PENERAPAN KEAMANAN OBJEK VITAL, DATA, DAN SIBER PADA PT KRAKATAU STEEL

Edy Soesanto[1], Kefas Kristian Telaumbanua[2], Muhammad Dzaky[3], Fransisca Nada Sherenika[4]

[1]Program Studi Teknik Perminyakan, Universitas Bhayangkara Jakarta Raya
e-mail: [1]*edy.soesanto@dsn.ubharajaya.ac.id*

[2,3,4]Ekonomi & Bisnis/Manajemen, Universitas Bhayangkara Jakarta Raya
e-mail: [2]*202010325205@mhs.ubharajaya.ac.id*, [3]*202010325162@mhs.ubharajaya.ac.id*,
[4]*fransisca.nada.sherenika18@mhs.ubharajaya.ac.id*

Abstract

Security is an important aspect in maintaining operational continuity and protecting company assets. PT Krakatau Steel as a company with vital objects and sensitive data, needs to implement strong security policies and practices. This study aims to analyze the application of vital object security, data security, and cybersecurity at PT Krakatau Steel. The research method used includes a literature review study, by describing the safeguards in PT Krakatau Steel.

Keywords: Vital Object Security, Data Security, Cyber Security, PT Krakatau Steel

Abstrak

Keamanan menjadi aspek penting dalam menjaga kelangsungan operasional dan melindungi aset perusahaan. PT Krakatau Steel sebagai perusahaan dengan objek vital dan data yang sensitif, perlu menerapkan kebijakan dan praktik keamanan yang kuat. Penelitian ini bertujuan untuk menganalisis penerapan keamanan objek vital, keamanan data, dan keamanan siber di PT Krakatau Steel. Metode penelitian yang digunakan meliputi studi literatur review, dengan mendeskripsikan pengamanan di dalam PT Krakatau Steel.

Keywords: Keamanan Objek Vital, Keamanan Data, Keamanan Siber, PT Krakatau Steel

1. PENDAHULUAN

Keputusan Presiden No. 63 Tahun 2004 tentang Pengamanan Obyek Vital Nasional, bersama dengan Undang-Undang Kepolisian Negara Republik Indonesia No. 2 Tahun 2002, mengarahkan Kepolisian Negara Republik Indonesia untuk menyusun pedoman Sistem Keamanan Nasional Obyek Vital untuk memberikan perlindungan, pengayoman, dan Layanan masyarakat [1].

Hal itu dipertegas dengan surat keputusan Kombes Pol Nomor: Skep 783/X/2005 yang menyatakan bahwa tempat-tempat yang menentukan adalah kawasan, tempat, bangunan, lembaga, dan bisnis yang strategis karena gangguan terhadap situs-situs penentu nasional tersebut sangat mempengaruhi kebutuhan manusia dan kepentingan nasional [2].

Regulasi Ketahanan Pangan Nasional bertujuan untuk meminimalkan bahkan mencegah dampak gangguan dan ancaman terhadap objek esensial nasional, yang dapat mengakibatkan bencana kemanusiaan, gangguan administrasi dan ancaman terhadap keamanan dan pertahanan negara, dan yang terpenting mencegah kerusakan. hasil pembangunan nasional [3].

Keamanan data sangat penting dalam perangkat, agar informasi yang diperlukan tidak dicuri atau dihapus oleh orang yang tidak bertanggung jawab. Sederhananya, keamanan informasi adalah langkah yang harus diambil oleh perusahaan atau individu untuk melindungi ekosistem teknologi informasi [4]. Dengan tingkat keamanan ini, bisnis atau individu tidak perlu lagi khawatir dengan pelanggaran keamanan [5].

Keamanan data adalah proses yang didukung peraturan dan teknologi untuk melindungi data dari kerusakan data, pengubahan data, dan penyebaran data yang disengaja atau tidak disengaja. Keamanan data harus mencakup tiga elemen penting termasuk kerahasiaan,

integritas dan ketersediaan. Ketiga elemen ini disebut sebagai triad CIA [6].

Keamanan siber adalah perlindungan sistem, jaringan, dan program terhadap serangan digital. Tujuan serangan ini biasanya untuk mengakses, mengubah, atau menghancurkan data sensitif. Menagih uang kepada pengguna atau mengganggu proses bisnis normal.

Perusahaan di berbagai industri seperti energi, transportasi, ritel, dan manufaktur menggunakan sistem digital dan koneksi berkecepatan tinggi untuk layanan pelanggan yang efisien dan bisnis yang hemat biaya. Sama seperti bisnis yang melindungi aset fisiknya, bisnis juga harus melindungi aset digitalnya dan melindungi sistemnya dari akses yang tidak diinginkan. Serangan keamanan dikenal sebagai serangan keamanan atau serangan keamanan. Serangan siber yang berhasil mengakibatkan pengungkapan, pencurian, penghapusan, atau pengubahan informasi rahasia [7]. Langkah-langkah keamanan siber melindungi dari serangan siber dan menawarkan banyak manfaat.

PT Krakatau Steel merupakan pemain utama dalam industri baja di Asia Tenggara. Perusahaan ini pertama kali didirikan pada tahun 1970. Perusahaan ini sebelumnya dikenal dengan nama Proyek Besi dan Baja Tricore. PT. Krakatau Steel merupakan industri baja pertama di Indonesia. pt. Krakatau Steel didirikan pada tahun 1970. Berdasarkan Surat Keputusan Pemerintah RI No. 35 Tahun 1970. Menurut Pasal 1 Peraturan Pemerintah, PT. Krakatau Steel didirikan dengan tujuan untuk menyelesaikan dan melaksanakan proyek industri limbah dengan bantuan Rusia dan mengembangkan industri baja Indonesia [8]**.**

Krakatau Steel merupakan salah satu basis industri utama nasional yang diatur melalui Keputusan Menteri Perindustrian Nomor 1. 466/m-fin/kep/8/2014. Setelah bernama Obvitnas, Krakatau Steel menjadi prihatin dengan apa yang harus dilakukan perusahaan untuk menjadi Obvitnas. Salah satunya implementasi dan sertifikasi sistem manajemen keamanan berdasarkan Perpol 7 tahun 2019. Terkait keamanan informasi dan siber, Krakatau Steel secara rutin melakukan pemeriksaan dan pengembangan lebih lanjut sistem keamanan informasi.

2. METODE

Penelitian ini menggunakan metode deskriptif dengan pendekatan kualitatif berupa literature review PT. Krakatau Steel. Dengan metode ini diharapkan dapat mengetahui penerapan benda-benda penting, data dan keamanan siber di PT Krakatau Steel [9].

3. PEMBAHASAN

Profil Perusahaan PT Krakatau Steel

PT Krakatau Steel didirikan pada tahun 1970 dan mulai beroperasi secara komersial pada tahun 1978. Perusahaan ini berlokasi di Cilegon, Banten, Indonesia. Krakatau Steel awalnya didirikan sebagai bagian dari proyek strategis pemerintah untuk mengembangkan industri baja di Indonesia [9].

PT Krakatau Steel bergerak dalam produksi baja terpadu dan produk turunannya. Perusahaan ini terlibat dalam berbagai tahap produksi baja, mulai dari pengolahan bijih besi, peleburan, pemurnian, pembentukan, hingga pengolahan produk baja seperti plat, batang, dan kawat.

Krakatau Steel memproduksi berbagai jenis produk baja, termasuk pelat baja, gulungan baja, batang baja, kawat baja, pipa baja, dan produk baja lainnya. Produk-produk ini digunakan dalam berbagai sektor industri, seperti konstruksi, otomotif, perkapalan, dan manufaktur.

Perusahaan memiliki kapasitas produksi yang besar. Krakatau Steel mampu memproduksi lebih dari 2 juta ton baja setiap tahunnya. Pabrik baja Krakatau Steel dilengkapi dengan fasilitas dan teknologi modern untuk memastikan kualitas produk yang tinggi.

PT Krakatau Steel berkomitmen untuk menjalankan operasinya secara berkelanjutan dan memperhatikan dampak lingkungan. Perusahaan ini telah mengimplementasikan berbagai program dan inisiatif lingkungan, termasuk pengelolaan limbah, penghematan energi, dan upaya pengurangan emisi gas rumah kaca. Krakatau Steel telah memperoleh berbagai sertifikasi dan pengakuan, seperti ISO 9001 untuk sistem manajemen mutu, ISO 14001 untuk sistem manajemen lingkungan, dan OHSAS 18001 untuk sistem manajemen keselamatan dan kesehatan kerja. Perusahaan juga meraih berbagai penghargaan dalam bidang kinerja, kualitas, dan kontribusi terhadap industri baja nasional.

PT Krakatau Steel memasok produk baja baik untuk pasar domestik di Indonesia maupun untuk ekspor ke berbagai negara di dunia. Perusahaan ini berperan penting dalam memenuhi kebutuhan baja di dalam negeri serta meningkatkan pertumbuhan industri baja nasional.

Objek Vital

Objek vital adalah komponen atau item yang sangat penting dan kritis dalam suatu sistem atau organisasi. Istilah "item kritis" sering digunakan dalam konteks keamanan dan kontinuitas operasional. Objek vital merujuk pada infrastruktur, fasilitas, atau entitas yang dianggap penting dan vital bagi keberlanjutan dan keamanan suatu negara atau organisasi. Objek vital sering kali merupakan target potensial serangan atau sabotase karena kerusakan atau gangguan terhadap objek tersebut dapat memiliki dampak serius pada operasional, keamanan, atau stabilitas suatu entitas [10].

Perlindungan dan keamanan objek vital sering menjadi perhatian utama bagi pemerintah dan lembaga terkait untuk memastikan kelangsungan fungsi dan keamanan nasional atau organisasional. Upaya keamanan meliputi pengawasan, pengamanan fisik, pengendalian akses, sistem pengawasan, dan langkah-langkah lain yang bertujuan untuk mencegah ancaman, serangan, atau kerusakan terhadap objek vital tersebut [11].

Keamanan Objek Vital di PT Krakatau Steel

Sebagai sebuah pabrik baja terintegrasi, PT. Krakatau Steel memiliki berbagai objek vital yang berperan penting dalam proses produksi baja. Berikut beberapa objek vital yang umumnya ada di PT. Krakatau Steel [12]:

a. Tanur Besi *(Blast Furnace)*
b. Tanur Tinggi *(High Furnace)*
c. Mesin Penyemprotan Terus Menerus *(Continuous Casting Machine)*
d. Pabrik Gulungan *(Rolling Mill)*
e. Lini Galvanisasi *(Galvanizing Line)*
f. Lini Pelapisan *(Coating Line)*
g. Unit Pengolahan Air *(Water Treatment Unit)*
h. Pusat Distribusi dan Penyimpanan *(Distribution Center and Warehousing)*

PT Krakatau Steel melakukan pengamanan pada objek vital mereka dengan menerapkan berbagai langkah dan strategi keamanan. Beberapa cara umum yang dapat digunakan oleh perusahaan seperti PT Krakatau Steel untuk melakukan pengamanan objek vital adalah sebagai berikut [13]:

a. Pengamanan Fisik
   PT Krakatau Steel menggunakan langkah-langkah pengamanan fisik untuk melindungi objek vital mereka. Ini termasuk penggunaan pagar, gerbang, penghalang, kamera pengawas, dan sistem keamanan lainnya untuk mencegah akses yang tidak sah ke area yang sensitif.
b. Pengamanan Elektronik
   Perusahaan juga menggunakan sistem keamanan elektronik seperti sistem pengawasan video (CCTV), sistem alarm, dan akses kontrol elektronik untuk memantau dan mengendalikan akses ke objek vital mereka.
c. Keamanan Siber
   PT Krakatau Steel mengimplementasikan langkah-langkah keamanan cyber untuk melindungi sistem informasi dan teknologi yang digunakan dalam operasional mereka. Ini termasuk perlindungan terhadap serangan siber, seperti penggunaan firewall, enkripsi data, dan pembaruan rutin perangkat lunak keamanan.
d. Pengawasan Personel
   Perusahaan melakukan pengawasan personel dengan ketat untuk memastikan hanya orang yang berwenang yang memiliki akses ke objek vital. Ini melibatkan penerapan kebijakan dan prosedur keamanan yang ketat, termasuk identifikasi dan autentikasi pengguna, pengawasan lalu lintas masuk dan keluar, serta pelatihan keamanan kepada karyawan.
e. Pengelolaan Resiko
   PT Krakatau Steel melakukan evaluasi risiko secara berkala untuk mengidentifikasi ancaman dan risiko terhadap objek vital mereka. Ini membantu perusahaan untuk mengambil tindakan pencegahan yang tepat dan mengelola risiko dengan efektif.
f. Kesiap Siagaan Darurat
   Perusahaan memiliki rencana kesiapsiagaan darurat yang terstruktur dan dilatih dengan baik untuk menghadapi situasi darurat yang mungkin terjadi. Ini meliputi evakuasi, pemadaman kebakaran, tanggap bencana, dan tindakan lainnya untuk melindungi objek vital dan keselamatan karyawan.

Penting untuk dicatat bahwa PT Krakatau Steel mungkin memiliki langkah-langkah keamanan tambahan yang disesuaikan dengan kebutuhan dan karakteristik objek vital mereka. Upaya keamanan yang kuat dan berkelanjutan adalah suatu keharusan untuk menjaga integritas dan keberlanjutan operasional objek vital perusahaan.

Keamanan Data

Keamanan data salah Satu hal yang penting: keamanan Data bukan hanya tentang data format manual (tradisional), tetapi juga valid data terkomputerisasi. Untuk Dukungan keamanan informasi, maka Institusi harus memiliki

kebijakan yang secara khusus mengatur informasi keamanan.

Dalam sistem umum Keamanan informasi harus bisa Tentukan mana yang Anda inginkan untuk mengakses informasi dan fitur fungsi mana yang dapat digunakan pengguna dan menyukai sistem dapat mengidentifikasi pengguna yang mana datang ke tangan Anda.

Metode akses yang paling umum digunakan adalah password. Password seharusnya diganti sesering mungkin. Sistem juga harus dapat memberikan batasan apabila pemakai salah dalam memasukkan password. (Huffman, 1999)

Keamanan Data PT Krakatau Steel

PT Krakatau Steel adalah salah satu perusahaan baja terbesar di Indonesia. Seperti perusahaan lainnya, keamanan data menjadi faktor penting dalam menjaga informasi dan sistem mereka. Secara umum, perusahaan-perusahaan besar seperti PT Krakatau Steel biasanya mengimplementasikan serangkaian langkah-langkah untuk menjaga keamanan data mereka. Beberapa praktik yang umum dilakukan oleh perusahaan untuk melindungi data sensitif termasuk:

a. Penggunaan Firewall
   PT Krakatau besar menggunakan firewall yang kuat untuk melindungi jaringan mereka dari ancaman eksternal dan mencegah akses yang tidak sah.
b. Enkripsi data
   Data yang sensitif biasanya dienkripsi untuk melindungi kerahasiaannya. PT Krakatau Steel mungkin menerapkan metode enkripsi yang kuat untuk data mereka saat disimpan dan dikirim melalui jaringan.
c. Pengendalian Akses
   PT Krakatau Steel mungkin memiliki kebijakan pengendalian akses yang ketat untuk memastikan bahwa hanya orang yang berwenang yang dapat mengakses data sensitif. Ini bisa melibatkan penggunaan kata sandi yang kuat, otentikasi dua faktor, dan pembatasan akses berdasarkan peran pengguna.
d. Pelatihan Karyawan
   Pelatihan keamanan data kepada karyawan menjadi langkah penting untuk memastikan bahwa mereka memahami praktik keamanan yang baik. PT Krakatau Steel mungkin menyediakan pelatihan reguler kepada karyawan mereka untuk meningkatkan kesadaran keamanan.
e. Pemantauan dan Deteksi Ancaman
   PT Krakatau Steel menggunakan perangkat lunak dan sistem pemantauan yang canggih untuk mendeteksi aktivitas yang mencurigakan atau ancaman keamanan. Ini dapat membantu mereka mengidentifikasi serangan atau pelanggaran keamanan dengan cepat dan mengambil tindakan yang sesuai.

Mengatasi masalah keamanan data di PT Krakatau Steel, atau dalam hal umum di perusahaan apa pun, membutuhkan pendekatan yang komprehensif dan berlapis. Berikut adalah beberapa langkah yang dapat diambil untuk meningkatkan keamanan data di perusahaan:

a. Evaluasi Risiko
   Lakukan audit keamanan lengkap untuk mengidentifikasi potensi kerentanan dan ancaman keamanan yang mungkin ada di PT Krakatau Steel. Identifikasi aset penting dan data sensitif yang perlu dilindungi.
b. Kebijakan Keamanan Data
   Membuat kebijakan keamanan data yang jelas dan komprehensif untuk mengatur pengelolaan, penyimpanan, dan akses data. Pastikan kebijakan tersebut mencakup langkah-langkah untuk melindungi data di berbagai lapisan, termasuk perlindungan fisik dan logika.
c. Akses yang Dikelola
   Terapkan sistem akses yang dikelola dengan baik dengan membatasi akses ke data sensitif hanya kepada orang-orang yang membutuhkannya untuk pekerjaan mereka. Gunakan autentikasi ganda, peran dan izin akses yang tepat, serta implementasikan prinsip kebutuhan untuk mengetahui siapa yang memiliki akses ke data sensitif.
d. Cadangan Data yang Teratur
   Buat kebijakan cadangan data yang konsisten dan lakukan backup data secara teratur. Pastikan salinan data yang di-backup disimpan di lokasi yang aman dan dapat diakses jika terjadi kejadian bencana atau kerusakan fisik.
e. Pembaharuan dan Patching
   Perbarui sistem dan perangkat lunak secara teratur dengan memasang patch keamanan terbaru. Ini akan membantu melindungi sistem dari kerentanan yang diketahui dan meningkatkan keamanan secara keseluruhan.

Keamanan Siber

Keamanan Siber (cybersecurity) merujuk pada praktik dan upaya yang dilakukan untuk melindungi sistem komputer, jaringan, perangkat lunak, dan data dari ancaman, serangan, atau akses yang tidak sah. Keamanan Siber berfokus pada

menjaga kerahasiaan, integritas, dan ketersediaan informasi elektronik.

Ancaman keamanan siber dapat berasal dari berbagai sumber, seperti peretas (hacker), malware (program jahat), serangan phishing (penipuan online), serangan DDoS (Denial of Service), pencurian data, atau penggunaan yang tidak sah terhadap informasi pribadi.

Keamanan Siber sangat penting karena semakin banyaknya penggunaan teknologi informasi dan ketergantungan pada sistem komputer dan jaringan dalam berbagai aspek kehidupan kita. Pelanggaran keamanan siber dapat menyebabkan kerugian finansial, pencurian identitas, kerusakan reputasi, dan bahkan dapat mengancam keselamatan dan privasi individu atau organisasi. Oleh karena itu, melindungi informasi dan sistem dari ancaman keamanan siber merupakan prioritas yang sangat penting dalam dunia digital saat ini.

Keamanan Siber PT Krakatau Steel

Keamanan siber menjadi isu yang semakin penting dalam era digital saat ini. Perusahaan-perusahaan seperti PT Krakatau Steel, yang beroperasi dalam industri manufaktur, menghadapi risiko yang signifikan terkait serangan siber dan pelanggaran keamanan data. Penelitian ini bertujuan untuk menganalisis keamanan siber di PT Krakatau Steel dengan fokus pada identifikasi ancaman, kerentanan, dan langkah-langkah mitigasi yang telah diadopsi oleh perusahaan. Metode penelitian yang digunakan meliputi studi literatur, wawancara dengan personel keamanan perusahaan, dan analisis data yang tersedia.

Sebagai perusahaan manufaktur besar, PT Krakatau Steel menghadapi berbagai macam ancaman keamanan siber. Beberapa ancaman yang mungkin dihadapi oleh PT Krakatau Steel termasuk: Serangan Malware, Serangan DDoS (Denial of Service), Upaya Peretasan dan Penyusupan, Serangan Phishing dan Social Engineering, Kelemahan dalam Infrastruktur dan Aplikasi, Kecurangan dan Pencurian Data.

PT Krakatau Steel perlu menerapkan langkah-langkah keamanan yang kuat, seperti firewall, sistem deteksi intrusi, enkripsi data, pemantauan lalu lintas jaringan, dan kebijakan keamanan yang ketat. Selain itu, pelatihan dan kesadaran keamanan untuk karyawan juga penting untuk mengurangi risiko serangan siber internal, seperti phishing dan social engineering. Dengan mengadopsi pendekatan yang holistik terhadap keamanan siber, PT Krakatau Steel dapat mengurangi risiko dan melindungi sistem, data, dan reputasi perusahaan.

Kebijakan keamanan siber harus disusun, diimplementasikan, dan diperbarui secara berkala dengan mempertimbangkan perubahan lingkungan dan ancaman keamanan yang berkembang. Penting juga untuk melibatkan tim keamanan siber yang berpengalaman dalam merancang dan mengelola kebijakan keamanan siber perusahaan. berikut adalah beberapa kebijakan keamanan siber yang umumnya diterapkan dalam perusahaan Krakatau Steel untuk melindungi sistem dan data:

a. Kebijakan Penggunaan Password
   1) Mewajibkan penggunaan kata sandi yang kuat, kompleks, dan unik.
   2) Menetapkan kebijakan perubahan kata sandi secara berkala.
   3) Menerapkan kebijakan larangan penggunaan kata sandi yang umum dan mudah ditebak.
b. Kebijakan Akses Pengguna
   1) Menerapkan kontrol akses yang ketat untuk memastikan bahwa setiap pengguna hanya memiliki akses ke sistem dan data yang sesuai dengan tanggung jawab dan kebutuhan kerjanya.
   2) Memberikan hak akses minimum yang diperlukan untuk menjalankan tugas pekerjaan.
   3) Melakukan manajemen identitas dan akses untuk mengontrol dan memantau akses pengguna.
c. Kebijakan Penggunaan Perangkat Pribadi (BYOD)
   1) Menerapkan kebijakan yang jelas tentang penggunaan perangkat pribadi di lingkungan kerja.
   2) Memastikan adanya langkah-langkah keamanan yang sesuai untuk perangkat yang digunakan oleh karyawan, seperti enkripsi dan perlindungan dari malware.
d. Kebijakan Patching dan Pembaharuan Perangkat Lunak
   1) Menetapkan kebijakan pembaruan perangkat lunak secara teratur untuk mengatasi kerentanan keamanan yang ditemukan.
   2) Memastikan bahwa semua sistem dan perangkat lunak yang digunakan dalam organisasi, termasuk sistem operasi, perangkat lunak aplikasi, dan perangkat jaringan, diperbarui dengan pembaruan keamanan terbaru.
e. Kebijakan Firewall dan Sistem Deteksi Intruksi

1) Menggunakan firewall untuk memantau dan mengendalikan lalu lintas jaringan yang masuk dan keluar dari perusahaan.
2) Menerapkan sistem deteksi intrusi (IDS) dan sistem pencegahan intrusi (IPS) untuk mendeteksi dan mencegah serangan dari luar.

f. Kebijakan Enkripsi Data
1) Menerapkan kebijakan enkripsi data untuk melindungi data sensitif yang disimpan dan ditransmisikan di dalam perusahaan.
2) Menggunakan enkripsi end-to-end saat data dikirim melalui jaringan untuk melindungi kerahasiaan data.

4. KESIMPULAN

Berdasarkan uraian hasil dan pembahasan di atas, penulis menyimpulkan bahwa keamanan data, keamanan objek vital, dan keamanan siber sangat penting bagi PT Krakatau Steel atau perusahaan manapun dalam industri yang sensitif.

Secara keseluruhan, keamanan data, keamanan objek vital, dan keamanan siber adalah aspek yang penting dalam menjaga integritas, keselamatan, dan keberlanjutan PT Krakatau Steel. Investasi dalam sistem keamanan yang kuat dan pematuhan terhadap praktik terbaik keamanan informasi adalah langkah yang penting untuk mengatasi ancaman yang ada dan melindungi kepentingan perusahaan serta para pemangku kepentingan yang terkait.

a. Keamanan objek vital: Perlindungan objek vital atau fasilitas kritis perusahaan, seperti pabrik atau infrastruktur yang penting, merupakan kebutuhan yang mendesak. Implementasi sistem keamanan fisik yang kuat, seperti pengawasan, pengendalian akses, dan penggunaan teknologi keamanan modern, dapat membantu melindungi objek vital dari ancaman internal dan eksternal.
b. Keamanan data: PT Krakatau Steel, sebagai perusahaan besar, mungkin memiliki data yang berharga dan sensitif yang harus dijaga dengan baik. Perlindungan data melibatkan penggunaan langkah-langkah keamanan teknologi informasi, seperti enkripsi data, kontrol akses, kebijakan keamanan yang ketat, serta pelatihan dan kesadaran terhadap keamanan informasi bagi karyawan.
c. Keamanan siber: Keamanan siber menjadi semakin penting dalam era digital saat ini. PT Krakatau Steel mungkin perlu melindungi infrastruktur IT-nya dari serangan siber, seperti malware, serangan DDoS, dan upaya peretasan. Penerapan sistem keamanan siber yang kuat, termasuk firewall, sistem deteksi intrusi, pemantauan keamanan jaringan, serta pelatihan keamanan bagi staf, merupakan langkah penting dalam menghadapi ancaman siber.

Saran

Berdasarkan uraian yang disampaikan oleh penulis, maka penulis menyampaikan saran, antara lain:

a. Implementasikan sistem pengawasan dan pemantauan yang efektif untuk mengawasi aktivitas di area-area kritis.
b. Terapkan sistem pengendalian akses yang ketat dengan menggunakan kartu akses, kode PIN, atau teknologi otentikasi lainnya.
c. Pastikan adanya prosedur keamanan yang jelas dan dilaksanakan dengan konsisten, termasuk dalam hal identifikasi, verifikasi, dan pembatasan akses terhadap objek vital.
d. Atur tata kelola identitas dan akses yang baik dengan pemberian izin akses yang tepat berdasarkan kebutuhan dan tanggung jawab pengguna.
e. Tetapkan kebijakan keamanan siber yang jelas dan terkini, dan pastikan dipahami oleh seluruh karyawan.

5. DAFTAR PUSTAKA

[1] H. Namudat, N. Karlina, And B. Rusli, "Analisis Kebijakan Pengamanan Objek Vital Di Pt Freeport Indonesia," *Responsive*, Vol. 1, No. 2, P. 39, 2019, Doi: 10.24198/Responsive.V1i2.20673.

[2] K. Nistrina And M. Ridwan, "Jurnal Sistem Informasi , J-Sika Volume 01 Nomor 02 , Desember 2020 Presepsi Siswa Terhadap Pembelajaran Online Di Masa Pandemic Covid-19 Issn : 2716 - 4195," *J. Sist. Inf.*, Vol. 01, 2020.

[3] N. Matondang, I. N. Isnainiyah, And A. Muliawatic, "Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: Rsud Xyz)," *J. Resti (Rekayasa Sist. Dan Teknol. Informasi)*, Vol. 2, No. 1, Pp. 282–287, 2018, Doi: 10.29207/Resti.V2i1.96.

[4] H. C. Chotimah, "Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara [Cyber Security Governance And Indonesian Cyber Diplomacy By National Cyber And Encryption Agency]," *J. Polit. Din. Masal. Polit. Dalam Negeri Dan Hub. Int.*, Vol. 10, No. 2, Pp. 113–128, 2019, Doi: 10.22212/Jp.V10i2.1447.

[5] E. Soesanto, A. Rohmawati, N. S. Anggraini, And S. N. Hanifah, "Ijm : Indonesian Journal Of Multidisciplinary Analisis Pengimplementasian Objek Vital Nasional , Pengamanan File , Dan Cyber Security Pada Pt . Angkasa Pura," Vol. 1, Pp. 217–224, 2023.

[6] J. Yulianto, S. Thamrin, Y. Ali, And A. Manab Idris, "Analisis Potensi Ancaman Asimetris Berdasarkan Kerentanan Keamanan Siber Sektor Industri Energi Baru Terbarukan (Ebt)," *J. Kewarganegaraan*, Vol. 6, No. 2, Pp. 2829–2835, 2022.

[7] H. Primawanti And S. Pangestu, "Diplomasi Siber Indonesia Dalam Meningkatkan Keamanan Siber Melalui Association Of South East Asian Nation (Asean) Regional Forum," *Glob. Mind*, Vol. 2, No. 2, Pp. 1–15, 2020, Doi: 10.53675/Jgm.V2i2.89.

[8] A. Farid, "Pengertian Cyber Security Dan 5 Metode Ancamannya," *Exabytes*, 26 September 2022. Https://Www.Exabytes.Co.Id/Blog/Pengertian-Cyber-Security/ (Diakses 6 Juni 2023).

[9] Its, "Keamanan Siber," *Its.Ac.Id*. Https://Www.Its.Ac.Id/It/Id/Keamanan-Siber/#:~:Text=Apa%20itu%20keamanan%20siber%3f,Atau%20mengganggu%20proses%20bisnis%20normal (Diakses 6 Juni 2023).

[10] H. Bsn, "Krakatau Steel Ditetapkan Salah Satu Obyek Vital Nasional Sektor Industri," *Bsn.Go.Id*, 10 Juli 2022. Https://Www.Bsn.Go.Id/Main/Berita/Detail/13053/Krakatau-Steel-Ditetapkan-Salah-Satu-Obyek-Vital-Nasional-Sektor-Industri (Diakses 6 Juni 2023).

[11] H. Abdi, "Profil Pt Krakatau Steel, Sejarah, Dan Produk-Produknya - Hot Liputan6.Com," *Www.Liputan6.Com*, 21 Desember 2022. Https://Www.Liputan6.Com/Hot/Read/5162007/Profil-Pt-Krakatau-Steel-Sejarah-Dan-Produk-Produknya (Diakses 6 Juni 2023).

[12] Amazon Aws, "Apa Itu Keamanan Siber? - Penjelasan Tentang Keamanan Siber - Aws," *Www.Amazon.Com*. Https://Aws.Amazon.Com/Id/What-Is/Cybersecurity/ (Diakses 6 Juni 2023).

[13] Johanna, "Pentingnya Keamanan Data Di Internet Dan Cara Menjaganya," *Dewaweb.Com*, 31 Januari 2023. Https://Www.Dewaweb.Com/Blog/Mengenal-Keamanan-Data/ (Diakses 6 Juni 2023).