Jurnal Bisnis, Logistik dan Supply Chain
(BLOGCHAIN)
OPEN ACCES ISSN: 2809-7491
https://ejournal-ibik57.ac.id/index.php/blogchain
Volume 3, Nomor 1, Mei (2023)
Halaman 23 – 32
DOI: https://doi.org/10.55122/blogchain.v3i1.714

ANALISIS POTENSI DAN STRATEGI PENCEGAHAN *CYBER CRIM* DALAM SISTEM LOGISTIK DI ERA DIGITAL

PENULIS [1)]**Dewi Rizka Yuniarti,** [2)]**Hafidz Fauzan Alfarizy,** [3)]**Zifron Siallagan,** [4)]**Mochamad Whilky Rizkyanfi**

ABSTRAK

Penelitian ini bertujuan untuk melakukan analisis terhadap potensi risiko *cyber crime* dalam sistem logistik, serta mengidentifikasi strategi pencegahan yang dapat diterapkan untuk mengurangi risiko tersebut. Penelitian ini menggunakan metode studi literatur. Metode studi literatur merupakan metode yang melibatkan serangkaian aktivitas yang terkait dengan cara mengumpulkan data dari sumber pustaka, melakukan pembacaan dan pencatatan informasi, serta melakukan analisis terhadap bahan penelitian yang telah dikumpulkan. Hasil penelitian menemukan bahwa ancaman serangan *cyber crime* pada sistem logistik dapat berasal dari berbagai pihak seperti peretas atau *hacker*, kelompok kriminal yang terorganisir, atau bahkan pekerja internal yang memiliki akses ke sistem logistik perusahaan. Kemudian terdapat strategi pencegahan *cyber crime* dalam sistem logistik yaitu: mengganti *password* secara berkala, *penetration testing*, memperbarui *software* yang digunakan, melaksanakan pelatihan karyawan, menggunakan kombinasi kata sandi yang rumit, menggunakan layanan *hosting* yang aman, membuat rencana keamanan sistem, melakukan enkripsi dan pencadangan data sensitif secara teratur, menggunakan WAF, dan menggunakan aplikasi blockchain.

Kata Kunci: Kejahatan Siber, Logistik, Teknologi

ABSTRACT

This study aims to analyze the potential risks of cyber crime in logistics systems and identify prevention strategies that can be applied to reduce those risks. This research uses a literature study method. The literature study method involves a series of activities related to how data is collected from library sources, information reading and recording, and analyzing the research material that has been collected. The research found that cyber crime attacks on logistics systems can come from various sources such as hackers, organized criminal groups, or even internal employees who have access to the company's logistics system. Prevention strategies for cyber crime in logistics systems include: regularly changing passwords, penetration testing, updating software used, conducting employee training, using complex password combinations, using secure hosting services, creating a system security plan, regularly encrypting and backing up sensitive data, using WAF, and using blockchain applications.

Keywords: *Cyber crime, Logistics, Technology*

AFILIASI

Prodi, Fakultas: [1-4)]Teknik Logistik, Fakultas Pendidikan Teknologi dan Kejuruan
Nama Institusi: [1-4)]Universitas Pendidikan Indonesia
Alamat Institusi: [1-4)]Jl. Dr. Setiabudhi No.229, Isola, Kec. Sukasari, Kota Bandung, Jawa Barat - 40154

KORESPONDENSI

Penulis: Dewi Rizka Yuniarti
Email: dewirizkaa@upi.edu

PENDAHULUAN

Pemanfaatan teknologi informasi yang terus berkembang dan selalu dibutuhkan oleh masyarakat sebagai faktor penunjang berbagai aktivitas. Berbagai lembaga sudah menerapkan teknologi informasi, seperti lembaga kesehatan, pendidikan, keuangan, pemerintahan, dan bidang industri. Teknologi Informasi dan Komunikasi memberikan dampak positif terhadap berbagai kegiatan. Teknologi memberikan kemudahan dan kenyamanan dalam banyak hal, dari berkomunikasi dengan orang-orang yang jauh, hingga melakukan transaksi bisnis secara *online*. Namun, semakin berkembangnya teknologi memberikan peluang untuk sarana dilakukan kejahatan baru.

Keamanan teknologi informasi (TI) adalah salah satu masalah utama yang menjadi perhatian bisnis—sistem yang diretas atau data yang dicuri dapat membuat perusahaan gulung tikar (Pearlson & Saunders, 2016). *Cyber crime* adalah salah satu bentuk aktivitas ilegal yang terjadi pada dunia maya melalui perantara komputer atau melalui peralatan elektronik lainnya dengan mencoba mendapatkan akses ke jaringan komputer secara ilegal dengan maksud merusak atau mencuri data (Putera et al., n.d., 2018). *Cyber crime* merupakan kegiatan yang bertentangan dengan hukum-hukum yang berlaku.

Dalam era digital, sistem logistik menjadi semakin kompleks dan terintegrasi, sehingga membuatnya lebih rentan terhadap serangan *cyber crime* yang dapat merusak reputasi perusahaan dan mengakibatkan kerugian finansial yang besar. Sehingga, analisis potensi dan strategi pencegahan *cyber crime* dalam sistem logistik sangat penting untuk memastikan keamanan dan keberlanjutan sistem logistik yang efisien.

Keamanan sistem informasi sangat penting untuk mencegah *cyber crime*. Sistem logistik modern menggunakan teknologi informasi untuk mengintegrasikan seluruh rantai pasok (Rusmana & Setyawan, 2021), mulai dari pemesanan hingga pengiriman produk kepada pelanggan. Dimana pengamanan data dan informasi dalam sistem logistik perlu ditingkatkan untuk mencegah akses yang tidak sah.

Menurut (Stallings, 2018), "Keamanan Sistem Informasi" merupakan upaya untuk melindungi sistem informasi, terutama data sensitif dan penting, dari akses yang tidak sah, perubahan, atau kerusakan. Konsep keamanan sistem informasi mencakup sejumlah faktor, seperti kerahasiaan, integritas, dan ketersediaan.

Selain itu, menurut (Wang, D., dan Liang, D., 2020), penggunaan teknologi blockchain juga dapat menjadi solusi untuk mencegah *cyber crime* dalam sistem logistik. Teknologi blockchain memungkinkan pengguna untuk memverifikasi keabsahan data secara otomatis dan dapat memberikan transparansi yang lebih tinggi dalam rantai pasok (Manners-Bel & Lyon, 2019; Paksoy et al., 2021). Dengan demikian, teknologi blockchain dapat membantu mencegah *cyber crime* dalam sistem logistik dengan meningkatkan keamanan dan validitas data.

(Wang, D., dan Liang, D., 2020) juga menjelaskan bahwa blockchain merupakan teknologi yang dapat memberikan keamanan yang sangat baik pada data, karena menggunakan sistem database terdesentralisasi dan terenkripsi yang menghindari manipulasi data atau akses yang tidak sah. Teknologi blockchain juga memiliki sistem pengauditan yang kuat dan dapat meningkatkan transparansi dalam pengelolaan data.

Dalam konteks logistik, teknologi blockchain dapat diterapkan dalam berbagai aspek, seperti identifikasi produk, pelacakan dan pengecekan kualitas, serta manajemen pengiriman. Dengan menerapkan teknologi blockchain, perusahaan logistik dapat memastikan bahwa data dan informasi yang beredar dalam sistemnya terlindungi dari *cyber crime*.

Keuntungan penggunaan teknologi blockchain juga dapat membantu meningkatkan kepercayaan pelanggan terhadap perusahaan

logistik. Hal ini karena teknologi blockchain dapat memastikan keaslian dan keabsahan data terkait produk yang dikirimkan.

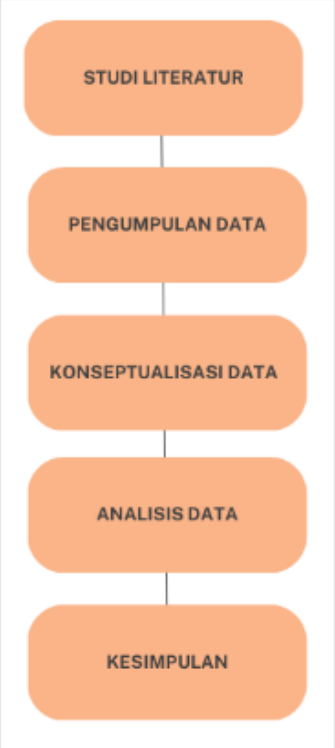
Strategi pencegahan *cyber crime* dalam sistem logistik perlu mencakup tindakan preventif, detektif, dan responsif serta melibatkan pihak-pihak yang terkait seperti perusahaan logistik, pemerintah, dan lembaga keamanan. Implementasi teknologi keamanan yang canggih seperti enkripsi data, blockchain, *firewall*, dan *monitoring* keamanan dapat membantu mencegah serangan *cyber crime* dalam sistem logistik. Dalam hal ini, perusahaan logistik harus memperhatikan dan mengikuti standar keamanan siber yang dikeluarkan oleh pemerintah dan lembaga keamanan, hal memastikan agar sistem keamanan yang digunakan selalu diperbarui dan terus dikembangkan sesuai dengan perkembangan teknologi dan jenis serangan baru. Selain itu, penting juga untuk melakukan pelatihan dan pengembangan kesadaran *cyber security* bagi karyawan dan pengguna sistem logistik agar mereka dapat memahami risiko *cyber crime* dan tindakan yang harus dilakukan untuk mencegahnya. Dengan demikian, gabungan strategi pencegahan dan implementasi teknologi keamanan yang baik, serta kesadaran *cyber security* yang baik, dapat membantu melindungi sistem logistik dari serangan *cyber crime*.

Penelitian ini bertujuan untuk melakukan analisis terhadap potensi risiko *cyber crime* dalam sistem logistik, serta mengidentifikasi strategi pencegahan yang dapat diterapkan untuk mengurangi risiko tersebut. Selain itu, tujuan dari artikel ini adalah untuk meningkatkan kesadaran mengenai pentingnya keamanan sistem logistik di era digital. Dalam mencapai tujuan tersebut, artikel ini akan membahas berbagai berbagai aspek terkait dengan risiko *cyber crime* dalam sistem logistik, termasuk jenis-jenis serangan *cyber crime* yang umum terjadi pada sistem logistik, dampak dari serangan *cyber crime* pada sistem logistik, serta berbagai strategi pencegahan yang dapat diterapkan untuk mengurangi risiko *cyber crime*.

METODE PENELITIAN

Penulis menggunakan pendekatan penelitian kualitatif dalam mengembangkan artikel ilmiah ini. Penelitian kualitatif adalah penelitian yang merujuk pada suatu metode penelitian yang menguji hipotesis dengan melakukan analisis terhadap hubungan antar-variabel (Fadlila et al., 2022, p. 40; Creswell, 2009:6). Metode penelitian kualitatif cocok digunakan untuk penelitian yang membutuhkan analisis mendalam dengan memanfaatkan berbagai data yang terdapat pada dokumen-dokumen sebelumnya (Fadlila et al., 2022, p .40). Tujuan dari penelitian kuantitatif adalah untuk menjelaskan suatu masalah dengan menghasilkan temuan yang dapat diterapkan secara umum.

Studi literatur merupakan salah satu cara memperoleh data menggunakan penelitian kualitatif. Metode studi literatur merupakan metode yang melibatkan serangkaian aktivitas yang terkait dengan cara mengumpulkan data dari sumber pustaka, melakukan pembacaan dan pencatatan informasi, serta melakukan analisis terhadap bahan penelitian yang telah dikumpulkan. Tujuan dari metode ini adalah untuk memperoleh pemahaman yang mendalam mengenai topik penelitian yang sedang dibahas.



Gambar 1. Metode Kualitatif Studi Literatur

HASIL DAN PEMBAHASAN

Potensi *Cyber crime* dalam Sistem Logistik

Ancaman serangan *cyber crime* pada sistem logistik dapat berasal dari berbagai pihak seperti peretas atau *hacker*, kelompok kriminal yang terorganisir, atau bahkan pekerja internal yang memiliki akses ke sistem logistik perusahaan. Serangan tersebut dapat terjadi melalui berbagai jenis serangan, menurut (Shen, X., Chen, H., Liu, H., dan Chen, Z., 2021) seperti :

Malware: adalah jenis serangan yang menggunakan perangkat lunak jahat untuk menginfeksi sistem logistik perusahaan dan mengumpulkan data, seperti informasi pelanggan, stok inventaris, dan transaksi keuangan .

Phishing: adalah jenis serangan yang menggunakan email atau situs web palsu untuk memperoleh informasi sensitif dari karyawan perusahaan, seperti kata sandi atau informasi keuangan.

Ransomware: adalah jenis serangan yang memaksa perusahaan membayar uang tebusan untuk mengembalikan akses ke sistem logistik yang terinfeksi. *Ransomware* umumnya mengunci atau mengenkripsi data sehingga perusahaan tidak dapat mengaksesnya.

Man-in-the-Middle (MITM): adalah jenis serangan yang memungkinkan penyerang untuk memantau atau mengubah komunikasi antara sistem logistik dan pihak lain, seperti vendor atau pelanggan. Penyerang dapat mencuri informasi sensitif, seperti kata sandi atau nomor kartu kredit.

Distributed Denial of Service (DDoS): adalah jenis serangan yang melumpuhkan sistem logistik dengan membanjiri lalu lintas jaringan dengan permintaan yang tidak perlu. Hal ini dapat menyebabkan penurunan kinerja sistem logistik atau bahkan penghentian total.

Serangan *malware* misalnya, dapat memperoleh akses ke sistem logistik perusahaan dan mengumpulkan data pribadi pelanggan atau informasi penting lainnya. Serangan *Ransomware* dapat mengenkripsi data dan meminta tebusan untuk mengembalikan data tersebut. Serangan *phishing* dapat memperoleh akses ke akun email atau jaringan perusahaan melalui pengiriman email palsu atau pesan teks.

Tabel 1. Persentase Serangan *Cyber Crime* dalam Sistem Logistik

Jenis Serangan	Persentase Serangan
Malware	35%
Phishing	25%
Ransomware	20%
Man-in-the-Middle (MITM)	10%
Distributed Denial of Service (DDoS)	10%

Sumber: (Shen, X. et al., 2021)

Dampak *Cyber crime* dalam Sistem Logistik

Serangan *cyber crime* pada sistem logistik dapat menimbulkan kerugian finansial yang signifikan bagi perusahaan. Kerugian dapat berasal dari biaya untuk memulihkan sistem logistik yang terkena serangan, biaya untuk memperbaiki kerusakan pada infrastruktur, atau biaya untuk membayar tebusan dalam serangan *Ransomware*. Selain itu, kerugian juga dapat berupa hilangnya data yang berharga, terutama jika data tersebut merupakan informasi penting seperti rencana produksi, rencana pemasaran, atau data pelanggan.

Selain itu, kerugian juga dapat berupa penundaan pengiriman produk atau layanan, yang dapat mengganggu operasi rantai pasok perusahaan. Hilangnya kepercayaan pelanggan akibat serangan *cyber crime* juga dapat menjadi kerugian yang signifikan bagi perusahaan, karena dapat mempengaruhi reputasi perusahaan dalam jangka panjang.

Sebagai contoh, pada tahun 2018, serangan siber terhadap perusahaan logistik Toll Group di Australia menyebabkan penundaan pengiriman dan kerugian finansial yang signifikan bagi perusahaan.

Tabel 2. Contoh Serangan *Cyber Crime* dalam Sistem Logistik

Tahun	Perusahaan	Jenis Serangan	Kerugian Finansial
2017	Maersk, FedEx, dll.	*WannaCry*	$1.2 miliar
2018	Toll Group (Australia)	*Malware*	$45 juta
2020	CMA CGM	*Ransomware*	$30 juta

Sumber: (Shen, X. et al., 2021)

Serangan *cyber crime* pada sistem logistik dapat memiliki dampak yang signifikan pada pihak yang terkait, baik secara operasional maupun finansial. Dalam operasional, serangan tersebut dapat mengganggu alur rantai pasok dan mengakibatkan keterlambatan pengiriman barang, kehilangan data penting.

Selain itu, serangan *cyber crime* juga dapat menimbulkan kerugian finansial yang besar, baik dalam bentuk biaya pemulihan sistem maupun kehilangan pendapatan akibat gangguan pada operasi. Ada beberapa dampak dari serangan *cybercrime* pada sistem logistik menurut (Shen, X., Chen, H., Liu, H., dan Chen, Z., 2021):

Kehilangan Data, serangan *cyber crime* seperti *malware* dan *phishing* dapat menyebabkan perusahaan kehilangan data yang penting, seperti data pelanggan, stok inventaris, dan transaksi keuangan. Kehilangan data dapat mengakibatkan kerugian keuangan yang signifikan, kerusakan reputasi, dan bahkan tuntutan hukum.

Gangguan Layanan, serangan *cyber crime* seperti DDoS dapat mengakibatkan gangguan pada layanan sistem logistik perusahaan. DDoS membanjiri lalu lintas jaringan dengan permintaan yang tidak perlu sehingga dapat menyebabkan penurunan kinerja sistem logistik atau bahkan penghentian total. Ini dapat menyebabkan kerugian keuangan dan reputasi yang signifikan, serta menimbulkan ketidaknyamanan bagi pelanggan yang membutuhkan layanan logistik perusahaan.

Kerugian keuangan, serangan *cyber crime* seperti *Ransomware* dapat mengakibatkan kerugian keuangan yang signifikan bagi perusahaan. *Ransomware* memaksa perusahaan membayar uang tebusan untuk mengembalikan akses ke sistem logistik yang terinfeksi. Perusahaan juga dapat mengalami kerugian finansial akibat biaya pemulihan sistem, penggantian peralatan yang rusak, dan hilangnya pendapatan akibat gangguan layanan.

Kerusakan reputasi, serangan *cyber crime* dapat merusak reputasi perusahaan di mata pelanggan, mitra bisnis, dan masyarakat umum. Jika perusahaan gagal melindungi data pelanggan atau mengalami gangguan layanan yang signifikan, maka hal ini dapat mengurangi kepercayaan dan

loyalitas pelanggan serta merusak citra perusahaan. Kerusakan reputasi dapat menyebabkan penurunan pendapatan dan hilangnya peluang bisnis di masa depan.

Jenis Kejahatan *Cyber Crime* dalam Sistem Logistik

Ada beberapa jenis kejahatan *cyber crime* yang umum terjadi pada sistem logistik, antara lain:

1) Peretasan Situs dan Email
   Kejahatan ini dapat dimaknai dengan email dan *deface website*. Yakni jenis kejahatan *cyber crime* yang dilakukan dengan meretas sebuah situs ataupun email, serta mengubah tampilannya. Dengan kata lain, tampilan web atau email seketika berubah akibat peretasan ini. Contoh kasus pada kejahatan siber ini yaitu, Transnet. Transnet merupakan perusahaan logistik milik Afrika Selatan ini mengalami serangan siber, sabotase, dan intrusi keamanan, yang mengakibatkan terganggunya proses dan fungsi normal TPT atau kerusakan peralatan atau informasi.

2) Remote Administrator Tools (RAT)
   RAT adalah *malware* yang memungkinkan pelaku untuk mengontrol perangkat dari jarak jauh jika alat tersebut terpasang atau

ter unduh dalam sebuah gadget. RAT yang terpasang pada ponsel korban dapat dengan mudah dikendalikan dari jarak jauh oleh pelaku. Dengan arti lainnya, ini akan menjadi 'pintu' bagi peretas untuk masuk ke dalam sistem *smartphone* korban. Salah satu kasus yang dapat diambil dari kejahatan ini yaitu, penipuan berkedok paket. Dari pengucapannya, temannya yang tidak tahu tentang modus penipuan berkedok paket tanpa mengetahuinya mengeklik file APK yang disebut sebagai 'cek resi'. Akibatnya, rekening di Bank Rakyat Indonesia miliknya dikuras habis.

3) Serangan *Ransomware*
Ransomware merupakan *malware* atau *software* yang menangkal pengguna mengakses sistem mereka hingga uang tebusan dibayarkan. Sektor transportasi dan logistik menjadi sasaran yang sangat diminati untuk serangan ini. Pada bulan Mei 2021, serangan *Colonial Pipeline* mengganggu pasokan bahan bakar jet dan bensin ke wilayah yang luas di wilayah tenggara AS. Sementara dampak keuangan langsung adalah pembayaran uang tebusan sebesar $4,4 juta, dampak keuangan dan sosial ekonomi tidak langsung terhadap pasokan terkait rantai jauh lebih besar.

4) Kejahatan *Phising*
Perusahaan logistik dan pelayaran semakin menjadi target serangan *phishing*. *Phishing* melibatkan penjahat dunia maya yang menghubungi organisasi target melalui email (*phishing*), telepon (*vishing*), atau pesan teks (*SMSishing*), dan berpura-pura sebagai orang atau organisasi yang sah.

Tujuan serangan ini adalah untuk memikat penerima agar menyerahkan data sensitif dan kata sandi untuk mengakses data secara ilegal demi keuntungan finansial. Contoh yang sangat relevan adalah selama pandemi, ketika penjahat dunia maya menggunakan teknik *phishing* untuk menargetkan *cold supply chain* COVID-19. Serangan tersebut memperoleh akses ke jaringan produsen penyimpanan suhu rendah Haier Biomedical sebelum menggunakan sistem emailnya sendiri untuk mendistribusikan email *phishing* lebih lanjut ke mitra yang terlibat dalam pengiriman vaksin.

Standar Keamanan Siber yang Dikeluarkan oleh Pemerintah

Keamanan Siber dan Pertahanan Siber mempunyai kaitan yang cukup erat, yaitu keduanya digunakan untuk melindungi dan menjaga kerahasiaan, integritas, dan ketersediaan data elektronik atau sistem elektronik.

Keamanan Siber dapat menjadi salah satu bentuk dari Pertahanan Siber. Di lain pihak, Pertahanan Siber dapat menjadi pertahanan aktif maupun pertahanan pasif. Pertahanan pasif yang relevan dapat dimasukkan dalam bidang keamanan siber.

Data dan informasi merupakan sumber daya yang penting untuk suatu badan atau lembaga di era digital saat ini. Ketersediaan, kemudahan penggunaan, dan keamanan informasi harus diperhatikan agar informasi tetap tersedia untuk publik.

Salah satu hal yang dapat mengganggu ketersediaan data yaitu ancaman siber. Untuk melindungi data dan menghindari segala ancaman siber, keamanan siber (*cyber security*) harus diterapkan. Keamanan siber (*cyber security*) adalah upaya untuk menjaga kerahasiaan, keutuhan dan ketersediaan informasi dari serangan digital.

Keamanan siber memiliki peran yang sangat penting, maka dari itu, negara hadir melalui Badan Siber dan Sandi Negara (BSSN) dengan membentuk *Computer Security Incident Response Team* (CSIRT) sebagai salah satu eksekutor keamanan siber di Indonesia. Computer Security Incident Response Team (CSIRT) adalah tim yang menyediakan layanan untuk mencegah, mengatasi dan menanggapi insiden keamanan siber di suatu wilayah yang bertanggung jawab

untuk penerimaan, peninjauan dan penindakan laporan dan aksi insiden keamanan siber.

Strategi Pencegahan *Cyber crime* dalam Sistem Logistik

Dalam mencegah kejahatan siber (*Cyber crime*) dalam sistem logistik, pentingnya strategi dan kewaspadaan yang tinggi dari seluruh karyawan atau anggota tim yang menggunakan sistem logistik. Beberapa strategi pencegahan yang tepat untuk menjaga keamanan sistem logistik dan membantu mencegah serangan *cyber crime* antara lain yaitu:

1) Mengganti *Password* Secara Berkala
   Dalam strategi mencegah *cyber crime* dalam sistem logistik, pengguna sistem logistik harus mengubah *password* mereka secara teratur, seperti setiap dua atau empat bulan sekali. Hal tersebut bertujuan untuk mengurangi risiko terjadinya pencurian *password* atau peretasan yang dapat menyebabkan kebocoran data atau kerugian keamanan lainnya. Dengan mengubah *password* secara teratur, pengguna sistem logistik dapat meningkatkan tingkat keamanan dan menghindari akses yang tidak sah ke dalam sistem.

2) Penetration Testing
   Salah satu cara untuk mencegah kejahatan siber adalah dengan melakukan pengujian penetrasi secara teratur. *Penetration Testing* merupakan salah satu cara pengujian keamanan pada struktur jaringan komputer yang dilakukan dengan cara yang menyerupai serangan dari seorang peretas.

   Pengujian penetrasi dilakukan oleh para ahli keamanan (*pentester*) dalam bentuk simulasi serangan siber untuk menguji seberapa aman sistem yang sedang digunakan. Dari hasil pengujian tersebut, akan diketahui kerentanan atau kelemahan yang ada pada sistem sehingga dapat segera diperbaiki.

3) Memperbarui *Software* yang Digunakan
   Salah satu pencegahan *cyber crime*, yaitu dengan melakukan pembaruan *software*. Pengembang *software* akan memperbarui versi sistem yang dikembangkan untuk meningkatkan kualitas *software* dari segi performa dan keamanan. Jika perusahaan masih menggunakan *software* lama, maka dengan mudah peretas dapat mengeksploitasi kerentanan tersebut untuk mendapatkan akses ke data yang bersifat penting, sehingga terjadi kebocoran data yang merugikan perusahaan dan pelanggan.

   Contoh dari serangan siber yang dapat menyebabkan kerugian besar bagi perusahaan adalah serangan *Ransomware WannaCry,* yang disebabkan oleh ketidakmampuan perusahaan untuk memperbarui sistem yang digunakan. Kasus tersebut dapat membuat perusahaan kehilangan data.

4) Melaksanakan Pelatihan Karyawan
   Tidak hanya disebabkan oleh kerentanan pada sistem keamanan, pelanggaran keamanan siber juga sering kali diakibatkan oleh kesalahan manusia. *Social engineering* merupakan jenis serangan yang sering digunakan untuk melakukan penipuan pada target, dan para peretas menggunakan taktik tersebut karena mereka menyadari bahwa manusia atau pengguna merupakan elemen paling rentan dalam sistem keamanan.

   Bagi sebuah perusahaan, penting dilakukannya pelatihan karyawan tentang keamanan *cyber*. Pelatihan keamanan *cyber* harus dilakukan secara rutin untuk mengikuti perkembangan teknologi terkini dan meminimalkan risiko kerentanan keamanan yang disebabkan oleh kelalaian karyawan.

5) Menggunakan Kombinasi Kata Sandi yang Rumit
   Menerapkan kata sandi yang rumit adalah cara yang efektif untuk mencegah *cyber crime* di perusahaan. Semua anggota staf di

perusahaan harus memastikan bahwa mereka menggunakan kata sandi yang rumit untuk seluruh sistem yang tersedia dan aplikasi yang mereka akses.

Selain itu, penting untuk tidak menggunakan kata sandi yang sama pada aplikasi yang berbeda. Menggunakan karakter yang cukup panjang, menggunakan kombinasi kata sandi seperti angka, huruf kecil, simbol, dan huruf kapital, dan menghindari penggunaan informasi pribadi seperti tanggal lahir sebagai password, merupakan beberapa tips dalam membuat kata sandi yang kuat.

6) Menggunakan Layanan Hosting yang Aman
Hosting adalah layanan yang menyediakan server untuk menyimpan halaman situs web sehingga dapat diakses melalui koneksi internet dari komputer di seluruh dunia (Sturm et al., 2017). Ada dua jenis layanan hosting yang tersedia, yaitu layanan hosting berbayar dan layanan hosting gratis.

Dalam mengelola suatu *website*, agar data yang ada terlindungi, disarankan untuk memastikan bahwa *website* tersebut menggunakan layanan hosting yang aman. Penting juga untuk memverifikasi bahwa layanan hosting yang digunakan memiliki perlindungan terhadap serangan *cyber crime*, termasuk serangan DDoS.

7) Membuat Rencana Keamanan Sistem (*System Security Plan*)
Rencana keamanan sistem adalah sebuah dokumen resmi yang memberikan penjelasan komprehensif mengenai kriteria keamanan untuk sistem informasi. Di dalam dokumen tersebut, dijelaskan mengenai cara membatasi akses bagi pengguna resmi, menjamin praktik-praktik keamanan oleh karyawan, dan memberikan penjelasan tentang tindakan yang harus diambil oleh karyawan ketika terjadi pelanggaran keamanan.

8) Melakukan Enkripsi dan Pencadangan Data Sensitif secara Teratur
Data merupakan aset berharga bagi suatu perusahaan. Dengan melakukan pencadangan data secara berkala, perusahaan dapat memperoleh manfaat dalam pemulihan data yang hilang akibat serangan *cyber crime* dan melindungi data saat terjadi kerusakan sistem komputer. Pencadangan data dapat dilakukan melalui beberapa perangkat, seperti drive eksternal portabel, USB stick atau USB flash drive.

Menyimpan data di *cloud* dengan penggunaan enkripsi ketika menyimpan dan mentransfer data merupakan salah satu cara untuk membackup data yang lebih aman.

9) Menggunakan WAF (Web Application Firewall)
Web Application Firewall (WAF) adalah aplikasi firewall yang berfungsi untuk melindungi web application atau situs perusahaan. Dengan penerapan WAF (Web Application Firewall), situs dapat terhindar dari beragam ancaman keamanan siber seperti DDoS attack, cross-site forgery, cross-site-scripting (XSS), SQL injection, dan sejenisnya. Sistem tersebut akan secara otomatis menolak dan memblokir akses ketika terdeteksi lalu lintas yang mencurigakan atau menunjukkan tanda-tanda sebagai ancaman terhadap keamanan *website* perusahaan.

10) Menggunakan Aplikasi Blockchain
Dalam sistem logistik, aplikasi blockchain dapat digunakan untuk mengamankan dan melacak seluruh proses logistik, mulai dari pemesanan, pengiriman, hingga pengiriman barang. Dengan menggunakan aplikasi blockchain, seluruh proses logistik dapat dimonitor secara *real-time* dan transparan, sehingga memudahkan pengawasan dan deteksi ketika terjadi kecurangan atau ancaman keamanan lainnya.

Aplikasi blockchain memungkinkan data untuk disimpan secara terdesentralisasi, yang artinya tidak ada satu entitas tunggal yang mengontrol atau memiliki akses ke seluruh data. Dengan demikian, risiko kebocoran atau peretasan data dapat dikurangi.

Selain itu, transaksi pada aplikasi blockchain menggunakan enkripsi yang kuat dan tersimpan dalam blok yang dienkripsi. Hal ini memastikan bahwa data tidak dapat diubah atau dimanipulasi tanpa persetujuan dari mayoritas pengguna.

Selain itu, setiap blok pada blockchain memiliki tanda waktu dan salinan yang didistribusikan ke setiap node pada jaringan, sehingga memungkinkan untuk memverifikasi keaslian dan integritas data.

KESIMPULAN

Berdasarkan analisis yang telah kami lakukan, dapat disimpulkan bahwa *cyber crime* merupakan ancaman serius dalam sistem logistik di era digital. Dalam menghadapi ancaman ini, perlu dilakukan strategi pencegahan yang tepat agar sistem logistik dapat berjalan dengan aman dan efisien.

Dalam menjalankan strategi pencegahan, perusahaan perlu melakukan pengawasan secara berkala, meningkatkan kesadaran serta keterampilan karyawan terkait dengan keamanan siber dan memperbarui sistem keamanan secara teratur. Dengan demikian, diharapkan dapat mengurangi risiko terjadinya *cyber crime* dalam sistem logistik dan meningkatkan efisiensi serta keamanan sistem secara keseluruhan.

REFERENSI

Arifah, D. A. (2011). Kasus cybercrime di indonesia. jurnal Bisnis dan Ekonomi, 18(2). https://www.unisbank.ac.id/ojs/index.php/fe3/article/view/2099

Brown, M. (2022, Oktober 13). The rising risk of cybercrime in the supply chain. The rising risk of cybercrime in the supply chain. Retrieved March 14, 2023, from https://www.supplychainquarterly.com/articles/7239-the-rising-risk

Cermati.com. (2022, November 21). 14 Jenis Cyber Crime, Kejahatan Internet yang Merugikan. Cermati.com. Retrieved March 14, 2023, from https://www.cermati.com/artikel/jenis-cyber-crime

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

Fadlila, A. I., Hermawan, B. Y. F. A., Pinasti, R. T., & Alifah, A. N. (2022). D-Locode: Aplikasi Peningkatan Keamanan Data Pengguna Layanan Logistik Dengan Metode Quick Response Code Pada Sistem Pengiriman Barang. Lomba Karya Tulis Ilmiah, 3(1), 31-46.

Feradhita. (2021, February 1). 9 Cara Mencegah *Cyber crime* Agar Tidak Terjadi di Perusahaan Anda. LOGIQUE. Retrieved March 14, 2023, from https://www.logique.co.id/blog/2021/02/01/cara-mencegah-cyber-crime

Manners-Bel, J., & Lyon, K. (2019). The logistics and supply chain innovation handbook : disruptive technologies and new business models (1st ed.). Kogan Page Limited. http://library.lol/main/B8AA75256B1FFE565FE9E5DC5BEED2D3

Maskun, S. H. (2014). Kejahatan Siber (Cyber Crime) Suatu Pengantar. Prenada Media.

Redaksi JNEWS. (2022, December 20). Bahaya RAT di Modus Penipuan Berkedok Paket. JNEWS Online. Retrieved March 14, 2023, from https://jnewsonline.com/bahaya-rat-di-modus-penipuan-berkedok-paket/

Paksoy, T., Koçhan, Ç., & Ali, S. S. (2021). Logistics 4.0: Digital Transformation of Supply Chain Management. Taylor & Francis Group, LLC. http://library.lol/main/C3AD4A686B200FEE74796AE141A5579C

Pearlson, K. E., & Saunders, C. S. (2016). Managing and Using Information Systems: A Strategic Approach (6th ed.). John Wiley & Sons, Inc. https://libgen.rocks/ads.php?md5=2264CEA57CF5E4D0346C493BB16E25F1

Rusmana, A. W., & Setyawan, I. (2021). Pengaruh Integrasi Supply Chain terhadap Kinerja Supply Chain. Jurnal Bisnis, Logistik Dan Supply Chain (BLOGCHAIN), 1(2), 67–76. https://ejournal-ibik57.ac.id/index.php/blogchain/article/view/329

Shen, X., Chen, H., Liu, H., & Chen, Z. (2021). The Impact Of Cybercrime On The Global Logistics Industry: An Empirical Study. International Journal of Production Economics, 231, 107904.

Siahaan, A. P. U. (2018). Pelanggaran cybercrime dan kekuatan yurisdiksi di Indonesia. Jurnal Teknik dan Informatika, 5(1), 6-9.

Stallings, W. &. (2018). Pearson Education. Computer Security: Principles and Practice, Inc.

Sturm, R., Pollard, C., & Craig, J. (2017). Application Performance Management (APM) in the Digital Enterprise : Managing Applications for Cloud, Mobile, IoT and eBusiness. Elsevier Inc. http://library.lol/main/D303C2D4F9FC015BEFDC3BA24461DFEA

Sutiono. (2016, October 13). 6 Cara Mencegah Cybercrime. DosenIT.com. Retrieved March 14, 2023, from https://dosenit.com/jaringan-komputer/security-jaringan/cara-mencegah-cybercrime

Vemuri, V. K. (2018). Blockchain: a practical guide to developing business, law, and technology solutions.

Wang, D., & Liang, D. (2020). Research on the Application of Blockchain Technology in Logistics Information Security. In Proceedings of the 1st International Conference on Management, Education, and Social Science (ICMESS 2020), (pp.352-356). Atlantis Press.