TUGAS MATA KULIAH E-COMMERCE

“ KEAMANAN BUSINESS PLAN GROWFI SCARF“

Dosen Pengampu :

Bapak Wartariyus, S.Kom, M.T.I

DISUSUN OLEH :

Muhamad Amirudin 2113025023

PROGRAM STUDI PENDIDIKAN TEKNOLOGI INFORMASI

FAKULTAS KEGURUAN DAN ILMU PENDIDIKAN

UNIVERSITAS LAMPUNG

2023

KATA PENGANTAR

Puji Syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya sehingga kami mampu menyelesaikan Laporan Penugasan Keamanan Business Plan sebagai tugas pertemuan ke 10 mata kuliah E-Commerce. Dalam laporan ini kami menyusun rencana bisnis yang berjudul "***Keamanan Business Plan Grow Scarf*".**

Kami mengucapkan terima kasih kepada semua orang yang telah membantu kami membuat laporan ini. Penulis terbuka untuk kritik dan saran karena mereka menyadari bahwa tulisan ini masih banyak kekurangan. Mudah-mudahan pembaca dan penulis akan mendapatkan pemahaman yang lebih baik tentang bagaimana merancang rencana bisnis.

Bandar Lampung, 30 November 2023

Muhamad Amirudin

DAFTAR ISI

BAB I
PENDAHULUAN

A. Latar Belakang

Dalam era globalisasi dan kemajuan teknologi informasi yang pesat, industri e-commerce telah menjadi pilar utama perdagangan global. Salah satu sektor yang terus berkembang di dalamnya adalah bisnis printing delivery. Dalam konteks ini, layanan cetak yang diantar langsung ke pelanggan menjadi solusi efisien bagi mereka yang enggan meninggalkan rumah. Meskipun terdapat peluang signifikan di sektor ini, tantangan terkait keamanan juga perlu diatasi untuk memastikan kelancaran operasional bisnis.

Keamanan dalam konteks bisnis e-commerce printing delivery mencakup perlindungan terhadap data pelanggan, transaksi keuangan, dan informasi bisnis secara keseluruhan. Ancaman seperti pencurian data, serangan pihak tidak bertanggung jawab, dan kebocoran informasi dapat mengancam kelangsungan bisnis dan kepercayaan pelanggan. Oleh karena itu, merancang rencana keamanan bisnis e-commerce menjadi sangat penting. Melihat tren pesatnya pertumbuhan internet di Indonesia, e-commerce menjadi pendorong utama pertumbuhan perusahaan di sektor ini. Seiring dengan perkembangan ini, bisnis printing delivery dapat memanfaatkan peluang untuk menjangkau konsumen lebih luas, namun perlu tetap memprioritaskan keamanan dalam setiap aspek operasionalnya. Dalam konteks teknologi modern, perubahan besar terjadi dalam berbagai aspek kehidupan manusia. Meskipun teknologi membawa manfaat dan keuntungan, perlu diakui bahwa juga muncul beberapa masalah dan risiko. Oleh karena itu, penggunaan teknologi dalam bisnis printing delivery harus diimbangi dengan tanggung jawab yang memadai.

Kepercayaan pelanggan menjadi kunci dalam bisnis ini, dan faktor keamanan memegang peranan sentral dalam membangun citra positif perusahaan. Dengan menjaga keamanan transaksi dan data pelanggan, bisnis printing delivery dapat memperkuat kepercayaan pelanggan dan membentuk citra positif dalam industri e-commerce. Dalam pengembangan rencana bisnis e-commerce untuk layanan printing delivery, penting untuk melakukan penelitian dan menerapkan strategi keamanan yang efektif. Hal ini tidak hanya

akan memastikan pertumbuhan bisnis, tetapi juga kelangsungan operasional dengan memperhatikan faktor-faktor keamanan yang mendasar.

B. Rumusan Masalah

Beberapa permasalahan utama yang perlu dipecahkan dalam konteks keamanan bisnis plan e-commerce mendirikan bisnis Printing Delivery adalah:

1. Adakah cara untuk mengatasi Tantangan Keamanan Data Pelanggan ?
2. Adakah cara untuk melindungi Keamanan Transaksi Keuangan ?

C. Tujuan Pembahasan

Tujuan pembahasan dalam makalah ini adalah :

1. Menganalisis Tantangan Keamanan Bisnis E-Commerce pada Bisnis Printing Delivery.
2. Mengidentifikasi Solusi dan Strategi Keamanan yang Efektif.

BAB II
PEMBAHASAN

A. Cara mengatasi Tantangan Keamanan Data Pelanggan

Berikut adalah beberapa cara untuk mengatasi masalah keamanan data pelanggan e-commerce: mengambil pendekatan yang luas dan berbagai langkah perlindungan :

1. Enkripsi Data

   Menggunakan teknologi enkripsi untuk melindungi data pelanggan selama pengiriman dan penyimpanan. Ini meningkatkan keamanan secara signifikan karena data yang dienkripsi sulit diakses oleh pihak yang tidak berwenang.
2. Pemilihan Platform Keamanan yang Tepat

   Pilih platform e-commerce dengan standar keamanan tinggi. Pilih penyedia layanan e-commerce dengan fitur keamanan seperti SSL (Secure Sockets Layer) untuk melindungi data saat berpindah antara server dan pengguna.
3. Verifikasi Identitas Pengguna

   Untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses dan melakukan transaksi di platform e-commerce, gunakan sistem verifikasi identitas yang kuat seperti otentikasi dua faktor (2FA).
4. Penyusunan Kebijakan Keamanan Internal

   Meningkatkan kesadaran keamanan karyawan dan menetapkan kebijakan keamanan internal yang jelas. Pelatihan rutin keamanan diperlukan dan seluruh karyawan yang terlibat dalam pengelolaan data pelanggan diajarkan praktik terbaik.
5. Monitoring Aktivitas yang Mencurigakan

   Menggunakan sistem pemantauan keamanan untuk menemukan aktivitas yang mencurigakan atau tidak biasa, seperti upaya akses yang tidak sah atau pengecekan berulang. Jika terdeteksi, aktivitas mencurigakan dapat dicegah lebih cepat.

6. Kebijakan Privasi yang Transparan

   Membuat kebijakan privasi yang jelas dan mudah dipahami pelanggan. Beri tahu pelanggan tentang cara data mereka digunakan, disimpan, dan dilindungi sehingga mereka yakin dan memahami risiko.

7. Pemeliharaan dan Pembaruan Sistem Keamanan

   Melakukan pemeliharaan dan pembaruan rutin sistem keamanan, termasuk perangkat lunak dan perangkat keras. Ini juga mencakup menginstal pembaruan keamanan terbaru untuk mencegah penggunaan celah keamanan yang mungkin telah ditemukan.

8. Backup Rutin

   Melakukan backup data secara teratur untuk mencegah kehilangan data penting dalam kasus serangan atau kejadian tak terduga lainnya. Backup juga dapat membantu dalam pemulihan data jika terjadi insiden keamanan.

Bisnis e-commerce dapat meningkatkan perlindungan data pelanggan dan menumbuhkan kepercayaan pelanggan yang lebih tinggi dengan menerapkan kombinasi strategi ini.

B. Bagaimana melindungi Keamanan Transaksi Keuangan ?

Dalam proses jual beli online, e-commerce telah membantu pengguna internet di seluruh dunia. Banyak bisnis e-commerce yang menjadikannya bisnis (baik produk maupun layanan), dan banyak konsumen online yang menggunakan layanan ini. Kepercayaan pelanggan adalah kunci kesuksesan bisnis, termasuk bisnis online berbasis e-Commerce. Layanan yang aman dan nyaman akan menumbuhkan kepercayaan pelanggan.

Kajian keamanan sistem di bidang e-commerce dilakukan untuk menyelesaikan masalah ini. Keselamatan ini bertujuan untuk membuat pembeli dan penjual merasa nyaman dan aman saat melakukan transaksi jual beli. Beberapa teknologi yang digunakan termasuk pemanfaatan Firewall, teknologi komputasi cloud, sertifikasi SSL (Secure Socket Layer), dan verifikasi kartu kredit.

a) Pengamanan Pada E-Commerce Menggunakan Sertifikasi SSL

Salah satu protokol pada jaringan komputer, khususnya di lapisan jaringan, adalah SSL (Secure Socket Layer). SSL melakukan enkripsi (perubahan paket data) dan enkripsi paket data antara komputer pengirim dan penerima. Dengan melakukan kedua proses ini, keamanan data di jaringan komputer dapat dijamin dengan baik. Semua entitas dalam jaringan komputer diatur oleh protokol. Salah satu lapisan pemodelan lapisan jaringan komputer adalah lapisan transportasi, yang bertanggung jawab untuk menangani proses transmisi paket data, juga dikenal sebagai transportasi, melalui penerapan berbagai protokol.

b). Pengamanan Pada E-Commerce Menggunakan Firewall

Firewall adalah kombinasi perangkat keras (hardware) dan perangkat lunak (software) komputer yang dirancang untuk melindungi jaringan komputer dengan mengawasi arus paket data dan mengaturnya. Firewall dapat berupa perangkat lunak (software) atau sistem yang terdiri dari kombinasi perangkat lunak dan perangkat keras komputer, yang dapat digunakan oleh pengguna komputer pribadi dan komputer server di dalam jaringan komputer. Tugas utama firewall adalah mengatur dan mengawasi lalu lintas paket data, yang memastikan keamanan jaringan.

c). Pengamanan Pada E-Commerce Menggunakan Teknologi Cloud Computing

Mengingat betapa pentingnya layanan keamanan untuk e-commerce untuk melindungi proses transaksi agar tidak disalahgunakan, melindungi penjual dan pembeli, mencegah tindak kejahatan di internet, dan meningkatkan kredibilitas layanan. Dengan demikian, memanfaatkan layanan yang ditawarkan oleh teknologi cloud computing adalah salah satu solusi yang dapat digunakan.

Cloud Computing dibezakan dengan setidaknya lima fitur yang membedakannya dari teknologi dan layanan lain di jaringan komputer. Fitur-fitur ini termasuk :

1. On Demand Self Service

   Salah satu fitur komputasi cloud adalah On Demand Self Service, yang

memungkinkan pengguna layanan cloud untuk secara mandiri memenuhi semua kebutuhan dan kemampuan komputasi mereka, seperti :

a. Ketersediaan penyimpanan jaringan sebagai penyimpanan digital pada jaringan media komputer
b. Server time sebagai system waktu di sisi computer server.
c. Meminimalisir interaksi dengan penyedia layanan (Service Provider dan Server)
d. Pelanggan dapat menggunakan layanan sesuai dengan permintaan (On Demand). Tiga jenis layanan (IAAS, PAAS, dan SAAS) dan empat model penyebaran (Publik, Private, Hybrid, dan Community Cloud) tersedia. Tiga jenis layanan ini juga termasuk dalam struktur komputasi cloud.

2. Broad Network Access

   Salah satu aspek cloud computing di mana layanan cloud computing membutuhkan akses ke jaringan yang luas. jaringan komputer yang memadai, baik pada internet, intranet, atau kombinasi kedua, pada skala besar, akan memudahkan penyediaan layanan kepada pengguna dari berbagai platform dan media. Misalkan komputer desktop, laptop, smartphone, dan lainnya. Akses luas ke jaringan akan melibatkan topologi jaringan, noda, server, perangkat penghubung (router, hub, dan switch), dan protokol jaringan pada beberapa lapisan jaringan komputer.

3. Resource Pooling

   Sumber daya berbagi adalah fitur cloud computing di mana sumber daya komputasi dapat diberdayakan di berbagai lokasi fisik (bukan hanya di satu lokasi fisik). Para pengguna layanan komputasi cloud (SAAS, PAAS, atau IAAS) dapat mengetahui bagaimana kebutuhan mereka dapat terpenuhi dengan lokasi fisik yang bebas (independen). Mereka juga tidak perlu mengetahui secara fisik atau teknis tentang server mana layanan tersebut berasal. Pengguna cukup memahami informasi teknis tentang informasi negara penyedia layanan cloud atau pusat data yang menyimpan data di jaringan cloud. Sumber daya

komputasi cloud, termasuk media penyimpanan, pemrosesan, memori, bandwith jaringan, dan virtual machine, terus bekerja untuk memenuhi kebutuhan pengguna.

4. Rapid Elasticity

   Rapid Elasticity adalah fitur komputasi awan di mana jumlah layanan dapat naik atau turun sesuai dengan kebutuhan pengguna yang bersifat On Demand (sesuai dengan kebutuhan Anda sebagai pengguna layanan) dalam waktu yang cepat. Hal ini akan membantu memenuhi kebutuhan pengguna untuk layanan cloud dari ketiga jenis layanan yang tersedia: SAAS, PAAS, dan IAAS. Selain itu, karakteristik Rapid Elasticity ini mencakup dukungan topologi yang lebih fleksibel untuk jaringan komputer, kualitas layanan yang lebih balk pada jaringan komputer (high service quality), penyajian layanan yang cepat (rapid provisioning), dan layanan dengan lokasi penentuan yang tak terbatas.

5. Measured Service

   Salah satu fitur Cloud Computing yang dapat diukur adalah Measured Service. Kualitas layanan (QoS) dan Kualitas Pengalaman (QoE) adalah dua cara untuk mengukur kualitas layanan pada komputasi awan. Kualitas layanan (QoS) adalah pengukuran kualitas layanan pada komputasi awan dari perspektif penyedia layanan (provider), sedangkan Kualitas Pengalaman (QoE) adalah pengukuran kualitas layanan pada komputasi awan dari perspektif pengguna.

   Dengan perkembangan teknologi yang semakin pesat dan banyaknya pihak yang berpartisipasi di dalamnya, sistem keamanan transaksi e-commerce sangat penting untuk memberikan rasa aman kepada pelanggan. Ini karena sebagian besar masyarakat saat ini adalah pengguna internet dan juga pengguna e-commerce. Oleh karena itu, sistem keamanan e-commerce sangat penting untuk memberikan rasa aman kepada pelanggan.

BAB III
PENUTUP

A. KESIMPULAN

Banyak situs web dan aplikasi e-commerce yang tersedia di Indonesia. Sebagian besar toko online menggunakan platform dan aplikasi terkenal. Pelanggaran data dan pencurian identitas sering terjadi dalam industri e-commerce. Pelanggaran data dan pencurian identitas diantisipasi melalui penggunaan berbagai teknologi alat keamanan. Meskipun e-commerce telah berkembang selama bertahun-tahun, masih ada masalah keamanan data. Solusi yang dapat memperkuat sistem hukum dan manajemen yang ada saat ini diperlukan. Untuk menjaga keamanan data, metode kriptografi yang lebih canggih juga perlu ditingkatkan.