E-ISSN : 2988-1986
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 4 No 10 Tahun 2024

PERANAN IT SECURITY DALAM MENGAMANKAN INFRASTRUKTUR DAN TRANSAKSI DI PERUSAHAAN E-COMMERCE

Aryanto Nur[1*], Danang Abu Hafid[2]
[1]Fakultas Teknik Informatika, Universitas Binasarana Informatika
[2]Jurusan Sistem Informasi, Fakultas Teknik Informatika, Universitas Binasarana Informatika
aryantonur@gmail.com, danangabuhafid@gmail.com

Abstrak

Pertumbuhan yang cepat di bidang teknologi informasi dan komunikasi telah mengubah cara perusahaan beroperasi, terutama di sektor *e-commerce*. Perusahaan *e-commerce* kini dapat menawarkan layanan lebih cepat dan efisien kepada konsumen, namun peningkatan ketergantungan pada teknologi juga meningkatkan risiko terkait keamanan data dan transaksi digital. Dalam konteks ini, keamanan IT (*IT Security*) memainkan peran penting dalam menjaga infrastruktur teknologi informasi dan melindungi data sensitif yang dipertukarkan selama transaksi *online*. Ancaman seperti serangan *Distributed Denial of Service* (*DDoS*), pencurian identitas, *malware*, dan penipuan transaksi merupakan tantangan utama yang harus dihadapi oleh perusahaan *e-commerce*. Tanpa strategi keamanan yang kuat, perusahaan *e-commerce* dapat kehilangan kepercayaan pelanggan, mengalami kerugian finansial, dan merusak reputasi mereka di pasar. Penelitian ini bertujuan untuk mengeksplorasi berbagai teknologi keamanan yang dapat diterapkan oleh perusahaan *e-commerce*, seperti enkripsi data, *firewall*, dan sistem deteksi intrusi (IDS/IPS). Selain itu, penelitian ini juga menganalisis pentingnya kepatuhan terhadap regulasi keamanan data, seperti *Payment Card Industry Data Security Standard* (PCI DSS), yang dirancang untuk melindungi transaksi kartu kredit. Dengan menggunakan pendekatan studi literatur, hasil penelitian ini diharapkan dapat memberikan wawasan mendalam mengenai peran strategis *IT Security* dalam mengamankan infrastruktur *e-commerce* dan menjaga kepercayaan konsumen di era digital.

Kata Kunci: IT Security, *e-commerce*, keamanan transaksi, infrastruktur TI, serangan siber.

Article History
Received: Oktober 2024
Reviewed: Oktober 2024
Published: Oktober 2024

Plagirism Checker No 234
Prefix DOI :
10.8734/Kohesi.v1i2.365

Abstract

The rapid evolution of information and communication technology has transformed the way companies operate, particularly in the e-commerce sector. E-commerce companies can now offer services more quickly and efficiently to consumers; however, the increased reliance on technology also heightens the risks associated with data security and digital transactions. In this context, IT security plays a crucial role in safeguarding the information technology infrastructure and protecting sensitive data exchanged during online transactions. Threats such as Distributed Denial of Service (DDoS) attacks, identity theft, malware, and transaction fraud are primary challenges that e-commerce companies must face. Without a robust security strategy, e-commerce companies may lose customer trust, incur financial losses, and damage their reputation in the market. This study aims to explore various security technologies that can be implemented by e-commerce companies, such as data encryption, firewalls, and intrusion detection systems (IDS/IPS). Additionally, this research the relevance of compliance with data security regulations, such as. the Payment Card Industry Data Security Standard (PCI DSS), which is designed to protect credit card transactions. By utilizing a literature study approach, the findings of this research are expected to provide in-depth insights into the strategic role of IT security in securing e-commerce infrastructure and maintaining consumer trust in the digital age.

Keywords: *IT Security, e-commerce, transaction security, IT infrastructure, cyber attacks.*

PENDAHULUAN

Perkembangan pesat teknologi informasi telah menciptakan peluang baru dalam dunia bisnis, terutama di sektor *e-commerce*. *E-commerce* mempermudah transaksi secara digital dengan konsumen, namun seiring dengan kemudahan tersebut muncul tantangan besar dalam hal keamanan data dan transaksi. Di Indonesia, pertumbuhan *e-commerce* sangat pesat, namun demikian, risiko terhadap serangan siber dan pelanggaran data pribadi juga meningkat Seiring bertambahnya *volume* transaksi yang dilakukan secara digital.

Ancaman seperti *Distributed Denial of Service* (*DDoS*), *malware*, pencurian identitas, dan penipuan transaksi *online* adalah beberapa risiko utama yang dihadapi oleh perusahaan *e-commerce*. Keamanan data pelanggan dan transaksi yang aman menjadi prioritas utama bagi perusahaan-perusahaan ini. Oleh karena itu, implementasi *IT Security* menjadi sangat penting untuk melindungi infrastruktur teknologi dan memastikan transaksi berjalan dengan aman.

Dalam konteks ini, perusahaan *e-commerce* harus memastikan bahwa sistem mereka memiliki tingkat keamanan yang tinggi melalui penerapan berbagai teknologi keamanan, seperti enkripsi, *firewall*, serta sistem deteksi dan pencegahan intrusi (IDS/IPS). Selain itu, kepatuhan terhadap standar keamanan seperti PCI DSS juga merupakan hal yang krusial untuk menjaga integritas data dan kepercayaan pelanggan.
Penelitian ini bertujuan untuk mengeksplorasi peranan *IT Security* dalam melindungi infrastruktur dan transaksi di perusahaan *e-commerce*, serta memberikan analisis terkait teknologi yang digunakan dan strategi mitigasi risiko yang dapat diterapkan.

TINJAUAN PUSTAKA

IT Security dalam E-Commerce

IT Security atau keamanan informasi teknologi merujuk pada berbagai langkah dan kebijakan yang diambil untuk melindungi sistem informasi dari ancaman yang dapat mengganggu atau mencuri data. Dalam *e-commerce*, keamanan IT sangat penting karena data yang dipertukarkan mencakup informasi sensitif, seperti data pribadi pengguna, informasi kartu kredit, dan detail transaksi lainnya. Penerapan strategi keamanan IT yang kuat sangat dibutuhkan untuk menjaga kerahasiaan, integritas, dan ketersediaan data, yang dikenal sebagai prinsip *CIA (Confidentiality, Integrity, and Availability).* Studi menunjukkan bahwa perusahaan *e-commerce* lebih rentan terhadap serangan siber karena sifat digital dari seluruh operasi mereka. Serangan siber sering kali memanfaatkan kelemahan dalam sistem keamanan untuk mencuri data atau merusak layanan.

Ancaman Siber dalam E-Commerce

Perusahaan *e-commerce* menghadapi berbagai ancaman siber, termasuk *Distributed Denial of Service* (DDoS), *malware*, dan . Agresi *DDoS* bertujuan untuk membanjiri lalu lintas jaringan, sehingga membuat layanan tidak dapat diakses oleh pengguna yang sah. *Malware* digunakan untuk mencuri informasi atau merusak sistem, sedangkan *phishing* dilakukan untuk menipu pengguna agar memberikan informasi sensitif. Ancaman ini meningkat selama pandemi COVID-19, seiring dengan peningkatan aktivitas digital dan transaksi online. Untuk melindungi diri dari ancaman tersebut, perusahaan harus mengadopsi teknologi keamanan yang canggih, seperti *firewall*, enkripsi, dan sistem deteksi intrusi (IDS/IPS).

Teknologi Keamanan di E-Commerce

Berbagai teknologi keamanan dapat diterapkan oleh perusahaan *e-commerce* untuk melindungi data dan transaksi mereka. Enkripsi data merupakan salah satu metode terbaik untuk melindungi informasi sensitif, seperti detail kartu kredit, selama proses transaksi. Selain itu, *firewall* sangat penting untuk melindungi jaringan perusahaan dari akses yang tidak sah, sedangkan sistem deteksi intrusi (IDS/IPS) membantu memantau aktivitas jaringan dan mendeteksi serangan yang mencurigakan. Perusahaan yang menggunakan pendekatan keamanan berlapis memiliki tingkat perlindungan yang lebih baik terhadap serangan siber.

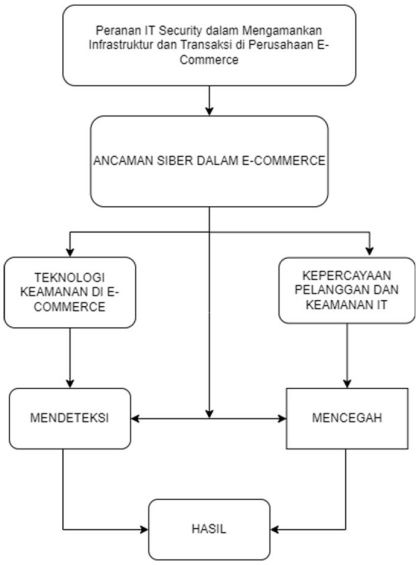
Regulasi Keamanan Data: PCI DSS

Dalam dunia *e-commerce*, regulasi keamanan data memainkan peran penting dalam menjaga keamanan transaksi *online*. Salah satu standar keamanan global yang diterapkan adalah Protokol PCI DSS. PCI DSS dirancang untuk melindungi informasi kartu kredit dan transaksi digital. Regulasi ini mencakup pedoman yang ketat untuk melindungi data, seperti penggunaan *firewall*, enkripsi data, dan kontrol akses. Meskipun banyak perusahaan besar yang mematuhi standar ini, perusahaan kecil sering kali menghadapi tantangan dalam implementasi karena keterbatasan sumber daya.

Kepercayaan Pelanggan dan Keamanan IT

Keamanan IT tidak hanya berfungsi untuk melindungi data perusahaan, tetapi juga untuk menjaga kepercayaan pelanggan. Pelanggan yang mengetahui bahwa platform *e-commerce* memiliki kebijakan keamanan yang kuat lebih cenderung melakukan transaksi dan mempercayakan data pribadi mereka. Transparansi dalam kebijakan privasi dan komunikasi yang jelas mengenai langkah-langkah keamanan yang diambil oleh perusahaan sangat penting untuk membangun hubungan yang kuat dengan pelanggan. Oleh karena itu, perusahaan harus secara aktif mengkomunikasikan langkah-langkah keamanan yang mereka terapkan

Dasar Pemikiran



Gambar 1 Dasar Pemikiran

METODE PENELITIAN

Penelitian ini menerapkan metode berbasis kuantitatif dengan pendekatan pengumpulan data melalui tinjauan literatur. Fokus dari penelitian ini adalah data sekunder yang berfokus pada keamanan teknologi informasi (*IT Security*) dalam melindungi infrastruktur dan transaksi *e-commerce* dari ancaman siber seperti , *malware*, dan *DDoS*. Metode penelitian kualitatif ini berbasis pada prinsip-prinsip filsafat *postpositivisme*, yang bertujuan untuk menganalisis keadaan objek secara natural, di mana peneliti berperan selaku instrumen utama. Proses pengumpulan data dijalankan dengan metode triangulasi, yaitu dengan memadukan berbagai

sumber informasi. Data yang dikumpulkan kemudian dianalisis secara induktif dengan penekanan pada makna yang lebih dalam dibandingkan sekadar generalisasi (Sugiyono, 2020).

Studi literatur yang dianalisis berfokus pada pemahaman dan interpretasi penulis mengenai peran *IT Security* dalam melindungi data pengguna dan transaksi *online* di *e-commerce* Studi kualitatif ini menerapkan metode analisis konten guna mengidentifikasi dan memahami realitas yang berlangsung dalam konteks ancaman siber *di e-commerce*. Analisis ini bersifat mendalam dan komprehensif, dengan tujuan untuk memahami berbagai aspek yang berkaitan dengan pengamanan data di platform *e-commerce* (Harnovinsah, 2019).

Teknik pengumpulan data dilakukan melalui dokumentasi dari sumber data sekunder, termasuk buku, artikel jurnal, laporan penelitian, dan referensi daring lainnya. Semua data ini dianalisis secara kualitatif dengan menggunakan *content analysis* untuk menggambarkan secara terperinci pendahuluan, ciri-ciri, dan karakteristik dari berbagai isu ancaman siber dimana telah dialami. Pendekatan Tujuannya adalah untuk memberikan wawasan yang lebih mendalam tentang isu tersebut. strategi *IT Security* yang diterapkan di perusahaan *e-commerce*, yang dapat dijadikan acuan dalam pengembangan solusi keamanan di masa mendatang.

HASIL DAN PEMBAHASAN

Perkembangan teknologi informasi telah mengubah cara pandang tentang batas wilayah, waktu, nilai-nilai, serta cara kerja menjadi lebih digital. Transformasi ini juga memengaruhi bentuk dan metode kejahatan berbasis teknologi, termasuk ancaman siber yang semakin sulit untuk diantisipasi oleh sistem hukum. Teknologi yang semakin maju menciptakan kejahatan berbasis teknologi informasi yang lebih kompleks, seperti kejahatan siber dalam *e-commerce*, yang menggunakan metode seperti *phishing*, *malware*, DDoS, dan *hacking* untuk menyerang sistem perusahaan. Dalam konteks hukum, perlindungan hukum berfungsi untuk melindungi kepentingan individu dan perusahaan, termasuk di sektor *e-commerce*.

Perlindungan hukum ini menjadi sangat penting dalam menghadapi tantangan keamanan informasi yang terus berkembang, khususnya dalam melindungi data pelanggan dan infrastruktur teknologi perusahaan dari ancaman-ancaman siber yang semakin canggih. Untuk memastikan kelangsungan bisnis dan keamanan data pelanggan, keamanan IT (*IT Security*) harus diterapkan secara menyeluruh di platform *e-commerce*.

Kejahatan siber dalam *e-commerce* sering kali melibatkan pelanggaran terhadap undang-undang yang mengatur tentang perlindungan data dan privasi, seperti Undang-undang Perlindungan Data Pribadi di beberapa negara, serta standar internasional seperti PCI DSS dan GDPR. Kejahatan-kejahatan ini termasuk penggunaan metode seperti skimming, *hacking*, dan *malware*, yang bertujuan untuk mencuri informasi sensitif atau mengganggu operasi bisnis secara digital.

Oleh karena itu, perusahaan *e-commerce* harus mematuhi regulasi keamanan dan menerapkan teknologi keamanan yang canggih untuk melindungi diri dari kejahatan tersebut. Kejahatan di dunia siber, seperti yang disebutkan oleh Sutherland dalam teori kejahatan kerah putih, kini lebih sering dilakukan oleh pelaku berstatus sosial tinggi dengan akses ke teknologi dan informasi perusahaan.

Dalam konteks *e-commerce*, kejahatan ini sering kali melibatkan teknik-teknik yang menggunakan *skimming* atau *phishing* untuk mencuri informasi pribadi pelanggan atau merusak infrastruktur teknologi. Perusahaan yang tidak menerapkan langkah-langkah keamanan yang ketat akan lebih rentan terhadap kejahatan seperti ini. Kejahatan siber yang dihadapi oleh perusahaan *e-commerce* mirip dengan kejahatan perbankan yang menggunakan *skimming*, *malware*, dan *hacking* untuk mengeksploitasi kelemahan dalam sistem digital. Sebagaimana dijelaskan oleh Yulianti (2020), kejahatan ini termasuk dalam kategori kejahatan ekonomi, yang bertujuan untuk mendapatkan keuntungan finansial melalui cara ilegal, dengan modus seperti pencurian data atau pengelabuan.

Sebagai kesimpulan, perusahaan *e-commerce* perlu meningkatkan peran *IT Security* dalam melindungi infrastruktur teknologi informasi dari serangan siber yang semakin kompleks. Hal ini mencakup penerapan teknologi seperti enkripsi, *firewall*, sistem deteksi intrusi, dan kepatuhan terhadap regulasi keamanan internasional. Perlindungan hukum dan keamanan teknologi yang solid sangat penting untuk menjaga kepercayaan pelanggan dan kelangsungan bisnis di era digital ini.

Kasus Kejahatan E-Commerce

1. *Phising*

Phishing adalah metode penipuan siber yang dilakukan dengan cara mengelabui korban untuk memberikan informasi pribadi atau finansial melalui *email*, pesan teks, atau situs *web* palsu yang tampak seperti asli. Kejahatan semakin marak terjadi di sektor *e-commerce* seiring meningkatnya transaksi digital. Penipu biasanya menargetkan pelanggan dengan mengirimkan pesan yang terlihat berasal dari perusahaan *e-commerce*, bank, atau platform pembayaran, mengarahkan mereka untuk mengungkapkan informasi *login* atau detail kartu kredit mereka. Beberapa kasus penipuan *phishing* yang terjadi di sektor *e-commerce* di Indonesia:

a. Kasus Tokopedia, Mei 2020 Dalam insiden besar ini, data sekitar 91 juta akun pengguna Tokopedia bocor. Para pelaku kejahatan menggunakan teknik *phishing* untuk menipu pengguna agar memberikan informasi *login* mereka, yang kemudian digunakan untuk mengakses data pribadi mereka dan bahkan melakukan pembelian ilegal menggunakan akun yang terhubung ke kartu kredit atau dompet digital.
b. Kasus Shopee, Februari 2021 Beberapa pengguna Shopee melaporkan kehilangan saldo di dompet digital mereka setelah menerima *email* palsu yang meminta mereka memperbarui informasi akun. *Email* tersebut dirancang menyerupai komunikasi resmi dari Shopee, dan pengguna yang tidak berhati-hati secara tidak sadar memberikan kredensial mereka kepada pelaku.
c. Kasus Bukalapak, April 2019 Bukalapak juga menjadi sasaran kejahatan *phishing*, di mana penipu mengirimkan pesan teks dan *email* yang berisi tautan palsu untuk "memverifikasi akun". Ketika pengguna melakukan klik tautan tersebut, mereka diarahkan ke halaman *login* palsu yang menyebabkan pencurian data akun. Metode yang

Digunakan dalam *Phishing* di *E-Commerce* Penipuan *phishing* biasanya mengikuti pola yang sistematis:

a. Mengirimkan *Email* atau Pesan Palsu: Pelaku mengirimkan *email* atau pesan teks yang terlihat seperti berasal dari perusahaan *e-commerce*, dengan informasi yang mendesak seperti "Perbarui akun Anda sekarang" atau "Ada aktivitas mencurigakan pada akun Anda".
b. Menyisipkan Tautan ke Situs Web Palsu: *Email* atau pesan tersebut berisi tautan ke situs *web* palsu yang menyerupai halaman *login* resmi dari *e-commerce*. Ketika korban memasukkan kredensial, data mereka dicuri.
c. Menggunakan Informasi yang Dicuri: Setelah memperoleh informasi *login*, pelaku dapat mengakses akun pengguna, melakukan pembelian ilegal, atau menjual informasi pribadi korban di pasar gelap. Perlindungan Hukum dan Tindakan Pencegahan di Indonesia Pelanggaran keamanan yang disebabkan oleh *phishing* di *e-commerce* diatur oleh berbagai undang-undang di Indonesia, termasuk:
    a. Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur kejahatan siber, termasuk penipuan *phishing*.
    b. Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, yang memastikan bahwa perusahaan *e-commerce* bertanggung jawab melindungi data dan transaksi pengguna mereka.

Untuk menangani kejadian *phishing*, perusahaan *e-commerce* harus meningkatkan keamanan IT mereka melalui metode seperti *Multi-Factor Authentication* (MFA) dan enkripsi SSL/TLS untuk mencegah akses tidak sah. Selain itu, perusahaan juga diwajibkan untuk mematuhi regulasi keamanan, seperti PCI DSS untuk menjaga keamanan data transaksi pembayaran. Konsumen juga diharapkan untuk melaporkan insiden ke pihak bank atau *e-commerce* yang bersangkutan agar tindakan segera dapat diambil, sesuai dengan Peraturan Bank Indonesia mengenai perlindungan konsumen jasa sistem pembayaran. Langkah Pengaduan Pengguna-pengguna yang menjadi korban *phishing* dapat mengajukan pengaduan kepada penyedia layanan *e-commerce* atau bank mereka melalui pusat layanan pelanggan, *call cent*er, atau secara langsung. Penyedia layanan diwajibkan untuk menyelesaikan pengaduan tersebut sesuai dengan Peraturan Bank Indonesia Nomor 22 Tahun 2020 tentang Perlindungan Konsumen. Kasus Terkait Seperti yang dilaporkan oleh berbagai sumber, serangan *phishing* menjadi semakin marak di Indonesia seiring dengan meningkatnya transaksi digital. Misalnya, kasus kebocoran data di Tokopedia dan Bukalapak menekankan pentingnya kesadaran pengguna dan penerapan sistem keamanan yang lebih ketat untuk memerangi serangan *phishing* di *e-commerce*.

Jenis-Jenis *Phising* di *E-Commerce*

a. *Email Phishing* untuk *E-Commerce*

    Penyerang mengirim *email* yang tampak seperti berasal dari toko online yang dikenal, menawarkan diskon atau promosi yang sangat menarik. *Email* ini sering kali berisi tautan yang mengarah ke situs palsu untuk mencuri informasi akun atau pembayaran.

b. Fake Order Confirmation

Penyerang mengirimkan *email* palsu yang mengonfirmasi pesanan yang tidak pernah dibuat. *Email* tersebut sering kali menyertakan tautan untuk mengecek status pesanan, yang mengarahkan korban ke situs *phishing*.

c. Spoofing Toko Online

Penyerang membuat situs *web* yang menyerupai situs *e-commerce* yang sah. Mereka dapat menawarkan produk dengan harga yang sangat rendah untuk menarik pelanggan. Ketika korban melakukan pembelian, informasi kartu kredit dan data pribadi mereka dicuri.

d. *Phishing* Melalui Media Sosial

Penyerang dapat menggunakan platform media sosial untuk menghubungi korban, sering kali dengan mengklaim sebagai layanan pelanggan dari toko online. Mereka bisa meminta informasi akun atau menawarkan promosi yang mengharuskan pengguna untuk mengklik tautan berbahaya.

e. SMS Phishing (Smishing)

Penyerang mengirimkan pesan teks yang mengklaim ada masalah dengan pesanan atau menawarkan diskon khusus. Pesan tersebut mengandung tautan yang mengarahkan korban ke situs palsu yang meminta informasi pribadi atau pembayaran.

f. Checkout Phishing

Pada tahap akhir pembelian, penyerang dapat mengarahkan pengguna ke halaman palsu untuk menyelesaikan pembayaran. Halaman ini dirancang untuk mencuri informasi kartu kredit atau detail akun pembayaran lainnya.

g. *Phishing* Melalui Aplikasi *E-Commerce* Palsu

Penyerang dapat membuat aplikasi palsu yang menyerupai aplikasi *e-commerce* populer. Ketika pengguna mengunduh dan masuk, informasi *login* dan data pribadi mereka dapat dicuri.

h. *Phishing* dengan Tawaran Palsu

Penyerang dapat mengirimkan *email* atau pesan yang menawarkan produk dengan harga tidak realistis, seperti barang elektronik terbaru. Saat pengguna mencoba membeli, mereka diarahkan ke situs .

i. Phishing Melalui Komentar atau Ulasan

Di beberapa platform e-commerce, penyerang dapat meninggalkan komentar atau ulasan yang berisi tautan ke situs phishing, mengarahkan pengguna untuk mengunjungi halaman palsu.

j. Business Email *Compromise (BEC) di E-Commerce*

Penyerang menyamar sebagai manajer atau eksekutif dalam perusahaan *e-commerce,* meminta karyawan untuk melakukan transfer dana atau mengungkapkan informasi sensitif dengan berpura-pura membutuhkan informasi tersebut.

Cara menanggulangi *Phising* dalam *E-Commerce*

a. Authentikasi Multifaktor (MFA)

Salah satu cara paling efisien untuk menanggulangi dengan cara mengimplementasikan *Multi-Factor Authentication* (MFA). MFA memastikan bahwa pengguna tidak hanya memerlukan kata sandi untuk mengakses akun mereka, tetapi juga faktor verifikasi tambahan, seperti kode yang dikirimkan ke ponsel atau otentikasi biometrik. Ini sangat membatasi kemampuan peretas untuk mengakses akun bahkan jika mereka berhasil mencuri kata sandi.

b. Edukasi Pengguna

1) Pengguna harus diberi edukasi tentang cara mengenali *email* atau pesan yang mencurigakan. Edukasi ini dapat mencakup:
2) Tidak mengklik tautan dalam *email* yang meminta informasi sensitif.
3) Mengecek URL situs yang dikunjungi untuk memastikan domain resmi digunakan.
4) Melaporkan *email* atau pesan mencurigakan kepada platform *e-commerce*.

c. Pemantauan *Email* dan Pemfilteran

E-commerce harus menggunakan sistem pemantauan *email* yang canggih untuk mendeteksi dan memblokir *email phishing* sebelum mencapai kotak masuk pengguna. Pemfilteran *email* berbasis AI juga dapat digunakan untuk mengenali pola *phishing* dan mengirimkan *email* berbahaya langsung ke folder *spam*.

d. Sertifikat SSL/TLS dan Enkripsi

Platform *e-commerce* harus memastikan bahwa semua komunikasi dengan pengguna, terutama yang terkait dengan transaksi, dienkripsi menggunakan protokol SSL/TLS. Dengan demikian, data yang dikirimkan antara pengguna dan platform terlindungi dari pihak ketiga yang berusaha untuk mengintip atau mencuri data tersebut.

e. Domain-*Based Message Authentication Reporting and Conformance* (DMARC)

DMARC adalah mekanisme yang memungkinkan pengirim *email* memverifikasi bahwa pesan tersebut benar-benar berasal dari domain yang sah. Penerapan DMARC, DKIM, dan SPF oleh perusahaan *e-commerce* dapat membantu mencegah *email phishing* dengan mengurangi peluang pesan palsu mencapai pengguna.

f. *Browser Warning System*s

Banyak *browser* modern sekarang memiliki sistem peringatan yang memblokir akses ke situs *web phishing*. Platform *e-commerce* dapat memastikan bahwa situs mereka terdaftar sebagai aman, dan juga mengedukasi pengguna tentang bahaya situs *web* yang tidak aman.

g. Upaya Pencegahan Tambahan

1) Verifikasi Dua Langkah di Platform

E-commerce harus memastikan semua penggunanya mengaktifkan verifikasi dua langkah, terutama saat melakukan transaksi sensitif seperti perubahan kata sandi atau detail pembayaran.

2) Notifikasi Aktivitas yang Mencurigakan:

Platform *e-commerce* dapat memberitahu pengguna jika ada aktivitas mencurigakan di akun mereka, seperti *login* dari lokasi atau perangkat yang tidak dikenal.

Phishing terus menjadi ancaman besar bagi perusahaan *e-commerce* karena teknik manipulatifnya yang memanfaatkan ketidakwaspadaan pengguna. Menggunakan pendekatan keamanan berlapis, seperti MFA, enkripsi, dan pemantauan *email* canggih, dapat secara efektif mengurangi risiko dan menjaga data pelanggan tetap aman.

2. *Malware*

Malware adalah salah satu ancaman siber paling berbahaya yang menargetkan perusahaan *e-commerce*. *Malware* adalah perangkat lunak berbahaya yang didesain untuk menyusup ke sistem komputer dan menyebabkan kerusakan, mencuri data, atau bahkan memata-matai aktivitas pengguna. *Malware* dapat masuk ke dalam sistem *e-commerce* melalui berbagai cara, termasuk *phishing emails*, download aplikasi berbahaya, atau penggunaan perangkat lunak yang tidak terlindungi. Dampaknya sangat merusak karena *malware* dapat mencuri data pelanggan, termasuk informasi kartu kredit, serta merusak infrastruktur teknologi.
Jenis-Jenis *Malware* yang umum dalam *E-Commerce*

a. *Ransomware*

Ransomware adalah jenis *malware* yang mengunci atau mengenkripsi data korban, kemudian meminta tebusan untuk mengembalikan akses ke data tersebut. *Ransomware* sangat berbahaya bagi *e-commerce* karena dapat menyebabkan downtime yang lama dan memaksa perusahaan untuk membayar sejumlah besar uang untuk mengembalikan sistem mereka.

Contoh serangan ransomware yang sangat merusak adalah serangan LockBit 3.0 yang menargetkan Bank Syariah Indonesia (BSI) pada Mei 2023. Serangan ini menyebabkan gangguan besar pada layanan bank, dengan kebocoran data sebesar 1,5 terabita yang mencakup informasi pribadi lebih dari 15 juta pelanggan. Data ini termasuk nama, alamat, nomor telepon, nomor kartu, dan informasi transaksi. Serangan tersebut menyoroti kelemahan dalam sistem keamanan BSI, terutama karena bank hasil merger sering kali memiliki infrastruktur IT yang masih belum stabil.

b. *Spyware*

Spyware adalah jenis *malware* yang dirancang untuk memata-matai aktivitas pengguna tanpa sepengetahuan mereka. Dalam *e-commerce*, spyware dapat digunakan untuk mencuri informasi *login* atau melacak aktivitas belanja online pengguna, termasuk informasi kartu kredit. Misalnya, sebuah situs *e-commerce* yang tidak terlindungi dengan baik dapat dengan mudah menjadi target spyware yang mengumpulkan data *login* pengguna dan mengirimkan informasi tersebut kepada peretas.

c. Trojans (Trojan Horse)

Trojans adalah jenis *malware* yang sering menyamar sebagai perangkat lunak atau aplikasi yang sah, tetapi sebenarnya dirancang untuk merusak sistem atau mencuri informasi. Dalam *e-commerce*, *trojan* sering digunakan untuk mencuri informasi *login* atau melakukan transaksi yang tidak sah. *Trojans* sering kali disisipkan dalam aplikasi pihak ketiga yang tidak aman. Pengguna yang mengunduh aplikasi berbahaya dari sumber yang tidak tepercaya bisa tanpa sadar menginstal *trojan*, yang kemudian dapat mencuri data sensitif atau bahkan mengendalikan perangkat pengguna.

d. Adware

Adware adalah jenis *malware* yang menampilkan iklan berlebihan di layar pengguna. Selain mengganggu pengalaman pengguna, adware sering kali disertai dengan kemampuan untuk melacak aktivitas online pengguna, termasuk data belanja dan transaksi di platform *e-commerce*. Data ini bisa dijual ke pihak ketiga atau digunakan untuk kegiatan penipuan. Adware biasanya muncul setelah pengguna tanpa sadar menginstal perangkat lunak yang disertai dengan iklan berbahaya. Di platform *e-commerce*, adware dapat mengarahkan pengguna ke situs *phishing* yang menyerupai halaman *checkout* asli.

Bagaimana *Malware* Menyebar di *E-Commerce :*

a. *Phishing Email*s dan Attachments

*Phishing email*s adalah salah satu metode penyebaran *malware* yang paling umum. *Email* yang tampak sah dikirim ke pengguna, sering kali mengaku berasal dari perusahaan *e-commerce* terkenal atau bahkan dari bank. Ketika pengguna membuka lampiran berbahaya atau mengklik tautan di dalam *email*, *malware* diinstal di perangkat mereka.

Pada serangan *malware* yang menargetkan Bank Syariah Indonesia, serangan tersebut dipicu oleh aktivitas *phishing*, di mana peretas menggunakan *email* berbahaya yang menyamar sebagai *email* resmi untuk memasukkan *malware* ke dalam sistem bank.

b. *Download* Software atau Aplikasi Berbahaya

Pengguna sering kali tanpa sadar mengunduh *malware* saat mereka menginstal perangkat lunak atau aplikasi dari sumber yang tidak tepercaya. Dalam dunia *e-commerce*, *malware* ini bisa mencuri data *login* pengguna atau bahkan menargetkan *server* perusahaan.

Aplikasi yang tidak sah, terutama yang diunduh dari situs pihak ketiga, adalah sumber umum *trojan* yang bisa mencuri data atau menyebarkan *malware* lebih lanjut.

c. Serangan Pengunduhan *Drive-By*

Drive-by download berlangsung ketika pengguna mengunjungi situs *web* yang tidak aman atau terinfeksi, dan *malware* otomatis diunduh ke perangkat mereka tanpa memerlukan interaksi pengguna. Situs *web e-commerce* yang rentan dapat menjadi korban serangan ini, di mana pengunjung tanpa sadar mengunduh *malware* hanya dengan membuka halaman. Banyak peretas menggunakan serangan ini dengan memanfaatkan iklan berbahaya atau situs yang telah disusupi untuk menyebarkan *malware* kepada pengunjung.

Kasus *Malware* di *E-Commerce* Pada tahun 2023, Bank Syariah Indonesia (BSI) terkena serangan *malware* yang menyebabkan layanan mereka lumpuh selama beberapa hari. *Malware* ini tidak hanya mengganggu operasional bank, tetapi juga mengakibatkan kebocoran data sebesar 1,5 terabita, termasuk data pribadi lebih dari 15 juta pelanggan. Kasus ini menunjukkan bagaimana *malware* dapat melumpuhkan perusahaan besar yang seharusnya memiliki sistem keamanan yang baik. Kasus lainnya adalah serangan *malware* terhadap Target, salah satu ritel besar di Amerika Serikat. Pada tahun 2013, Target menjadi korban *malware* yang menyerang sistem pembayaran mereka, menyebabkan pencurian informasi kartu kredit lebih dari 40 juta pelanggan. *Malware* berhasil menyusup ke dalam jaringan perusahaan melalui *email phishing* yang menjangkau *vendor* mereka, lalu menyebar ke sistem pembayaran.

Di sektor *e-commerce*, *malware* sering menyusup melalui *email* berbahaya atau aplikasi yang tidak terlindungi. *Malware* ini bisa mengambil kendali atas sistem perusahaan, mencuri data pelanggan, atau merusak operasional bisnis. Dengan semakin banyaknya pengguna yang melakukan transaksi online, risiko serangan *malware* semakin tinggi, terutama bagi perusahaan yang tidak menerapkan sistem keamanan yang memadai. Cara kerja *malware* di platform *e-commerce* meliputi penyusupan melalui tautan *phishing*, lampiran *email* berbahaya, atau aplikasi tidak terpercaya. Setelah sistem terinfeksi, *malware* dapat memengaruhi performa platform dengan berbagai cara:

a. Penurunan performa secara tiba-tiba karena *malware* mengonsumsi sumber daya sistem.
b. Kegagalan sistem yang sering terjadi karena penggunaan CPU atau RAM yang tinggi akibat *malware*.
c. Penghapusan atau kerusakan data pelanggan, menyebabkan perusahaan kehilangan informasi penting.
d. Iklan *pop-up* yang muncul secara terus-menerus atau pengalihan browser ke situs *web* yang tidak diinginkan.

Untuk mencegah hal ini, perusahaan *e-commerce* harus memastikan sistem mereka diperbarui secara berkala, menggunakan antivirus dan *firewall* yang kuat, serta melakukan pemindaian rutin untuk mendeteksi *malware*.

Cara Menanggulangi *Malware* dalam *E-Commerce*

a. Penerapan Perangkat Lunak Antivirus dan Anti-*Malware*

   Perusahaan *e-commerce* harus memasang perangkat lunak antivirus dan anti-*malware* yang dapat mendeteksi dan mencegah perangkat lunak berbahaya. Sistem antivirus dapat secara otomatis melakukan pemindaian terhadap *file* yang masuk dan memblokir *malware* sebelum merusak sistem.

b. Pembaruan Perangkat Lunak Berkala

   Banyak serangan *malware* terjadi karena kelemahan atau celah di dalam perangkat lunak yang sudah lama tidak diperbarui. Pembaruan perangkat lunak berkala (patching) sangat penting untuk menutup celah keamanan yang dapat dieksploitasi oleh *malware*. Perusahaan *e-commerce* harus memastikan bahwa perangkat lunak mereka selalu mutakhir.

c. Enkripsi Data

   Untuk mencegah *malware* mencuri data sensitif, seperti informasi kartu kredit dan *login* pelanggan, *e-commerce* harus menggunakan enkripsi data. Data yang dienkripsi akan sulit diakses oleh peretas meskipun mereka berhasil menyusup ke dalam sistem.

d. Pemantauan Jaringan dan Sistem Deteksi Intrusi (IDS/IPS)

   Pemantauan jaringan secara real-time adalah salah satu langkah kunci untuk mendeteksi adanya aktivitas mencurigakan yang bisa mengindikasikan infeksi *malware*. Sistem Deteksi dan Pencegahan Intrusi (IDS/IPS) berfungsi untuk memantau lalu lintas jaringan dan mendeteksi pola serangan *malware* yang mencoba menyusup.

e. Isolasi Sistem yang Terinfeksi

Jika *malware* berhasil masuk ke dalam sistem, langkah cepat yang harus diambil adalah mengisolasi perangkat yang terinfeksi dari jaringan utama. Ini dapat mencegah penyebaran *malware* lebih lanjut ke seluruh jaringan dan meminimalisir kerusakan.

f. Edukasi Pengguna dan Karyawan

Karyawan dan pengguna perlu diedukasi tentang bahaya *malware* dan cara-cara mencegahnya. Sebagian besar *malware* disebarkan melalui *phishing* atau tautan berbahaya, sehingga kesadaran pengguna sangat penting. Pengguna dan karyawan harus diberi tahu untuk tidak mengklik tautan yang mencurigakan atau mendownload *file* dari sumber yang tidak tepercaya.

g. Upaya Pencegahan Tambahan

1) Backup Data Secara Rutin: Melakukan backup data secara berkala memastikan bahwa perusahaan dapat memulihkan data mereka dengan cepat jika terjadi serangan *malware*.
2) Penggunaan *Firewall* dan *Gateway* Keamanan: *Firewall* harus digunakan untuk memblokir akses berbahaya ke jaringan perusahaan. Next-Generation *Firewall* (NGFW) lebih efektif karena dapat memfilter lalu lintas berdasarkan konten, bukan hanya alamat IP.

Malware merupakan ancaman yang sangat serius bagi perusahaan *e-commerce*. Dengan serangan yang canggih dan terus berkembang, perusahaan harus mengadopsi pendekatan keamanan yang menyeluruh, mulai dari pemantauan jaringan hingga edukasi karyawan. Implementasi teknologi keamanan yang mutakhir, seperti antivirus, *firewall*, dan enkripsi data, sangat penting untuk melindungi sistem *e-commerce* dari *malware*.

3. DDOS

Distributed Denial of Service (DDoS) adalah salah satu jenis serangan siber yang bertujuan untuk membuat layanan atau situs Halaman *web* tidak dapat diakses oleh pengguna yang sah. Penyerangan ini bekerja dengan cara mengirimkan sejumlah besar permintaan ke *server*, jaringan, atau sistem tertentu secara bersamaan dari berbagai sumber, sehingga menyebabkan kelebihan beban pada sistem tersebut. Hal ini dapat mengganggu operasional bisnis, terutama untuk platform *e-commerce* yang sangat bergantung pada ketersediaan layanan secara online.

Bagaimana DDoS Bekerja? DDoS menggunakan jaringan komputer yang terinfeksi *malware*, yang dikenal sebagai botnet, untuk menyerang target. Botnet ini terdiri dari ribuan hingga jutaan perangkat, seperti komputer, *server*, atau bahkan perangkat IoT (Internet of Things), yang dikendalikan oleh penyerang tanpa sepengetahuan pemiliknya. Ketika serangan dimulai, setiap perangkat dalam botnet mengirimkan permintaan ke *server* atau situs *web* yang menjadi target. Akibatnya, *server* kelebihan beban dan menjadi tidak responsif, membuat layanan tidak tersedia bagi pengguna yang sah.

Ada tiga jenis serang DDoS utama:

a. Volumetric Attacks

Serangan ini menggunakan bandwidth yang besar untuk membanjiri jaringan dengan lalu lintas berlebih, seperti menggunakan protokol ICMP (*ping*) atau UDP (*User Datagram Protocol*) untuk membuat *server* tidak dapat menangani permintaan.

b. Application Layer Attacks

Serangan ini menargetkan aplikasi tertentu, seperti situs *web* atau layanan online, dengan menggunakan permintaan HTTP yang sah secara berlebihan, sehingga *server* aplikasi tidak dapat memproses permintaan lainnya.

c. Protocol Attacks

Menargetkan lapisan protokol dalam jaringan, seperti *SYN Floods* atau serangan *Ping of Death*, yang memanfaatkan kelemahan dalam protokol komunikasi untuk melumpuhkan sistem.

Dampak Serangan DDoS pada *E-Commerce* Di sektor *e-commerce*, serangan DDoS dapat menimbulkan kerugian yang sangat besar. Ketika sebuah situs *e-commerce* tidak dapat diakses, pelanggan tidak bisa melakukan transaksi, yang mengakibatkan:

a. Kehilangan pendapatan: Terutama jika serangan terjadi selama masa penjualan besar atau promosi khusus.
b. Penurunan kepercayaan pelanggan: Jika pelanggan mengalami kesulitan dalam mengakses situs *e-commerce*, mereka mungkin mencari alternatif lain, sehingga menurunkan kepercayaan mereka terhadap platform.
c. Kerugian reputasi: Serangan *DDoS* yang berhasil dapat merusak citra perusahaan di mata publik dan investor, terutama jika serangan ini menyebabkan *downtime* yang signifikan.
d. Kerugian operasional: Biaya pemulihan dari serangan *DDoS* bisa sangat tinggi, termasuk biaya perbaikan sistem dan perangkat keras yang terpengaruh.

Kasus Serangan DDoS :

Serangan Dyn (2016): Dyn, sebuah penyedia layanan DNS yang digunakan oleh platform besar seperti Amazon, Netflix, dan Twitter, mengalami serangan DDoS yang masif. Serangan ini dilakukan oleh botnet Mirai yang memanfaatkan perangkat IoT yang terinfeksi *malware*. Akibat serangan ini, banyak situs besar menjadi tidak dapat diakses selama beberapa jam, yang menyebabkan kerugian finansial dan reputasi.

Kasus GitHub (2018): GitHub, sebuah platform hosting kode sumber, menjadi target serangan DDoS terbesar pada tahun 2018. Serangan ini mencapai lalu lintas sebesar 1.35 Tbps (terabyte per detik), membuat GitHub tidak dapat diakses selama beberapa waktu. Serangan tersebut berhasil dihentikan dengan menggunakan layanan mitigasi DDoS yang kuat.

Cara Mencegah dan Mengatasi Serangan DDoS

a. Penggunaan Content Delivery *Network*s (CDN)

CDN mendistribusikan konten di berbagai *server* yang terletak di berbagai lokasi geografis. Dengan menyebarkan lalu lintas jaringan ke berbagai titik, CDN membantu mengurangi beban pada *server* utama saat terjadi serangan DDoS, sehingga situs tetap dapat diakses oleh pengguna.

b. Penerapan Web Application *Firewall* (WAF)

WAF digunakan untuk melindungi situs *e-commerce* dari serangan DDoS pada tingkat aplikasi. WAF dapat menganalisis permintaan yang datang dan memblokir lalu lintas yang mencurigakan sebelum mencapai *server* utama.

c. Solusi Anti-DDoS Khusus

Banyak perusahaan *e-commerce* menggunakan layanan anti-DDoS khusus, seperti Cloudflare, Akamai, atau Amazon Web Services (AWS), yang secara otomatis mendeteksi dan menghentikan serangan DDoS dengan menurunkan lalu lintas berlebih ke *server* cloud mereka sebelum mencapai *server e-commerce*.

d. Pemantauan Jaringan Secara Real-Time

Pemantauan lalu lintas jaringan secara terus-menerus sangat penting untuk mendeteksi potensi serangan DDoS sejak dini. Sistem pemantauan yang kuat dapat mendeteksi pola lalu lintas yang tidak normal dan memberikan peringatan untuk tindakan segera.

e. Sistem Deteksi dan Pencegahan Intrusi (IDS/IPS)

IDS/IPS memantau jaringan untuk mendeteksi anomali dan memblokir serangan yang terdeteksi. Sistem ini penting untuk mendeteksi serangan DDoS pada tahap awal dan menghentikan aktivitas berbahaya sebelum merusak *server*.

Menurut *UpGuard (2022),* serangan DDoS menjadi salah satu ancaman utama terhadap perusahaan *e-commerce*, yang menyebabkan gangguan operasional yang signifikan

Serangan DDoS merupakan ancaman serius bagi perusahaan *e-commerce* karena dampaknya yang besar terhadap ketersediaan layanan, pendapatan, dan reputasi perusahaan. Namun, dengan penerapan solusi keamanan yang tepat seperti CDN, WAF, dan layanan anti-DDoS, perusahaan dapat secara efektif mencegah dan memitigasi serangan ini. Keamanan jaringan yang proaktif dan pemantauan lalu lintas secara real-time juga menjadi elemen penting dalam menghadapi ancaman DDoS yang terus berkembang.

4. *Hacking*

Hacking adalah ancaman besar dalam dunia *e-commerce*, yang mencakup segala bentuk akses tidak sah ke sistem, data, atau jaringan untuk mencuri informasi atau merusak sistem. Hackers sering menargetkan platform *e-commerce* karena besarnya volume transaksi finansial dan data pelanggan yang disimpan, seperti informasi pembayaran dan detail pribadi. Ini membuat *e-commerce* sangat rentan terhadap serangan seperti *SQL injection, Cross-Site Scripting* (XSS), serta metode *hacking* lainnya.

Jenis-Jenis serangan dalam *E-Commerce*

a. *SQL Injection*

SQL Injection adalah salah satu teknik *hacking* yang paling umum di sektor *e-commerce*. Dalam serangan ini, peretas memasukkan kode berbahaya ke dalam kueri *SQL* di aplikasi *web*. Ini memungkinkan peretas untuk mengakses, memodifikasi, atau bahkan menghapus data dari basis data *e-commerce*. Serangan ini sering terjadi karena kurangnya validasi input dari pengguna di situs *e-commerce*. Contoh: Pada tahun 2017, platform *e-commerce* populer di India, Zomato, terkena serangan *SQL Injection* yang menyebabkan data lebih dari 17 juta pengguna bocor, termasuk *email* dan kata sandi yang dienkripsi.

b. *Cross-Site Scripting* (XSS)

XSS memungkinkan peretas menyuntikkan *script* berbahaya bagi situs *web* yang selanjutnya dijalankan di peramban pengguna.. Serangan ini bisa mencuri informasi pribadi pengguna, seperti cookie atau informasi *login*. XSS biasanya mengeksploitasi formulir input pengguna yang tidak memiliki validasi yang tepat.

Misalnya, pada tahun 2020, platform *e-commerce* besar di AS mengalami serangan XSS, di mana hacker menyusupkan kode *JavaScript* berbahaya ke halaman *checkout*, yang memungkinkan mereka mencuri informasi pembayaran pengguna saat mereka menyelesaikan pembelian.

c. *Brute Force Attack*

Brute Force Attack adalah bentuk serangan yang terjadi ketika peretas mencoba menebak kredensial *login* pengguna dengan menjalankan kombinasi kata sandi secara otomatis sampai berhasil. Perusahaan *e-commerce* sering kali menjadi target serangan ini karena banyak pelanggan yang menggunakan kata sandi yang lemah atau mudah ditebak. Brute force *attack*s sering kali berhasil karena lemahnya kebijakan kata sandi atau kurangnya penggunaan autentikasi multi-faktor (MFA). Misalnya, situs *e-commerce* yang tidak memiliki batas jumlah percobaan *login* bisa menjadi target utama peretas.

d. *Man-in-the-Middle* (MitM) *Attack*

Selama serangan MitM, peretas mencegat komunikasi antara pengguna dan situs *web e-commerce* untuk mencuri informasi, seperti kredensial *login* atau detail kartu kredit. Serangan ini sering terjadi ketika pengguna terhubung ke jaringan *Wi-Fi* publik yang tidak aman, yang memungkinkan peretas mengakses data yang dikirimkan antara perangkat pengguna dan *server e-commerce*. Contoh: Pada tahun 2018, sebuah perusahaan *e-commerce* besar mengalami serangan MitM yang menyebabkan pencurian data ribuan pelanggan selama transaksi yang dilakukan melalui jaringan *Wi-Fi* publik di pusat perbelanjaan.

Strategi Pencegahan *Hacking* di *E-Commerce*

a. Penerapan HTTPS dan Sertifikat SSL/TLS

Mengamankan situs *web e-commerce* dengan HTTPS dan sertifikat SSL/TLS adalah langkah awal untuk melindungi komunikasi antara *server* dan pengguna dari serangan *Man-in-the-Middle* (MitM). HTTPS mengenkripsi data selama transmisi, membuat informasi sensitif seperti data *login* dan informasi pembayaran aman dari akses peretas. Platform *e-commerce* besar seperti Amazon dan eBay sudah lama menggunakan SSL/TLS untuk melindungi data pelanggan dan transaksi, dan mereka juga mengedukasi pelanggan tentang pentingnya mengakses situs melalui HTTPS. Teknologi enkripsi SSL/TLS telah terbukti efektif dalam melindungi informasi sensitif, seperti data kartu kredit, selama transaksi online *(SecuritySenses, 2021)*

b. Pemeriksaan Keamanan Berkala (*Penetration Testing*)

Penetration testing atau pengujian penetrasi secara berkala sangat penting untuk mengidentifikasi potensi celah keamanan dalam sistem dan aplikasi *web*. Penetration testing meniru serangan peretas untuk menguji kerentanan yang mungkin ada, seperti *SQL Injection*, XSS, atau kelemahan dalam konfigurasi *server*. Perusahaan *e-commerce* besar sering kali

bekerja sama dengan perusahaan keamanan siber untuk melakukan pengujian penetrasi, memastikan bahwa sistem mereka tetap terlindungi dari ancaman *hacking* terbaru.

c. Kebijakan Keamanan Kata Sandi dan MFA

Salah satu langkah yang sering diremehkan namun sangat penting adalah kebijakan keamanan kata sandi. Platform *e-commerce* harus memberlakukan kebijakan kata sandi yang kuat, seperti mewajibkan penggunaan karakter campuran (huruf besar, kecil, angka, dan simbol), serta membatasi jumlah percobaan *login*. Authentikasi Multifaktor (MFA) juga merupakan lapisan perlindungan tambahan yang signifikan. Dengan MFA, peretas tidak akan bisa mengakses akun meskipun mereka mengetahui kata sandi pengguna karena mereka juga memerlukan kode verifikasi yang dikirimkan ke perangkat pengguna.

d. Penggunaan WAF (Web Application *Firewall*)

WAF adalah *firewall* yang dirancang untuk melindungi aplikasi *web* dari serangan umum, seperti *SQL Injection*, XSS, dan serangan lainnya yang sering digunakan dalam *hacking e-commerce*. WAF memonitor dan memfilter lalu lintas jaringan yang masuk untuk mendeteksi serangan sebelum mencapai *server web*. Sebagai contoh, platform *e-commerce* seperti Shopee dan Lazada menggunakan WAF untuk melindungi situs mereka dari berbagai ancaman yang bisa merusak keamanan data pengguna.

e. Tokenisasi Data Pembayaran

Tokenisasi adalah proses menggantikan data sensitif, seperti informasi kartu kredit, dengan token yang tidak memiliki nilai di luar konteks transaksi tertentu. Dengan menggunakan tokenisasi, perusahaan *e-commerce* dapat mengurangi risiko pencurian data karena data asli tidak disimpan atau diproses di *server e-commerce*.

f. Pemantauan dan Logging Real-Time

Pemantauan real-time dan logging sangat penting dalam mendeteksi aktivitas mencurigakan. Dengan menggunakan sistem pemantauan yang canggih, perusahaan *e-commerce* dapat mendeteksi percobaan *hacking* atau aktivitas abnormal di jaringan dan mengambil tindakan pencegahan segera. Logging juga membantu dalam melakukan investigasi jika terjadi pelanggaran keamanan.

Hacking adalah ancaman besar bagi perusahaan *e-commerce* yang menyimpan data pelanggan dalam jumlah besar. Tanpa strategi keamanan yang kuat, serangan seperti *SQL Injection*, XSS, *brute force attack*s, dan *Man-in-the-Middle attack*s dapat menyebabkan kerugian besar, termasuk pencurian data, kehilangan kepercayaan pelanggan, dan kerusakan reputasi. Oleh karena itu, penerapan enkripsi data, WAF, MFA, serta pemantauan dan pengujian penetrasi berkala sangat penting untuk melindungi sistem *e-commerce* dari serangan *hacking*.

SIMPULAN

Kemajuan teknologi informasi (TI) memberikan banyak keuntungan bagi perusahaan *e-commerce* dalam hal kecepatan dan efisiensi layanan. Namun, bersamaan dengan itu, risiko yang dihadapi dalam transaksi digital juga meningkat secara signifikan. Salah satu tantangan terbesar yang dihadapi oleh perusahaan *e-commerce* adalah ancaman serangan siber, seperti *Distributed Denial of Service* (DDoS), pencurian identitas, *malware*, juga , yang dapat berdampak besar pada keamanan data dan kepercayaan pelanggan.

Peranan *IT Security* sangat vital dalam melindungi infrastruktur TI serta data sensitif yang dipertukarkan selama transaksi online. Dalam konteks *e-commerce*, penerapan teknologi keamanan yang canggih seperti enkripsi data, *firewall*, dan sistem deteksi intrusi (IDS/IPS) menjadi kunci dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Selain itu, kepatuhan terhadap regulasi keamanan data, seperti PCI DSS, juga merupakan langkah krusial yang harus diambil oleh perusahaan untuk melindungi data pembayaran pelanggan.

Serangan seperti DDoS bertujuan untuk membuat layanan tidak dapat diakses oleh pengguna sah, yang dapat menimbulkan kerugian finansial serta merusak reputasi perusahaan. *Malware*, yang sering kali digunakan untuk mencuri informasi pelanggan, juga merupakan ancaman yang sangat serius bagi perusahaan *e-commerce*.

Untuk menghadapi ancaman ini, diperlukan penerapan sistem keamanan berlapis, seperti penggunaan perangkat lunak antivirus yang canggih, pembaruan perangkat lunak secara berkala, dan penerapan enkripsi data. Dalam hal serangan *phishing*, perusahaan juga harus menerapkan Authentikasi Multifaktor (MFA) sebagai langkah tambahan untuk mengamankan akun pelanggan.

Dalam jurnal ini, dibahas pula pentingnya kepercayaan pelanggan dalam keberhasilan perusahaan *e-commerce*. Pelanggan yang merasa aman akan lebih cenderung untuk melakukan transaksi, sehingga transparansi dalam kebijakan privasi dan komunikasi mengenai langkah-langkah keamanan yang diambil oleh perusahaan sangat penting untuk membangun kepercayaan tersebut. Selain teknologi keamanan, peningkatan kesadaran pelanggan dan edukasi karyawan mengenai ancaman siber juga harus menjadi prioritas. Banyak serangan siber berhasil karena kurangnya pemahaman mengenai , *malware*, atau celah keamanan lainnya. Oleh karena itu, memberikan edukasi yang tepat tentang cara mengidentifikasi ancaman siber dan melaporkan aktivitas mencurigakan dapat membantu perusahaan mencegah kerugian yang lebih besar. Sebagai kesimpulan, perusahaan *e-commerce* harus secara proaktif mengadopsi teknologi keamanan yang canggih dan mematuhi regulasi internasional untuk melindungi data pelanggan serta infrastruktur TI mereka. Perlindungan hukum dan teknologi yang solid sangat penting dalam menghadapi tantangan keamanan yang semakin kompleks di era digital ini.

SANJUNGAN DAN UCAPAN TERIMA KASIH

Saya mengucapkan terima kasih sebesar-besarnya kepada Tuhan Yang Maha Esa, serta kepada kawan, rekan, kerabat, dan semua pihak yang telah berperan penting dalam membantu pelaksanaan serta penulisan penelitian ini hingga terselesaikannya jurnal ilmiah ini.

DAFTAR PUSTAKA

[1] Peranan Penting *Network Security* dalam melindungi Data dan Jaringan https://cyberhub.id/pengetahuan-dasar/peran-network-security (diakses 7 Oktober 2024)

[2] 9 Peranan Penting *Information Security* Manager https://itgid.org/insight/artikel-it/information-security (diaksess 7 Oktober 2024)

[3] Pentingnya Peran Cyber Security untuk menjaga keamanan *E-Commerce* https://ids.ac.id/peran-cyber-security-untuk-keamanan-*e-commerce* (diakses 8 Oktober 2024)

[4] Cybersecurity, 2024. Pengertian Hacker, Jenis, dan Metode Peretasan-nya. https://vida.id/id/blog/hacker-adalah. (diakses 8 Oktober 2024)

[5] Upaya Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo Mbanking https://journal.unilak.ac.id/index.php/gh/article/download/18827/6495 (diakses 8 Oktober 2024)

[6] E-Commerce Security and Fraud Issues and Protections https://link.springer.com/chapter/10.1007/978-3-319-58715-8_11 (diakses 8 Oktober 2024)

[7] Data Risk Mitigation: How To Keep Your Organization's Data Safe https://www.datagrail.io/blog/data-privacy/data-risk-mitigation/ (diakses 9 Oktokber 2024)

[8] Qasaimeh, M., Halemah, N. A., Rawashdeh, R., Al-Qassas, R. S., & Qusef, A. (2022). *Systematic Review of E-commerce Security Issues and Customer Satisfaction Impact. 2022 International Conference on Engineering & MIS* (ICEMIS), 45–48. https://doi.org/10.1109/ICEMIS56295.2022.9914393 (diakses 10 Oktober 2024)

[9] Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). *Protection of Personal Data in the Context of E-Commerce. Journal of Cybersecurity and Privacy*, 4(3), 6–9. https://doi.org/10.3390/jcp4030034 (diakses 10 Oktober 2024)

[10] Breach Investigations Report https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf (diakses 10 Oktober 2024)

[11] Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual (diakses 10 Oktober 2024)

[12] 13 Juta Data Bocor Bukalapak Dijual di Forum Hacker https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker (diakses 10 Oktober 2024)

[13] Kasus Serangan Malware Bank Syariah Indonesia (BSI) Mei 2023 https://koran.tempo.co/read/berita-utama/482085/7-fakta-dugaan-serangan-ransomware-oleh-lockbit-ke-bsi (diakses 10 Oktober 2024)

[14] Kasus Serangan DDoS di Indonesia: Apa yang Terjadi dan Cara Menghindari? https://www.jagoweb.com/kasus-serangan-ddos-di-indonesia-apa-yang-terjadi-dan-cara-menghindari (diakses 10 Oktober 2024)