam terhadap implementasi keamanan informasi PT. Indofood, dengan fokus pada peran objek vital, pengamanan file, dan pengamanan cyber. Dengan mempelajari langkah-langkah yang diambil oleh PT. Indofood dalam menjaga keamanan informasi, diharapkan dapat ditemukan wawasan yang berharga mengenai praktik terbaik dalam menjaga keamanan informasi di sektor industri makanan dan minuman.

Melalui analisis ini, diharapkan dapat dievaluasi keberhasilan PT. Indofood dalam melindungi objek vital, file-file penting, dan infrastruktur teknologi informasi mereka dari ancaman yang ada. Hasil dari penelitian ini juga diharapkan dapat memberikan rekomendasi dan panduan bagi PT. Indofood dalam peningkatan keamanan informasi mereka di masa yang akan datang.

METODE

Dalam penelitian ini, menurut (Firman, 2015) Metode penelitian kualitatif merupakan analisis data dilakukan selama proses pegumpulan dan setelah data dikumpulan secara keseluruhan. Beriringan dengan pengumpulan data, dilakukan analisis (interpretasi) dengan maksud mempertajam fokus pengamatan serta memperdalam masalah yang relevan dengan pokok permasalahan yang diteliti. Analisis data selama proses pengumpulan data amat penting artinya bagi peneliti untuk melakukan pengamatan terfokus terhadap permasalahan yang dikaji. Pada penelitian kali ini akan menggunakan metode kualitatif dengan pengumpulan data seperti analisis dokumen, dan tinjauan literatur untuk mendapatkan pemahaman yang komprehensif tentang keamanan informasi di PT. Indofood. Selanjutnya, analisis data yang dikumpulkan akan dilakukan untuk mengidentifikasi kelemahan yang ada serta mengusulkan langkah-langkah perbaikan yang dapat diambil oleh PT. Indofood guna memperkuat keamanan informasi mereka.

Penelitian ini memiliki relevansi yang signifikan bagi mahasiswa jurusan manajemen, khususnya yang memiliki minat dalam bidang keamanan informasi dan manajemen risiko. Dengan memahami praktik terbaik dan tantangan yang dihadapi oleh perusahaan seperti PT. Indofood, mahasiswa dapat mengembangkan pengetahuan dan pemahaman yang lebih mendalam dalam mempersiapkan diri untuk menghadapi kebutuhan dan tuntutan sektor bisnis yang terus berkembang dalam era digital ini.

HASIL DAN PEMBAHASAN

PT. Indofood adalah salah satu perusahaan makanan dan minuman terbesar di Indonesia. Dalam operasinya, PT. Indofood perlu menjaga keamanan informasi dan data yang dimilikinya. Beberapa peran penting dalam menjaga keamanan informasi di PT. Indofood meliputi:

Implementasi Objek Vital pada PT. Indofood:

Dalam Keputusan Presiden Nomor 63 Tahun 2004 disebutkan bahwa obyek vital nasional adalah kawasan/lokasi/bangunan/instalasi dan/atau usaha yang menyangkut hajat hidup orang banyak, kepentingan negara, dan/atau sumber pendapatan negara yang bersifat strategis. Mengingat peranannya yang cukup strategis, obyek vital nasional membutuhkan sistem pengamanan yang lebih kuat dan didasarkan atas standar sistem pengamanan yang ketat, sehingga mampu memperkecil risiko dan dampak keamanan yang ditimbulkan akibat adanya ancaman dan gangguan keamanan (Namudat et al., 2019).

PT. Indofood merupakan perusahaan besar yang beroperasi di berbagai sektor industri makanan dan minuman. Objek vital merujuk pada aset atau komponen penting dalam infrastruktur teknologi informasi PT. Indofood. Ini dapat mencakup server pusat, sistem jaringan, atau basis data yang menyimpan data kritis perusahaan. Pengamanan objek vital ini menjadi prioritas utama untuk memastikan ketersediaan, integritas, dan kerahasiaan data yang disimpan di dalamnya.

Untuk melindungi sistem objek vital, seperti infrastruktur jaringan, sistem IT, dan data penting, perusahaan mungkin mengadopsi langkah-langkah keamanan yang meliputi:

1. Evaluasi risiko: Perusahaan akan melakukan evaluasi risiko terhadap sistem objek vital mereka. Ini melibatkan mengidentifikasi ancaman potensial, rentang kerusakan yang mungkin terjadi, dan kemungkinan terjadinya insiden keamanan. Dengan pemahaman yang baik tentang risiko, perusahaan dapat mengambil langkah-langkah yang sesuai untuk melindungi sistem objek vital.
2. Pengamanan fisik: Fasilitas fisik yang menyimpan sistem objek vital mungkin dilindungi dengan langkah-langkah keamanan fisik seperti sistem keamanan pintu, pengawasan CCTV, dan akses terbatas untuk memastikan bahwa hanya personel yang diizinkan yang dapat mengakses area tersebut.
3. Keamanan jaringan: PT. Indofood menerapkan langkah-langkah keamanan jaringan yang kuat untuk melindungi sistem objek vital dari ancaman siber. Ini termasuk penggunaan firewall, enkripsi data, pemantauan lalu lintas jaringan, dan penggunaan

keamanan jaringan terbaru untuk melindungi dari serangan malware dan upaya penyusupan.

4. Pengaturan akses: Perusahaan dapat menerapkan kebijakan pengaturan akses yang ketat untuk sistem objek vital. Hanya personel yang diotorisasi yang diberikan hak akses tertentu sesuai dengan tanggung jawab dan peran mereka. Ini membantu meminimalkan risiko akses yang tidak sah dan menjaga kerahasiaan dan integritas data.
5. Pemantauan dan pemulihan: PT. Indofood memiliki sistem pemantauan keamanan yang canggih untuk mendeteksi dan merespons insiden keamanan dengan cepat. Selain itu, perusahaan juga mungkin memiliki rencana pemulihan bencana yang terstruktur untuk memastikan bahwa sistem objek vital dapat dipulihkan dengan cepat setelah terjadinya insiden keamanan.
6. Pelatihan keamanan: Penting bagi PT. Indofood untuk melibatkan personel mereka dalam pelatihan keamanan yang berkala. Ini membantu meningkatkan kesadaran mereka tentang ancaman keamanan dan mengajarkan praktik terbaik untuk melindungi sistem objek vital.

Implementasi Pengamanan File pada PT. Indofood:

Pengamanan file adalah langkah-langkah yang diambil untuk melindungi integritas dan kerahasiaan file-file yang disimpan di sistem PT. Indofood. Ini dapat mencakup penerapan hak akses yang tepat, enkripsi data, dan penggunaan tanda tangan digital untuk memverifikasi keaslian file. Pengamanan file ini membantu mencegah akses yang tidak sah dan modifikasi yang tidak diizinkan terhadap informasi yang disimpan.

Implementasi pengamanan file pada PT. Indofood akan melibatkan serangkaian langkah-langkah keamanan untuk melindungi integritas, kerahasiaan, dan ketersediaan file yang dimiliki oleh perusahaan. Berikut ini beberapa praktik yang umumnya digunakan dalam pengamanan file:

1. Pengendalian Akses: PT. Indofood menerapkan sistem pengendalian akses yang ketat untuk memastikan bahwa hanya pengguna yang diotorisasi yang memiliki hak akses untuk mengakses file-file tertentu. Hal ini dapat mencakup pengaturan izin berbasis peran (role-based access control) di mana hak akses diberikan berdasarkan peran atau tanggung jawab pengguna dalam organisasi.
2. Enkripsi Data: PT. Indofood menggunakan teknik enkripsi untuk melindungi kerahasiaan file. Enkripsi akan mengubah file menjadi format yang tidak dapat dibaca tanpa kunci enkripsi yang sesuai. Hal ini membantu melindungi file dari akses yang tidak sah bahkan jika ada upaya untuk mencuri atau mengakses data secara langsung.

3. Backup dan Pemulihan: Perusahaan memiliki kebijakan backup rutin untuk file-file kritis. Ini melibatkan pencadangan (backup) secara teratur dari file-file yang penting dan menyimpannya di tempat yang aman. Jika terjadi kehilangan data atau serangan, file-file tersebut dapat dipulihkan dari cadangan (backup) yang tersedia.
4. Monitoring Aktivitas: PT. Indofood menggunakan alat pemantauan untuk memantau aktivitas file. Hal ini membantu mendeteksi dan melacak upaya akses yang tidak sah atau aktivitas yang mencurigakan terhadap file-file yang sensitif. Pemantauan ini memungkinkan tindakan cepat untuk mengatasi ancaman keamanan atau insiden yang terjadi.
5. Pengaturan Kebijakan Keamanan: Perusahaan mungkin memiliki kebijakan keamanan yang jelas terkait dengan penggunaan dan pengelolaan file. Kebijakan ini dapat mencakup ketentuan tentang penyimpanan file, berbagi file, penggunaan perangkat penyimpanan eksternal, dan tindakan keamanan lainnya yang harus diikuti oleh karyawan.
6. Pelatihan dan Kesadaran Keamanan: PT. Indofood mungkin memberikan pelatihan secara rutin kepada karyawan tentang pentingnya keamanan file dan praktik terbaik yang harus diikuti. Ini membantu meningkatkan kesadaran karyawan tentang risiko keamanan file dan mengajarkan mereka tindakan yang harus diambil untuk melindungi file dengan benar.

Implementasi pengamanan file dapat menjadi proses yang berkelanjutan, mengikuti perkembangan teknologi dan ancaman keamanan baru. Oleh karena itu, penting untuk terus memantau tren keamanan terkini dan memperbarui langkah-langkah keamanan sesuai kebutuhan untuk melindungi file-file perusahaan.

Implementasi Pengamanan Cyber pada PT. Indofood:

Keamanan merupakan salah satu aspek yang sangat penting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Masalah keamanan sering berada diurutan setelah tampilan, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting (Risawandi et al., 2021). Pengamanan cyber melibatkan langkah-langkah untuk melindungi sistem komputer, jaringan, dan infrastruktur teknologi informasi PT. Indofooddari ancaman cyber. Ini mencakup perlindungan terhadap serangan malware, peretasan, phishing, atau serangan siber lainnya. PT. Indofood mungkin menggunakan perangkat lunak keamanan, firewall, sistem deteksi intrusi, dan praktik keamanan jaringan lainnya untuk mengurangi risiko serangan cyber.

Implementasi pengamanan cyber pada PT. Indofood melibatkan serangkaian langkah-langkah untuk melindungi sistem komputer, jaringan, dan data perusahaan dari ancaman siber. Berikut adalah beberapa praktik yang digunakan dalam pengamanan cyber:

1. Firewalls dan Sistem Proteksi Jaringan: PT. Indofoodmungkin menggunakan perangkat keras dan perangkat lunak firewall untuk mengawasi lalu lintas jaringan dan mencegah akses yang tidak sah. Selain itu, sistem proteksi jaringan lainnya seperti Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS) juga dapat diterapkan untuk mendeteksi dan merespons serangan siber yang berpotensi.
2. Pembaruan Perangkat Lunak: Perusahaan akan memastikan bahwa sistem operasi, perangkat lunak, dan aplikasi yang digunakan diupdate secara teratur dengan pembaruan keamanan terbaru. Ini membantu menutup celah keamanan yang diketahui dan mengurangi risiko eksploitasi.
3. Keamanan Email: PT. Indofood menggunakan solusi keamanan email seperti filter spam dan skrining malware untuk mengidentifikasi dan memblokir email berbahaya atau mencurigakan. Selain itu, pelatihan kesadaran keamanan email dapat diberikan kepada karyawan untuk mengenali dan menghindari serangan phishing atau email palsu.
4. Manajemen Identitas dan Akses: Perusahaan mungkin menerapkan solusi manajemen identitas dan akses (Identity and Access Management - IAM) untuk mengelola hak akses pengguna, menerapkan otentikasi yang kuat, dan memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem dan data.
5. Enkripsi Data: PT. Indofood menerapkan enkripsi data untuk melindungi kerahasiaan dan integritas data yang sensitif. Enkripsi dapat diterapkan pada data saat transit dan saat istirahat untuk memastikan bahwa hanya pihak yang berwenang yang dapat membaca atau memanipulasi data tersebut.
6. Pemantauan Keamanan dan Respons Kejadian Insiden: Perusahaan dapat menggunakan alat pemantauan keamanan untuk mendeteksi aktivitas mencurigakan atau serangan siber yang sedang berlangsung. Tim respons kejadian insiden (incident response team) dapat ditugaskan untuk merespons dan menangani serangan dengan cepat untuk meminimalkan dampaknya.
7. Pelatihan Kesadaran Keamanan: PT. Indofood memberikan pelatihan kesadaran keamanan cyber secara rutin kepada karyawan. Ini meliputi pengajaran tentang ancaman siber, praktik keamanan yang baik, dan tindakan yang harus diambil jika

terjadi insiden keamanan. Kesadaran karyawan yang tinggi dapat membantu mencegah serangan dan meningkatkan keamanan secara keseluruhan.

8. Pengujian Keamanan (Security Testing): Perusahaan mungkin melakukan pengujian keamanan seperti penetrasi (penetration testing) dan pemindaian kerentanan (vulnerability scanning) secara berkala untuk mengidentifikasi dan memperbaiki kerentanan dalam sistem dan jaringan mereka sebelum penyerang melakukannya.

KESIMPULAN

Berdasarkan analisis terhadap keamanan informasi PT. Indofood, dapat disimpulkan bahwa perusahaan tersebut memiliki pendekatan yang komprehensif dalam melindungi objek vital, mengamankan file, dan menerapkan langkah-langkah keamanan cyber. PT. Indofood telah mengambil langkah-langkah proaktif untuk menjaga keutuhan, kerahasiaan, dan ketersediaan sistem dan data perusahaan.

Dalam hal objek vital, PT. Indofood telah melakukan evaluasi risiko dan mengidentifikasi sistem dan infrastruktur kritis yang perlu dijaga dengan ketat. Langkah-langkah seperti pengendalian akses, pengamanan fisik, dan pelatihan keamanan mungkin telah diimplementasikan untuk melindungi objek vital tersebut.

Pada pengamanan file, perusahaan mungkin telah mengadopsi kebijakan pengaturan akses yang ketat, menggunakan enkripsi data untuk melindungi kerahasiaan, serta melaksanakan backup rutin dan pemulihan data. PT. Indofoodmungkin juga memonitor aktivitas file secara terus-menerus dan memiliki kebijakan keamanan yang jelas terkait dengan penggunaan dan pengelolaan file.

Dalam pengamanan cyber, PT. Indofoodmungkin telah menggunakan firewall, sistem proteksi jaringan, dan pembaruan perangkat lunak yang teratur untuk melindungi sistem dan jaringan perusahaan dari ancaman siber. Penggunaan solusi keamanan email, manajemen identitas dan akses, serta enkripsi data juga mencerminkan komitmen perusahaan terhadap keamanan cyber. Pelatihan kesadaran keamanan dan pengujian keamanan yang dilakukan secara berkala dapat membantu meningkatkan kesiapan dan respons terhadap serangan.

Secara keseluruhan, PT. Indofood telah menunjukkan kesadaran yang baik terhadap keamanan informasi dan melaksanakan langkah-langkah penting untuk melindungi objek vital, mengamankan file, dan menghadapi ancaman siber.

REFERENSI

Firman. (2015). Analisis Data Dalam Kualitatif. *Article*, *4*, 1–13.

Namudat, H., Karlina, N., & Rusli, B. (2019). Analisis Kebijakan Pengamanan Objek Vital Di Pt Freeport Indonesia. *Responsive*, *1*(2), 39. https://doi.org/10.24198/responsive.v1i2.20673

Risawandi, R., Rozzy, R., & Irsan, M. (2021). Pengamanan Data Menggunakan Teknik Quick Response Code Pada Aplikasi Manajemen Informasi Ikatif Unimal Berbasis Android. *Jurnal Tika*, *6*(03), 224–230. https://doi.org/10.51179/tika.v6i03.752