Cross-border
Vol. 6 No. 1 Januari-Juni 2023, page 691-697

p-ISSN: 2615-3165
e-ISSN: 2776-2815

SISTEM *CYBER SECURITY* DAN PENGAMANAN FILE PADA PENGAMANAN OBJEK VITAL PT TELKOM INDONESIA (PERSERO) Tbk

Edy Soesanto*
Program Studi Teknik Perminyakan,Universitas Bhayangkara Jakarta Raya, Indonesia
edy.soesanto@dsn.ubharajaya.ac.id

Donni Ferdinan Irawan
Program Studi Manajemen,Universitas Bhayangkara Jakarta Raya, Indonesia
202010325169@mhs.ubharajaya.ac.id

Damar Asmarani
Program Studi Manajemen,Universitas Bhayangkara Jakarta Raya, Indonesia
202010325208@mhs.ubharajaya.ac.id

Putri Octavia Maharani
Program Studi Manajemen,Universitas Bhayangkara Jakarta Raya, Indonesia
202010325202@mhs.ubharajaya.ac.id

ABSTRACT

This study discusses the cyber security system and file security in securing vital objects of PT Telkom Indonesia (Persero) Tbk. In the context of a critical telecommunications company, maintaining the security and confidentiality of vital objects and information stored in files is critical. This study identifies security measures that are generally implemented by PT Telkom Indonesia (Persero) Tbk in protecting vital objects and files containing important information. These measures include the use of firewalls, intrusion detection, protection against DoS attacks, data encryption, user identification and authentication, and continuous security monitoring. In addition, this research also provides suggestions for improving the cyber security system and file security of PT Telkom Indonesia (Persero) Tbk. These suggestions include increasing security awareness, regular security audits, collaboration with external parties, enhanced security monitoring, and research and innovation in cybersecurity. By implementing these steps and suggestions, PT Telkom Indonesia (Persero) Tbk can improve cyber security and file security on their vital objects, so as to protect information that is very important for the company and their customers.

Keywords: *Cyber Security, File Security, and Vital Object Security.*

ABSTRAK

Penelitian ini membahas tentang sistem keamanan cyber dan pengamanan file pada pengamanan objek vital PT Telkom Indonesia (Persero) Tbk. Dalam konteks perusahaan telekomunikasi yang penting, menjaga keamanan dan kerahasiaan objek vital serta informasi yang disimpan dalam file sangat penting. Penelitian ini mengidentifikasi langkah-langkah keamanan yang umumnya diterapkan oleh PT Telkom Indonesia (Persero) Tbk dalam melindungi objek vital dan file-file yang berisi informasi penting. Langkah-langkah ini meliputi penggunaan firewall, deteksi intrusi, perlindungan terhadap serangan DoS, enkripsi data, identifikasi dan otentikasi pengguna, serta pemantauan keamanan yang terus-menerus. Selain itu,

penelitian ini juga memberikan saran-saran untuk meningkatkan sistem keamanan siber dan pengamanan file PT Telkom Indonesia (Persero) Tbk. Saran-saran tersebut meliputi peningkatan kesadaran keamanan, audit keamanan teratur, kolaborasi dengan pihak eksternal, pemantauan keamanan yang ditingkatkan, dan riset serta inovasi dalam bidang keamanan siber. Dengan menerapkan langkah-langkah dan saran-saran ini, PT Telkom Indonesia (Persero) Tbk dapat meningkatkan keamanan siber dan pengamanan file pada objek vital mereka, sehingga dapat melindungi informasi yang sangat penting bagi perusahaan dan pelanggan mereka.
Kata Kunci: Pengamanan Siber, Pengamanan File, dan Pengamanan Obyek Vital.

PENDAHULUAN

Cyber security adalah salah satu aspek penting dalam sistem pengamanan obyek vital nasional, karena berkaitan dengan perlindungan data, informasi, dan jaringan komunikasi dari serangan cyber yang dapat merusak, mengubah, menghapus, atau mencuri data dan informasi penting Menurut (Ardiyanti, 2014)

Pengamanan File merupakan salah satu faktor penting yang harus diperhatikan dalam komunikasi terutama dengan kemajuan dan perkembangan teknologi pada masa kini menurut (Solehudin, 2019). Pesatnya perkembangan teknologi memberikan banyak dampak positif bagi masyarakat seperti kemudahan memperoleh informasi, pertukaran data dan pesan penyebaran informasi, pengiriman pesan, dan sebagainya.

Sistem pengamanan objek vital adalah sistem yang bertujuan untuk melindungi objek vital dari ancaman, gangguan, dan sabotase yang dapat mengganggu kepentingan nasional. pengamanan obyek vital nasional tersebut ditujukan untuk meminimalisir dan bahkan mencegah dampak gangguan dan ancaman terhadap objek vital nasional yang dapat mengakibatkan terjadinya bencana kemanusiaan, terganggunya pemerintahan, terancamnya keamanan dan pertahanan negara serta yang paling dihindari adalah rusaknya hasil pembangunan nasional menurut (Namudat et al., 2019).

PT Telkom Indonesia (Persero) Tbk atau Telkom adalah salah satu Badan Usaha Milik Negara (BUMN) yang bergerak di bidang telekomunikasi dan digital. Telkom memiliki beberapa objek vital yang berkaitan dengan infrastruktur telekomunikasi dan digital, seperti gedung pusat, stasiun bumi satelit, tower BTS, kabel bawah laut, data center, dan lain-lain. Objek-objek vital tersebut harus dijaga dan dilindungi dengan baik agar dapat berfungsi secara optimal dan aman.

Telkom sebagai BUMN wajib menerapkan nilai-nilai utama yang didefinisikan sebagai nilai-nilai Amanah, Kompeten, Harmonis, Loyal, Adaptif, dan Kolaboratif yang mendasari perilaku insan BUMN. Nilai-nilai ini diimplementasikan tidak hanya dalam lingkungan pekerjaan, melainkan justru dimulai dari diri sendiri dan keluarga. Nilai-nilai ini diharapkan dapat meningkatkan kinerja dan reputasi Telkom sebagai BUMN yang unggul dan berkontribusi bagi akselerasi digital Indonesia.

Namun, dalam pelaksanaannya, Sistem Pengamanan Objek Vital PT Telkom masih menghadapi berbagai kendala dan tantangan. Beberapa kendala dan tantangan tersebut antara lain adalah kurangnya sumber daya manusia yang profesional dan terlatih dalam bidang pengamanan, kurangnya peralatan dan teknologi yang canggih dan terintegrasi

dalam sistem pengamanan, kurangnya koordinasi dan komunikasi antara pihak-pihak terkait dalam sistem pengamanan, serta kurangnya kesadaran dan tanggung jawab dari seluruh insan Telkom dalam menjaga dan melindungi objek vital perusahaan.

Oleh karena itu, penulis tertarik untuk melakukan penelitian tentang Sistem Pengamanan Objek Vital, Cyber Security dan Pengamanan File PT Telkom Indonesia (persero) Tbk. Penelitian ini bertujuan untuk mengetahui bagaimana Sistem *Cyber Security* dan Pengamanan File Pada Pengamanan Objek Vital PT Telkom Indonesia (persero) Tbk, serta faktor-faktor apa saja yang mempengaruhi peran tersebut. Penelitian ini diharapkan dapat memberikan informasi dan masukan bagi pihak-pihak terkait dalam meningkatkan kualitas sistem pengamanan objek vital cyber security dan pengamanan file Telkom.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif. Penelitian kualitatif adalah suatu proses penelitian untuk memahami fenomena-fenomena manusia atau sosial dengan menciptakan gambaran yang menyeluruh dan kompleks yang dapat disajikan dengan kata-kata, melaporkan pandangan terinci yang diperoleh dari sumber informan, serta dilakukan dalam latar setting yang alamiah (Walidin, Saifullah & Tabrani, 2015: 77).

Penelitian kualitatif lebih berfokus kepada proses daripada hasil penelitian, membatasi masalah penelitian, berdasarkan fokus, menggunakan kriteria tersendiri untuk memvaliditas data, menggunakan desain sementara. Hasil penelitian dirundingkan dan disepakati oleh manusia dan dijadikan sebagai sumber data.

HASIL DAN PEMBAHASAN

Gambaran tentang PT Telkom Indonesia (persero) Tbk

Perusahaan Telekomunikasi sudah ada sejak masa Hindia Belanda dan yang menyelenggarakan adalah pihak swasta.Sedangkan perusahaan Telekomunikasi Indonesia (PT. TELKOM) sendiri juga termasuk bagian dari perusaahaan tersebut yang mempunyai bentuk badan usaha *Post-en Telegraaflent* dengan *Staats blaad* No.52 tahun 1884.Dan sejak tahun 1905 perusahaan Telekomunikasi sudah berjumlah 38 peusahaan.Namun setelah itu pemerintah Hindia Belanda mengambil alih perusahaan tersebut yang berdasar kepada *Staatsblaad* tahun 1906. Dan sejak itu berdirilah *Post, Telegraf en Telefoon Dients* (PTT-Dients),dan perusahaan ini ditetapkan sebagai Perusahaan Negara berdasar Staats blaad No.419 tahun 1927 tentang Indonesia *Bedrijven Weet* (I.B.W Undang-Undang Perusahaan Negara).

PT. Telekomunikasi Selular adalah nama merek dari operator GSM dan jaringan telepon UMTS Mobile yang beroperasi di Indonesia. Perusahaan ini didirikan pada tahun 1995, dan merupakan anak perusahaan dari Telkom Indonesia. Saat ini perusahaan memiliki 160 juta pelanggan. PT. Telekomunikasi Selular Beroperasi di Indonesia dengan GSM 900-1800 MHz, jaringan 3G dan 4G, dan internasional melalui 323 mitra roaming internasional di 170 negara (akhir September 2008). Perusahaan ini menyediakan pelanggan dengan pilihan antara tiga kartu prabayar simPATI, Loop dan Kartu As, atau layanan pasca bayar kartuHALO, serta berbagai layanan dan program.

Gambaran tentang Objek Vital PT Telkom Indonesia (persero) Tbk

Pada gambaran objek vital PT Telkom setelah tanggal pemotongan pengetahuan saya pada September 2021. Sebagai gantinya, saya dapat memberikan gambaran umum tentang objek vital yang umumnya terkait dengan operator telekomunikasi seperti PT Telkom.

Objek vital (critical infrastructure) merujuk pada aset, sistem, atau layanan yang sangat penting bagi kelangsungan hidup, keamanan, dan stabilitas suatu negara atau organisasi. Bagi operator telekomunikasi seperti PT Telkom, objek vital mungkin meliputi:

1. Jaringan Komunikasi: Jaringan telekomunikasi fisik dan nirkabel yang mencakup infrastruktur kabel serat optik, infrastruktur jaringan seluler, dan peralatan komunikasi yang digunakan untuk menghubungkan pengguna akhir dan memberikan layanan komunikasi suara dan data.
2. Pusat Data: Pusat data atau data center yang digunakan untuk menyimpan, mengelola, dan memproses data penting, termasuk data pelanggan, data jaringan, dan sistem pendukung operasional. Pusat data sering menjadi objek vital karena keberlanjutan operasional dan keamanan data yang disimpan di dalamnya.
3. Sistem Manajemen Jaringan: Sistem yang digunakan untuk mengelola dan memantau jaringan telekomunikasi, termasuk sistem pemantauan kinerja jaringan, manajemen kapasitas, manajemen keamanan, dan sistem manajemen perangkat keras dan perangkat lunak.
4. Peralatan Jaringan Utama: Perangkat keras dan perangkat lunak yang digunakan untuk mengoperasikan dan mengendalikan jaringan telekomunikasi, seperti perute, switch, server, dan perangkat jaringan lainnya. Keberlanjutan operasional peralatan jaringan ini sangat penting untuk menjaga konektivitas yang stabil.
5. Layanan Komunikasi Darurat: Layanan komunikasi yang khusus disediakan untuk keperluan darurat, seperti sistem telepon darurat, layanan panggilan darurat, atau jaringan khusus yang diaktifkan dalam situasi krisis atau bencana.

Pemahaman lebih lanjut mengenai objek vital PT Telkom dapat diperoleh melalui sumber informasi yang terkait, seperti dokumen kebijakan atau laporan keberlanjutan yang diterbitkan oleh perusahaan.

Gambaran tentang Pengamanan File PT Telkom Indonesia (persero) Tbk

Pengamanan file melibatkan serangkaian langkah untuk melindungi informasi yang terdapat dalam file dari akses yang tidak sah atau perubahan yang tidak diizinkan. Beberapa langkah pengamanan file yang umum dilakukan meliputi:

1. Penggunaan kata sandi: Melindungi file dengan mengatur kata sandi yang kuat dan rahasia. Kata sandi harus terdiri dari kombinasi huruf (baik huruf besar maupun huruf kecil), angka, dan karakter khusus. Selain itu, penting juga untuk menghindari penggunaan kata sandi yang mudah ditebak.

2. Enkripsi file: Menggunakan algoritma enkripsi untuk mengubah isi file menjadi format yang tidak dapat dibaca oleh pihak yang tidak berwenang. Enkripsi dapat dilakukan pada level file atau pada level seluruh sistem penyimpanan.
3. Otorisasi akses: Mengatur hak akses untuk file, sehingga hanya pengguna yang diizinkan yang dapat membuka, mengedit, atau menghapus file tersebut. Ini dapat dilakukan melalui pengaturan izin pada sistem operasi atau perangkat lunak pengelolaan file.
4. Backup file: Melakukan backup (pencadangan) file secara teratur merupakan tindakan pengamanan yang penting. Dengan memiliki salinan cadangan file, informasi yang terdapat di dalamnya dapat dipulihkan jika terjadi kehilangan atau kerusakan.
5. Perangkat lunak keamanan: Menggunakan perangkat lunak keamanan seperti firewall, antivirus, dan antispyware dapat membantu melindungi file dari serangan malware atau upaya akses yang tidak sah.

Pengamanan file merupakan upaya yang penting untuk menjaga kerahasiaan dan integritas informasi yang disimpan dalam file. Melalui langkah-langkah pengamanan yang tepat, risiko kebocoran data atau manipulasi file oleh pihak yang tidak berwenang dapat dikurangi.

Penggunaan kata sandi yang kuat dan enkripsi file membantu melindungi isi file dari akses yang tidak sah. Hanya pengguna yang memiliki kata sandi yang benar atau kunci dekripsi yang tepat yang dapat membuka atau membaca isi file. Otorisasi akses memastikan bahwa hanya pengguna yang memiliki izin yang sesuai yang dapat mengakses, mengedit, atau menghapus file tersebut.

Backup file secara teratur merupakan langkah penting dalam pengamanan file. Dengan memiliki salinan cadangan, risiko kehilangan data karena kegagalan perangkat keras, serangan malware, atau kesalahan pengguna dapat diminimalkan. Backup file juga memungkinkan pemulihan data jika terjadi insiden keamanan.

Penggunaan perangkat lunak keamanan seperti firewall, antivirus, dan antispyware membantu mendeteksi dan mencegah serangan malware serta melindungi file dari ancaman jaringan.

Gambaran tentang Pengamanan *Cyber* PT Telkom Indonesia (persero) Tbk

Berikut ini adalah gambaran umum tentang pengamanan siber yang biasanya diterapkan oleh perusahaan seperti PT Telkom Indonesia (Persero) Tbk:

1. Keamanan Jaringan: PT Telkom Indonesia (Persero) Tbk melaksanakan langkah-langkah keamanan jaringan yang kuat untuk melindungi infrastruktur jaringan dan sistem komunikasi mereka. Ini meliputi penggunaan firewall, deteksi intrusi, dan perlindungan terhadap serangan Denial of Service (DoS) yang bertujuan untuk mencegah akses yang tidak sah atau upaya merusak jaringan.
2. Enkripsi Data: PT Telkom Indonesia (Persero) Tbk menerapkan enkripsi data untuk melindungi keamanan informasi yang sensitif. Enkripsi dapat digunakan dalam komunikasi dan penyimpanan data untuk mencegah akses oleh pihak yang tidak berwenang. Identifikasi dan Otentikasi Pengguna: PT Telkom Indonesia (Persero)

Tbk menggunakan mekanisme identifikasi dan otentikasi pengguna yang kuat untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses ke sistem dan data penting. Ini mungkin meliputi penggunaan kata sandi yang kompleks, autentikasi dua faktor, atau teknologi biometrik.

3. Pemantauan Keamanan: PT Telkom Indonesia (Persero) Tbk memiliki sistem pemantauan keamanan yang terus-menerus untuk mendeteksi dan menanggapi ancaman siber yang mungkin timbul. Ini termasuk pemantauan lalu lintas jaringan, pemantauan log kejadian, dan analisis keamanan untuk mendeteksi aktivitas mencurigakan atau serangan potensial.
4. Pelatihan dan Kesadaran Keamanan: PT Telkom Indonesia (Persero) Tbk menyadari pentingnya melibatkan karyawan dan pengguna dalam keamanan siber. Mereka memberikan pelatihan dan kesadaran keamanan yang rutin kepada karyawan untuk membantu mereka mengenali ancaman siber dan mengambil langkah-langkah yang tepat dalam menjaga keamanan informasi.

Harap dicatat bahwa informasi ini bersifat umum dan mungkin berbeda di PT Telkom Indonesia (Persero) Tbk secara spesifik. Untuk mendapatkan informasi terkini dan lebih rinci mengenai gambaran pengamanan cyber PT Telkom Indonesia (Persero) Tbk, disarankan untuk merujuk ke sumber informasi resmi mereka seperti laporan keberlanjutan, kebijakan keamanan, atau pernyataan publik mereka terkait dengan keamanan siber.

KESIMPULAN

Berdasarkan gambaran umum yang diberikan, dapat disimpulkan bahwa PT Telkom Indonesia (Persero) Tbk memiliki perhatian yang serius terhadap keamanan siber dan pengamanan file. Sebagai operator telekomunikasi terkemuka, mereka menyadari pentingnya melindungi objek vital dan informasi yang disimpan dalam file dari ancaman cyber yang mungkin timbul.

PT Telkom Indonesia (Persero) Tbk menerapkan langkah-langkah keamanan jaringan, termasuk penggunaan firewall, deteksi intrusi, dan perlindungan terhadap serangan DoS, untuk mencegah akses yang tidak sah atau upaya merusak jaringan. Mereka juga menggunakan enkripsi data untuk melindungi informasi yang sensitif, serta menerapkan identifikasi dan otentikasi pengguna yang kuat untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses ke sistem dan data penting. Selain itu, PT Telkom Indonesia (Persero) Tbk memiliki sistem pemantauan keamanan yang terus-menerus untuk mendeteksi dan menanggapi ancaman siber, serta memberikan pelatihan dan kesadaran keamanan kepada karyawan.

DAFTAR PUSTAKA

Suheri, A. (2018). KEAMANAN FILE DENGAN TEKNIK ZIGZAG DAN HUFFMAN. *Media Jurnal Informatika*, *9*(2).

Baba, M. A. (2017). *ANALISIS DATA KUALITATIF.* Makassar: tAksara Timur.

Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 5(1).

Fadli, M. R. (2021). Memahami desain metode penelitian kualitatif. Humanika, Kajian Ilmiah Mata Kuliah Umum, 21(1), 33-54.

Namudat, H., Karlina, N., & Rusli, B. (2018). ANALISIS KEBIJAKAN PENGAMANAN OBJEK VITAL DI PT FREEPORT INDONESIA. Responsive: Jurnal Pemikiran Dan Penelitian Administrasi, Sosial, Humaniora Dan Kebijakan Publik, 1(2), 39-44.

PT Nusa Halmahera Minerals. . (2022). *KEBIJAKAN PRIVASI*. Retrieved Mei Minggu, 2023, from https://www.nhm.co.id/ina/kebijakan-privasi/

Purnomo, H. (2017). Penilaian Tingkat Kapabilitas Proses Tata Kelola Teknologi Informasi Dengan Cobit 5 Pada Domain Edm (Studi Kasus Di Pt. Nusa Halmahera Minerals) . *(Doctoral dissertation, Universitas Gadjah Mada).*

Saputra, A. D. (n.d.). Analisis kinerja kipas utama pada tambang bawah tnah toguraci di PT Nusa Halmahera Minerals, Maluku Utara.

Suriadi S., S. R. (2019). Peran Direktorat Pengamanan Obyek Vital Kepolisian Daerah Maluku Utara dalam Pengamanan Kawasan Pertambangan. *Khairun Law*, 33-34.

Suryana, A. (2007). Tahap-tahap Penelitian Kualitatif Mata Kuliah Analisis Data Kualitatif. Bandung: Universitas Pendidikan Indonesia.

Tipton, Harold F. dan Krause, Micki, 2007, Information Security Management Handbook, Sixth Edition. Auerbach Publications

Wati, L. (2013). ANALISIS KEBIJAKAN PEMERINTAH KOTA PEKANBARU UNTUK PENGEMBANGAN DAN PENATAAN PASAR TRADISIONAL (STUDY KASUS PADA PASAR PAGI ARENGKA PEKANBARU) (Doctoral dissertation, Universitas Islam Negeri Sultan Syarif Kasim Riau).