BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan globalisasi ekonomi telah melahirkan kompetisi dunia usaha yang semakin ketat diikuti dengan perkembangan teknologi informasi yang menyebabkan perubahan dan cara pandang hidup manusia dan suatu organisasi. Media baru komunikasi manusia telah berkembang pesat, seperti komputer yang berkembang pesat dari sekedar piranti lunak untuk manajemen informasi hingga piranti untuk telekomunikasi. Multimedia interaktif dan jalan raya informasi, dan komponen terkait internet memungkinkan terciptanya ekonomi baru berdasarkan jaringan intelegensi manusia., ekonomi baru ini disebut dengan Ekonomi Digital. Salah satu unsur strategis bagi daya saing organisasi bisnis dalam ekonomi digital ini adalah pengelolaan sistem informasi akuntansi sedemikian rupa sehingga menjadi sumber keunggulan daya saing perusahaan.

Dunia perdagangan ekonomi digital tidak lagi dibatasi dengan ruang dan waktu. Mobilitas manusia yang tinggi menuntut dunia perdagangan mampu menyediakan layanan jasa dan barang dengan instan sesuai dengan permintaan konsumen. Dalam ekonomi digital, individu dan perusahaan mengeruk kekayaan dengan mengaplikasikan pengetahuan, jaringan intelegensi manusia, dan berbagai usaha manufaktur, pertanian, dan jasa. Transaksi dalam ekonomi digital ini lebih dikenal dengan nama *e-Commerce* dan *e-Business*.

Electronic Commerce merupakan penggunaan media elektronik untuk melakukan perniagaan / perdagangan, seperti penggunaan telepon, *fax*, ATM, *handphone*, banking, dan secara khusus penggunaan Internet untuk melakukan perniagaan. Searah dengan pesatnya perkembangan Teknologi Informasi dan berkembangnya *e-Commerce* membawa dampak yang menguntungkan dan juga merugikan. Dampak positif dari penggunaan *e-Commerce* antara lain, *Revenue Stream* baru, *Market Eksposure*, menurunkan biaya, meningkatkan *customer loyality*, meningkatkan *value chain*, serta *Global reach*. Sedangkan dampak yang merugikan dalam penggunaan *e-Commerce* antara lain kehilangan segi finansial secara langsung karena kecurangan, pencurian informasi rahasia yang berharga, kehilangan kesempatan bisnis karena gangguan pelayanan, penggunaan akses ke sumber oleh pihak yang tidak berhak, kehilangan kepercayaan dari para konsumen, serta kerugian yang tidak terduga.

Kita telah banyak melihat dan mendengar kejadian pada jaringan internet yang menghadapi serangan virus, pembajakan *software*, sampai dengan masalah pencurian kartu kredit. Untuk yang terakhir ini, efeknya telah mengglobal sehingga banyak penyelenggara *dot.com* atau perusahaan delivery yang tidak percaya akan keabsahan kartu dari Indonesia, terutama dari pulau Jawa. Hal ini sangat memberatkan perkembangan ekonomi kita. Sistem keamanan dalam pembelian dan pembayaran melalui *e-Commerce* sangatlah penting, karena akan mempengaruhi tingkat kepercayaan orang dalam melakukan transaksi bisnis secara online.

Salah satu perusahaan *webstore* terbesar yang ada adalah eBay Company. Perusahaan ini merupakan salah satu perusahaan perintis yang beroperasi melalui *e-commerce*. Ebay Company ini sendiri pernah mengalami masalah pada websitenya karena diserang oleh *Distributed Denial of Service Attack* (*DDoS attack*) sehingga tidak dapat memberikan layanan (*down*) selama beberapa jam. Serangan ini mengakibatkan baik perusahaan maupun customer mengalami kerugian secara finansial yang tidak kecil jumlahnya, karena mempengaruhi sistem yang ada di perusahaan tersebut, termasuk juga sistem pembelian dan pembayarannya. Selain itu sering terjadi pencurian *password* para membership customer di eBay Company tersebut, sehingga terjadi penyalahgunaan yang menyebabkan kerugian baik finansial maupun moril bagi para pelanggan, seperti pencurian *ID*, penagihan barang yang tidak pernah dibeli pada kartu kredit, mendapat kiriman email *SPAM*, dan sebagainya.

Padahal seperti yang telah kita ketahui, eBay merupakan salah satu perusahaan *webstore* terkemuka yang memiliki sistem keamanan yang cukup memadai. Perusahaan ini telah menggunakan sistem keamanan yang sesuai dengan standar keamanan *website* yang ditetapkan, baik dalam prosedur pembayaran maupun pembelian. Namun dalam pelaksanaanya masih saja terjadi kecurangan dan penyimpangan yang dapat menimbulkan kerugian bagi kedua belah pihak.

Kejadian seperti ini membuktikan bahwa perusahaan webstore besar dan terkemuka pun memiliki kelemahan yang dapat ditembus oleh pihak – pihak yang tidak bertanggungjawab. Sistem pengendalian keamanan dalam pembelian dan pembayaran melalui e-commerce yang efektif pada suatu perusahaan dapat terlihat

dengan tidak adanya kecurangan dan kerugian dari kedua belah pihak yang diakibatkan adanya pencurian, dan pengiriman barang yang sesuai dengan pesanan para konsumen, kecermatan data dan semua prosedur yang ditetapkan telah berjalan dengan baik.

Berdasarkan uraian tersebut di atas, maka saya selaku penulis ingin menulis penelitian skripsi dengan judul

"**Analisis Sistem Keamanan Dalam Pembelian dan Pembayaran Melalui e-Commerce Pada eBay Company**"

B. Perumusan Masalah

Bertitik tolak pada latar belakang yang diuraikan sebelumnya, maka yang akan menjadi bahan penelitian yaitu :

1. Bagaimana prosedur sistem informasi keamanan dalam pembelian dan pembayaran melalui *e-Commerce* pada *eBay Company*?
2. Apakah prosedur pengendalian sistem keamanan dalam pembelian dan pembayaran yang berjalan dalam perusahaan sudah memadai?

C. Pembatasan Masalah

Transaksi melalui *e-Commerce* memiliki banyak aspek, yaitu pemasaran, penjualan, pembelian, dan pelayanan, penulis menitikberatkan masalah pada kegiatan sistem keamanan dalam pembelian dan pembayaran melalui *e-Commerce* pada *eBay*

Company, melalui situsnya *http://www.eBay.com*. Pembatasan masalah ini untuk memudahkan dalam pembahasan dan tidak menyimpang dari masalah pokoknya.

D. Tujuan Penelitian

Berdasarkan dari permasalah yang telah dipaparkan, tujuan dari penelitian ini adalah :

1. Untuk memahami penerapan prosedur sistem informasi keamanan dalam pembelian dan pembayaran melalui *e-Commerce* pada *www.eBay.com* .
2. Untuk mengetahui apakah prosedur pengendalian sistem keamanan dalam pembelian dan pembayaran yang berjalan dalam perusahaan sudah memadai.

E. Manfaat Penelitian

Manfaat penelitian yang diharapkan dari hasil penelitian :

1. Bagi Penulis

   Penelitian ini sangat berguna bagi penulis untuk menambah wawasan dan pengalaman dalam menganalisa Sistem Informasi Akuntansi di bidang sistem keamanan dan untuk mengetahui mengenai penerapan dan pengendalian sistem keamanan dalam pembelian dan pembayaran melalui *e-Commerce* .

2 Bagi Perusahaan

   Dari hasil penelitian dapat dijadikan informasi bagi perusahaan untuk menganalisa kembali apakah sistem keamanan dalam pembelian dan

pembayaran melalui *e-Commerce* yang diterapkan telah berjalan dengan baik dan sesuai.

3. Bagi Masyarakat

   Masyarakat luas dapat lebih mengenal tentang *e-Commerce*, khususnya tentang keamanan dalam bertransaksi menggunakan *e-Commerce*, yang merupakan tuntutan kemajuan dari globalisasi ekonomi.

F. Landasan Teori

1. Pengertian Sistem

Sistem dapat dijelaskan dengan sederhana sebagai seperangkat elemen yang digabungkan satu dengan yang lainnya untuk suatu tujuan bersama. Setiap sistem terdiri dari beberapa elemen – elemen, dan elemen – elemen tersebut merupakan bagian yang terpadu dari suatu sistem yang bersangkutan.

Menurut George H. Bodnar dan Williams S. Hopwood Sistem adalah

"Suatu kumpulan dari sumber daya - sumber daya yang saling berhubungan dengan beberapa tujuan yang dapat dicapai."

Sedangkan pengertian sistem menurut Robert G. Murdick, Joel Eross, dan James R. Claggett dalam bukunya *Sistem Informasi untuk Manajemen Modern*

"Suatu sistem adalah seperangkat elemen yang membentuk kegiatan, atau suatu prosedur, atau bagan pengolahan yang mencari suatu tujuan atau tujuan – tujuan bersama dengan mengoperasikan data dan atau barang pada waktu rujukan tertentu untuk menghasilkan informasi dan atau energi dan atau barang."

Elemen – elemen sistem tersebut berhubungan erat satu dengan yang lain dan tidak dapat berdiri lepas sendiri – sendiri, mereka saling berinteraksi dan saling berhubungan membentuk suatu kesatuan sehingga sasaran suatu sistem dapat tercapai interaksi dalam suatu sistem itu sedemikian rupa sehingga dicapai suatu kesatuan dan terintegrasi dan terpadu.

2. Pengertian Informasi

Informasi sangat penting di dalam suatu organisasi. Suatu sistem yang kurang memberikan informasi akan sulit mendukung keputusan yang tepat. Menurut G. Murdick, Joel Eross, dan James R. Claggett, informasi terdiri dari data yang telah diambil kembali, diolah atau sebaliknya digunakan untuk tujuan informatif atau kesimpulan, argumentasi, atau sebagai dasar untuk peramalan atau pengambilan keputusan.

Pengertian teknologi informasi menurut Christopher Pas & Bryan Lowes "Proses pengumpulan, pemrosesan dan interpretasi data baik dari lingkungan luar maupun dalam perusahaan dengan menggunakan teknologi informasi dalam komputer".

Menurut George H. Bodnar dan William S. Hopwood di dalam buku *Accounting Information System* sistem informasi merupakan penggunaan teknologi komputer di dalam sebuah organisasi untuk memberikan informasi bagi para pengguna.

Informasi merupakan komoditi penting bagi semua organisasi. Suatu sistem yang kurang mendapat informasi lama kelamaan akan tertinggal, tidak dapat mengikuti perkembangan yang ada, akhirnya akan menjadi kurang atau tidak bermanfaat.

Sumber dari informasi adalah data. Data merupakan bentuk yang masih mentah, belum dapat bercerita banyak, sehingga perlu diolah lebih lanjut. Data dapat berbentuk simbol – simbol semacam huruf – huruf atau alphabeth, angka – angka, bentuk – bentuk suara, sinyal – sinyal, gambar – gambar dan sebagainya. Data diolah melalui model untuk menghasilkan informasi.

3. Pengertian Sistem Informasi Akuntansi

Tujuan akhir dari kegiatan akuntansi adalah penerbitan laporan – laporan keuangan, baik yang diolah secara manual ataupun secara terkomputerisasi. Data – data keuangan tersebut selanjutnya akan ditransformasikan menjadi informasi yang dibutuhkan.

Dalam buku *Accounting*, (*Horngren, Harrison Jr, Bamber*, 2002) menjelaskan bahwa Sistem Informasi Akuntansi merupakan kombinasi dari orang – orang, catatan – catatan, dan prosedur – prosedur yang digunakan dalam bisnis untuk menyajikan data finansial. Setiap sistem informasi akuntansi yang terjadi dapat dicatat dengan dua cara yaitu manual dan komputerisasi.

Menurut George H. Bodnar dan Williams S. Hopwood pengertian dari *Sistem Informasi Akuntansi* (SIA) sebagai berikut

"Sistem Informasi Akuntansi (SIA) adalah kumpulan sumber daya, seperti manusia dan peralatan yang diatur untuk mengubah data menjadi informasi. Informasi ini dikomunikasikan kepada beragam pengambil keputusan. SIA mewujudkan perubahan ini secara manual atau komputerisasi".

Pengguna informasi akuntansi dibagi menjadi dua ; yaitu eksternal dan internal. Yang termasuk pengguna eksternal antara lain para pemegang saham, investor, kreditor, lembaga pemerintahan, pelanggan dan penjual, pesaing, dan masyarakat. Sedangkan yang pengguna internal informasi akuntansi terdiri dari para manajer dari berbagai level dalam perusahaan.

Sistem Informasi Akuntansi ini secara luas kita gunakan dalam siklus pemrosesan transaksi, penggunakan teknologi informasi, dan perkembangan sistem informasi. Fungsi dari sistem informasi adalah bertanggung jawab untuk data processing (DP). DP adalah dasar dari aplikasi sistem informasi akuntansi dalam setiap organisasi. Fungsi sistem informasi dalam perusahaan-perusahaan berkembang dari struktur organisasi yang sederhana yang meliputi beberapa orang, menjadi struktur yang kompleks yang meliputi banyak jenis spesialisasi dalam perusahaan.

4. E-Commerce

1. Pengertian E-Commerce

E-Commerce merupakan transformasi dari perkembangan ekonomi saat ini, dengan jaringan komunikasi global dan terbuka yang menghubungkan ribuan

jaringan komputer, melalui sambungan telepon umum dan pribadi (pemerintah maupun swasta).

Pengertian *e-Commerce* menurut F. Rayport dan Bernard J. Jaworski dalam bukunya *e-Commerce* (2001:hal 3) yaitu :

"*E-Commerce* adalah suatu teknologi yang memediasi pertukaran antara bagian (individual, organisasi, atau antara keduanya) sebaik elektronik berbasis aktivitas intra dan interorganisasi yang memfasilitasi setiap pertukaran dengan menggunakan media elektronik, yaitu internet dan web".

Sedangkan pengertian *e-Commerce* menurut buku *Management Information System for The Information Age*, *e-Commerce* merupakan perdagangan, tetapi merupakan perdagangan yang dipercepat dan ditambah dengan teknologi informasi, dengan penggunaan internet. Hal ini memungkinkan para pelanggan, konsumen, dan perusahaan untuk menampilkan kekuatan dari hubungan baru yang tidak mungkin tanpa penggunaan teknologi.

Dengan adanya *e-Commerce* segala batasan wilayah dan jarak dalam pemasaran yang selama ini ada dapat diatasi, karena pelayanan transakasi dan pengiriman barang atau jasa via internet atau *channel* elektronik dapat dilakukan kapan saja dan dimana saja. Setiap perusahaan dapat membuka tokonya selama 24 jam non stop, tentu saja secara virtual, yang dapat membantu menghemat biaya pembangunan gedung.

2. Karakteristik E-Commerce

Beberapa karakteristik *e-Commerce* menurut Jeffrey F. Rayport dan Bernard J. Jaworski dalam bukunya *e-Commerce* yaitu :

a. Merupakan pertukaran informasi secara digital antara beberapa bagian

   Pertukaran informasi ini bisa antara dua bagian koordinasi dari arus jasa dan barang atau pengiriman pesanan elektronik. Pertukaran ini bisa antara organisasi, individual, atau antar keduanya.

b. Termasuk aktivitas intra dan antarorganisasi yang mendukung pertukaran

   Ruang lingkup *e-Commerce* yaitu semua elektronik berbasis aktivitas intra dan interorganisasi, baik pertukaran secara langsung atau tidak langsung yang mendukung pertukaran pasar. Dalam hal ini *e-Commerce* mempengaruhi 2 hal yaitu bagaimana organisasi bisnis berhubungan dengan pihak eksternal (pelanggan, supplier, partner, pesaing, dan pasar-pasar) dan bagaimana organisasi bisnis tersebut beroperasi secara internal dalam mengatur aktivitas, proses, dan sistem mereka.

c. Merupakan perantara teknologi

   E-Commerce berpindah dari penggunaan teknologi transasksi sederhana kepada sebuah teknologi perantara hubungan. Tempat dimana penjual dan pembeli bertemu untuk bertransasksi, berpindah dari pasar fisik ke pasar maya atau virtual. Oleh sebab itu, kesuksesan dari sebuah bisnis bergantung pada seberapa baik layar dan mesin melayani pelanggan dan keinginan mereka.

3. Jenis- Jenis e-Commerce

a. *BUSINESS TO BUSINESS (B2B),* yaitu transasksi yang dilakukan antar perusahaan yang berperan sebagai penjual sekaligus sebagai pembelinya. Contohnya yaitu transasksi penjualan dan pembelian yang dilakukan oleh *distribution outlet (DISTRO)* yang melakukan transaksi dengan salah satu produk yang mereka pasarkan, dimana perusahaan yang memproduksi barang tersebut berasal dari luar negeri.

b. *BUSINESS TO CONSUMER (B2C)*, yaitu transaksi yang dilakukan antara perusahaan dengan individual, dimana perusahaan berperan sebagai penjual dan individu sebagai pembelinya. Contohnya yaitu perusahaan *Plasa.Com* yang menyediakan informasi kepada khalayak umum untuk mencari barang – barang atau berita yang diinginkan.

c. *CONSUMER TO CONSUMER (C2C),* yaitu transaksi yang dilakukan oleh individu yang menjual barang atau jasanya kepada individu lain. Biasanya transaksi ini bersifat tidak formal dan pribadi, dan juga hubungan yang dilakukan oleh pembeli dan penjual merupakan hubungan pertemanan, dan juga dimana barang – barang yang diperjualbelikan tidaklah terlalu besar wujud maupun harganya, misalnya baju dan buku.

d. *GOVERNMENT TO GOVERNMENT (G2G),* yaitu transaksi yang terjadi antara pemerintah, baik antar pemerintah pusat ke pemerintah daerah maupun antar pemerintah negara yang satu dengan negara yang lain, misalnya transaksi untuk ekspor dan impor.

e. *GOVERNMENT TO BUSINESS (G2B),* yaitu transaksi yang terjadi antara pemerintah dengan pihak swasta, disini dapat dicontohkan yaitu pihak swasta memfasilitasi gedung pemerintah, bisa berupa alat – alat kantor, sofa, maupun alat – alat elektronik yang diperlukan di dalam gedung pemerintahan tersebut.

f. *GOVERNMENT TO CITIZEN (G2C),* yaitu transaksi yang terjadi antara pemerintah dengan warga negaranya, salah satu contohnya yaitu pembayaran tagihan telepon dan listrik yang bisa dilakukan lewat bank yang ditunjuk oleh pemerintah.

4. Sistem Informasi Pembelian dan Pembayaran Pada e-Commerce

a. Sistem Informasi Pembelian Pada *e-Commerce*

Belanja secara elektronik merupakan suatu usaha mengkombinasikan katalog belanja dengan proses belanja langsung di toko yang bersangkutan. Aplikasi berbasis Web menawarkan interaktivitas yang lebih baik daripada katalog, dan juga memiliki kemampuan untuk menggunakan bentuk – bentuk media seperti audio, video klip, animasi, yang bisa ditambahkan pada teks, dan gambar.

Semua ini merupakan cara – cara membuat kegiatan belanja menjadi lebih menarik, dan pada akhirnya bisa menjual barang. Keberhasilan belanja online tergantung hampir seluruhnya pada kenyamanan belanja dengan faktor – faktor seperti media yang diperkaya.

Situs Web perusahaan menjadi identitas toko elektronik. Pembeli "masuk" toko dengan cara browsing di situs Web toko. Sewaktu pembeli mengunjungi

toko elektronik, atau situs Web, ia melihat – lihat beragam produk yang dijual. Beragam produk yang dijual dapat dilihat pada katalog. Katalog produk secara khusus terdiri dari kode produk, deskripsi produk, harga, dan informasi lain. Si pembeli membaca penjelasan dari produk tersebut, melihat harganya, dan memutuskan apakah membeli atau tidak. Barang yang diinginkan ditampung dalam sebuah troli belanja elektronik.

Seperti pada troli belanja konvensional, aspek – aspek penting lain dari troli belanja elektronik adalah pelangan bisa memilih item – item, bisa melacak harga total yang harus dibayarnya dan membandingkan dengan dana yang dimilikinya, dan bisa mengubah jumlah barang yang akan dibeli atau tidak jadi membeli barang yang sudah dipilih sebelumnya.

b. Sistem Informasi Pembayaran Pada *e-Commerce*

Sewaktu pembeli selesai memilih item – item yang ingin dibelinya, sistem pemroses pembayaran mengambil detil – detil informasi dari troli belanjanya. Sistem itu juga menanyakan beberapa informasi tambahan untuk melengkapi order, misalnya alamat pengiriman, cara pengiriman, metode pembayaran dan sebagainya. Pada titik ini pembeli diberi pilihan untuk meninjau kembali ordernya bila perlu.

Pelanggan memiliki beberapa pilihan dalam melakukan pembayaran. Kartu kredit dan kartu debit adalah metode pembayaran yang paling populer di hampir semua toko retail, baik toko retail biasa atau toko retail elektronik. Semua sistem

pemproses pembayaran elektronik bisa menangani pembayaran lewat kartu kredit dan cek.

Sistem pemroses pembayaran berhubungan dengan gateway pembayaran dalam memverfikasi keotentikan metode pembayaran si pelanggan atas semua barang belanjaanya. Untuk kartu kredit, gateway pembayaran memeriksa nomor kartu kredit dan tanggal kadaluarsanya, memverifikasi kepemilikannya, dan menentukan apakah saldo di kartu kredit masih mencukupi untuk membayar semua belanjaanya.

Pada situs toko elektronik, sistem pemrosesan pembayaran menyimpan semua catatan terperinci mengenai keseluruhan transaksi sehingga bisa disesuaikan kembali sewaktu pembayaran diterima oleh institusi finansialnya. Dalam hal ini, mempertahankan catatan transaksi menjadi penting dilakukan, dan catatan – catatan tersebut harus dijaga ketat. Penyerang yang bisa menembus catatan – catatan tersebut merupakan ancaman keamanan yang besar karena ia dapat mengetahui identitas pelanggan dan instrumen – instrumen pembayarannya untuk melakukan penipuan.

5. Sistem dan Prosedur Electronic Payment System

Untuk dapat menerima sistem pembayaran melalui *credit card* melalui sebuah *website*, terdapat 3 elemen penting, yaitu :

1. Sebuah formulir bagi website tersebut, yaitu berupa formulir pemesanan barang / jasa (*order form*). Dan formulir tersebut digabungkan dengan teknologi sistem keamanan seperti SSL (*Secure Socket Layer*).
2. Memiliki rekening *credit card* pada sebuah bank
3. *Payment processing* untuk melayani dan sebagai penghubung antara sebuah *website* dengan bank yang bersangkutan.

Dalam *e-Commerce* sistem pembayaran ini disebut FEDI (*Financial Electronic Data Interchange*). FEDI ini terdiri dari 3 jenis, yaitu :

1. ***Credit card & Smart Card***

   Credit card merupakan jenis pembayaran secara kredit melalui bank, sedangkan *Smart Card* merupakan kartu plastik seukuran kartu kredit, yang terdapat sebuah *chip*, dimana informasi digital dapat diketahui.

2. ***Financial Cybermedia***

   Merupakan internet dasar yang digunakan perusahaan – perusahaan, yang memudahkan bagi setiap orang untuk membayar orang lain melalui internet.

3. ***Electronic Bill Presentment and Payment*** **(EBPP)**

   Cara kerja sistem ini adalah dengan mengirimkan tagihan kita melalui internet (berupa email) dan memberi kita kemudahan untuk membayar tagihan tersebut (jika jumlah tagihan tersebut benar) melalui cara yang kita inginkan.

Formulir pemesanan *online* yang digunakan adalah formulir yang biasa digunakan. Hanya saja pembuatan formulir dibuat dengan menggunakan bahasa pemprograman HTML dan disiapkan untuk menggunakan sebuah naskah CGI

(*Commin Gateway Interface*) cara standar bagi Web server dalam menyediakan akses ke informasi dan program di luar sistem dan protokol normal web agar formulir online tersebut dapat melakukan hal – hal sebagai berikut :

1. Mengirimkan informasi *credit card* ke *Payment – payment software*, yang mana akan mengirimkan transaksi tersebut ke bank yang bersangkutan.
2. Mengirimkan sebuah *e-mail* kepada siapapun yang mengisi pemesanan, dengan disertai informasi atas pemesanan dan *customer mailing address* bila datanya tepat.
3. Membuat sebuah halaman konfirmasi bagi pelanggan. Halaman ini selain berisi sebagai ucapan terima kasih atas pemesanan mereka, juga meminta nomor telepon dan atau alamat *e-mail* yang dapat dihubungi jika terjadi masalah dengan pesanan pelanggan.

6. Pengendalian Untuk Transaksi melalui E-commerce

Pengendalian dalam sistem transaksi melalui *e-Commerce* sangat penting, karena jaringan komputer bersifat terbuka dan umum untuk global, sehingga tidak menutup kemungkinan akan munculnya kerugian – kerugian yang ditimbulkan dari dalam dan luar perusahaan. Untuk itulah diperlukan suatu pengendalian yang diharapkan dapat mengurangi hal tersebut. Pengendalian yang diterapkan pada sistem informasi sangat berguna untuk mencegah atau menjaga hal – hal yang tidak diinginkan.

Sumber potensial dari permasalahan yang timbul pada *e-Commerce* adalah perhatian konsumen terhadap *privacy* dan *security* di internet. Transaksi bisnis secara

elektronik hanya dapat berhasil jika pertukaran finansial antara pihak yang bersangkutan dapat terlaksana dalam suatu cara yang sederhana, diterima secara universal, aman serta biaya sistem yang murah. Sistem pembayaran telah banyak diajukan sekarang ini, beberapa diantaranya masih berbasis pada mekanisme tradisional dengan menggunakan *credit card*, dan yang lainnya sudah mulai menggunakan desain baru seperti *electronic money*.

Keamanan beberapa sistem yang dapat digunakan untuk mengamankan pemesanan penjualan antara lain :

1. **SSL (*Secured Socket Layer*)**

   Sangat populer digunakan karena didukung oleh kebanyakan browser, dan oleh kebanyakan *Internet Service Provider* (ISP). SSL adalah protokol keamanan internet yang menyediakan privasi, aplikasi klien / server selalu diidentifikasi secara opsional. Menggunakan sebuah *secure web protokol* seperti SSL mempunyai 2 tujuan utama :

   a. Meng-enkrip data *credit card* yang sedang ditransmisikan, sehingga akan menyulitkan pihak ketiga untuk memecahkannya.

   b. Mensertifikasi pesan yang datang dari suatu tempat, sehingga akan menyulitkan bagi pihak ketiga untuk memalsukan transaksi tersebut. Hal ini yang dinamakan *digital certificate*.

2. **Kerberos**

   Merupakan protokol untuk melakukan otentifikasi, *accounting*, dan audit. Namun dua tujuan terakhir ini tidak pernah diimplementasikan. Kerberos

menggunakan sistem otentifikasi terpusat pada sebuah server. Tidak seperti pada sistem otentifikasi pada umumnya, Kerberos tidak menggunakan sistem enkripsi kunci publik, dan hanya menggunakan sistem enkripsi kunci simetris. Protokol ini mengasumsikan terdapatnya satu atau lebih server dan beberapa klien dalam satu jaringan.

3. **Pretty Good Privacy (PGP)**

   Pada awalnya PGP ditujukan untuk mengamankan pengiriman email. Sekarang PGP dapat digunakan untuk mengamankan semua jenis file program dan data. Dokumentasi PGP sering menyebut istilah *secret key* (kunci rahasia) untuk menyebut kunci privat (pasangan kunci publik dalam terminologi enkripsi kunci publik). Ini dapat membingungkan pembaca yang belum lama berkecimpung dalam bidang kriptografi.

Berikut ini adalah berbagai solusi pengendalian yang dapat dilakukan untuk mengatasi masalah keamanan transaksi, yaitu :

a. Pembuatan rekening, dalam hal ini, konsumen atau bisnis membuat kesepakatan secara *offline* (dengan telepon, *mail, faks*, dan lain sebagainya) untuk pembayaran melalui kartu kredit atau penciptaan suatu macam kredit. Pesanan kemudian dapat dibuat dengan blangko input pada halaman web atau melalui email.
b. Pesanan Pembelian Sistem, ini melibatkan pembelian atau uang virtual untuk digunakan bersama berbagai macam vendor yang dalam hal ini enskripsi ditawarkan dalam sebuah pesan email melalui mail serve MIME, enskripsi

PGP atau penggunaan HTTP yang aman, atau SSL sehingga dapat mengirim data kartu kredit atau yang lainnya kepada masing – masing vendor.

7. Keamanan Situs

Hampir semua bisnis mempunyai beberapa perhatian yang sama tentang situs web, karena seseorang dapat memperoleh informasi transaksi, memutuskan dan mengubah data atau merusak data. Dan hal ini dapat ditangani melalui metode yang telah ada diantaranya :

1. *Firewall*

   Sebuah *firewall* biasanya adalah kombinasi perangkat keras dan lunak yang menjamin bahwa hanya *entry* yang terotorisasi ke dalam sistem yang diizinkan. *Firewall* dapat berupa sebuah komputer, *router*, atau peralatan komunikasi yang menyaring akses untuk melindungi jaringan dari mudah diserang, gangguan ilegal, kecelakaan, atau tindak kejahatan, misalnya untuk melindungi jaringan perusahaan dari pengacau ilegal saat pengguna komputer perusahaan mengakses ke layanan internet. Perlu dicatat, bahwa *firewall* bisa berupa seperangkat *hardware* atau *software* atau bisa juga berupa seperangkat aturan dan prosedur (*policy*) yang ditetapkan oleh organisasi.

   Firewall juga dapat berfungsi sebagai akses *unauthorized* yang akan keluar atau masuk ke jaringan LAN dan ke Internet. Kalau dimisalkan dalam sebuah konstruksi bangunan, *firewall* dirancang dan dibuat untuk menjaga agar api tidak menjalar dari salah satu bagian bangunan ke bagian yang lain.

2. *Password*

Merupakan pertahanan terakhir untuk sebuah sistem komputer. Sistem otentikasi ini kita gunakan untuk melakukan koneksi, misalnya ke email, *sharing file, sharing devices*, dan lain – lain. Setiap *password* yang kita masukkan haruslah dikenali oleh databasenya. Biasanya *password* berupa beberapa karakter yang bisa berupa angka atau huruf. Beberapa cara untuk melindungi *password* adalah :

1. Jangan pernah memakai *password* menggunakan kata – kata yang ada di kamus, apalagi kamus Bahasa Inggris, karena akan memudahkan para *hacker* melakukan penebakan password dengan program khusus yang disebut *dictionary attack*.
2. Gunakan kombinasi huruf dan angka
3. Buatlah *password* sepanjang minimal 5 karakter
4. Gantilah *password* secara berkala
5. Jangan menggunakan *password* yang sama untuk berbagai otentikasi lain
6. Gabungkan huruf besar dan huruf kesil
7. Jangan menggunakan *password* dengan data pribadi
8. *Password* harus mudah diingat

3. Proteksi File

Jika halaman Web perusahaan dikelola oleh penyedia akses internet maka file – file perusahaan dari pengubahan oleh orang lain, serta juga akan melindungi informasi pembelian konsumen perusahaan agar tidak dibaca oleh orang lain.

4. E-mail yang aman

   Ada beberapa cara untuk mendapatkan email yang aman. Yang paling terkenal adalah ekstensi keamanan baru untuk MIME yang disebut *Secure Multipurpose Internet Main Extension* (S/MIME). Dengan ini berarti bahwa e-mail atau file – file yang di *attack* dapat dengan aman ditransmisikan di atas internet dan tidak dapat dibuka atau dibaca dalam persinggahan.

5. *Enkripsi*

   Enkripsi adalah sebuah proses dimana sebuah pesan (*plaintext*) ditransformasikan ke bentuk pesan lain (*chipertext*) menggunakan fungsi matematis, dan sebuah *enkripsi password special* yang dikenal dengan istilah *key*. *Enkripsi* mencakup informasi sehingga informasi tersebut relaitf tidak dapat diakses. Metode – metose enkripsi yang disebut *"Strong Encryption"* yang sekarang tersedia dapat digunakan. Karena dengan metode ini dapat menghabiskan waktu lebih dari 100 tahun waktu komputer untuk memecahkanya jika tidak mengetahui kode pembukanya.

5. EDP (*Electronic Data Processing*) Pada Perusahaan

Dengan majunya teknologi maka penggunaan sistem manual dan mekanikal dalam pengolahan data ditinggalkan dan mengarah penggunaan sistem elektronis. Ada tiga perhatian dalam penggunaan sistem elektronis yaitu pemrosesan data yang kompleks tanpa kekeliruan, dapat melakukan pekerjaan yang sulit dengan teliti dan melaksanakan perhitungan – perhitungan dengan lebih cepat.

Sebagian besar organisasi menggunakan EDP (*Electronic Data Processing*) setidaknya sebagai alat bantu, dalam memproses informasi akuntansi dan keuangan. Sistem EDP dapat ditentukan menurut kompleksitas tekhniknya dan sejauh mana sistem EDP digunakan dalam organisasi.

Pada pemrosesan secara online, sistem online memungkinkan akses langsung ke dalam komputer. Transaksi – transaksi dapat dimasukkan secara langsung ke dalam sistem sehingga master file dimukhtahirkan pada saat entri dibuat, daripada ditangguhkan seperti pada *basic batch*. Demikian pula, keluaran dari status isi file data berjalan tersedia bila dibutuhkan. Sistem online menggunakan terminal *display* baik untuk tujuan masukan maupun keluaran. Sistem ini memungkinkan suatu pemrograman dan beberapa fungsi operator tertentu dilaksanakan secara online.

Ada lima tugas dalam bagian EDP, yaitu :

1. *System Analisis*

   Bertanggung jawab menyusun suatu sistem baik yang menyangkut tujuan sistem itu sendiri.

2. *Programmer*

   Bertanggung jawab untuk pembuatan *flowchart*, menyusun instruksi, menguji dan mendokumentasikan hasilnya.

3. Operator

   Bertanggung jawab untuk pengolahan data melalui sistem dengan menggunakan program komputer dengan mengikuti petunjuk yang telah dibuat.

4. *Librarian*

   Bertanggung jawab untuk menyimpan program komputer files transaksi dan catatan lainnya. Perhitungan fisik harus dilakukannya karena kepekaannya dan kerahasiaannya.

5. *Group Control*

   Bertanggung jawab menguji keefektifan dan keefisisenan suatu sistem yang diterapkan, yang menjadi perhatiannya tidak hanya masukkan dan keluaran tetapi juga kebebasan pengunci yang mengoperasikannya.

6. Sejarah Sistem Keamanan Internet

Beberapa peristiwa penting yang terjadi dalam sistem keamanan jaringan internet baik di luar negeri maupun di Indonesia sendiri adalah sebagai berikut :

a. Di luar negeri

1. *1988*. Keamanan sistem mail *sendmail* dieksploitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem internet. Kegiatan ini dapat diklasifikasikan sebagai *"Denial of Service Attack"*. Diperkirakan biaya yang digunakan untuk memperbaiki dan hal – hal lain yang hilang adalah sekitar $100juta. Di tahun 1990 Morris dihukum (*convicted*) dan hanya didenda $10.000.
2. *10 Maret 1997*. Seorang *hacker* dari Massachussetts berhasil mematikan sistem telekomunikasi di sebuah bandara lokal. (Worcester, Massachussetts) sehingga mematikan komunikasi di menara kontrol dan

menghalau pesawat yang hendak mendarat. Dia juga mengacaukan sistem telepon di Rutland, Massachussetts. *(http://www.news.com/News/Item/Textonly/0,25,20278,00.html?pfv http://www.news.com/News/Item/0,4,20226,00.html)*

3. *07 Februari 2000 (Senin) sampai dengan 09 Februari 2000 pagi (Rabu).* Beberapa web terkemuka di dunia diserang oleh *Distributed Denial of Service Attack* (*DDoS attack*) sehingga tidak dapat memberikan layanan (*down*) selama beberapa jam. Tempat yang diserang antara lain *Yahoo!, Buy.com, eBay, CNN, Amazon.com, ZDNet, E-Trade*. FBI mengeluarkan tools untuk mencari program TRINOO atau *Tribal Flood Net* (TFN) yang diduga digunakan untuk melakukan serangan dari berbagai penjuru dunia.
4. *04 Mei 2001*. Situs *Gibson Research Corp*. (*grc.com*) diserang *Denial of Service Attack* oleh anak berusia 13 tahun sehingga *bandwidth* dari *grc.com* yang terdiri dari dua TI connection menjadi habis. Steve Gibson kemudian meneliti *software* yang digunakan untuk menyerang (*DoS bot*, *SubSeven Trojan*), *channel* yang digunakan untuk berkomunikasi (via IRC), dan akhirnya menemukan beberapa hal tentang DoS attack ini. Informasi lengkapnya ada di situs *www.grc.com*.

b. Di Indonesia

1. *Akhir Januari 1999*. Domain yang digunakan untuk Timor Timur (.tp) diserang sehingga hilang. Domain untuk Timor Timur ini diletakan pada

sebuah *server* di Irlandia yang bernama *Connect-Ireland*. Pemerintah Indonesia disalahakan atau dianggap melakukan kegiatan *hacking* ini. Menurut keterangan yang diberikan oleh *administratror Connect-Ireland*, 18 serangan dilakukan secara serempak dari seluruh penjuru dunia. Akan tetapi berdasarkan pengamatan, domain Timor Timur tersebut di-hack dan kemudian ditambah *sub domain need.tp*. Berdasarkan pengamatan situasi, *need.tp* merupakan sebuah perkataan yang sedang dipopulerkan oleh *"Beavis and Butthead"* (sebuah acara TV di MTV). Dengan kata lain, *cracker* yang melakukan serangan tersebut kemungkinan penggemar (atau paling tidak pernah menonton) acara tersebut. Jadi, ada kemungkinan serangan ini dilakukan oleh seseorang dari Amerika Utara.

2. *Januari 2000*. Beberapa situs Web Indonesia diacak – acak oleh cracker yang menamakan dirinya *fabianclone* dan *naisenodni* (kata Indonesia dibalik). Situs yang diserang termasuk Bursa Efek Jakarta, BCA, dan *Indosatnet*. Selain situs yang besar tersebut masih banyak situs lainnya yang tidak dilaporkan.
3. *September dan Oktober 2000*. Setelah berhasil membobol Bank Lippo, kembali *Fabianclone* beraksi dengan menjebol web milik Bank Bali.
4. *16 April 2001*. Polda DIY meringkus seorang *carder* Yogya. Tersangka diringkus di Bantul dengan barang bukti sebuah paket yang berisi lukisan (Rumah dan Orang Indian) berharga Rp 30 juta. Tersangka berstatus mahasiswa STIE Yogyakarta.

5. *Juni 2001*. Seorang mahasiswa alumni ITB membuat beberapa situs yang mirip (persis sama) dengan situs *klikbca.com* yang digunakan BCA untuk memberikan layanan *Internet Banking*. Situs yang dibuatnya menggunakan nama domain yang mirip dengan *klikbca.com* yaitu *kilkbca.com, wwwklikbca.com, clikbca.com,* dan *klickbca.com*. Sang user mengaku bahwa memperoleh PIN dari beberapa nasabah BCA yang salah mengetikan nama situs layanan *Internet Banking* tersebut.
6. *20 April 2004*. Situs dan sistem jaringan komputer KPU pusat berhasil dijebol dan *cracke*r mengganti informasi yang ada dalam sistem tersebut seperti nama partai dan mencoba mengganti tabulasi perolehan suara. Dengan *SQL Injections, cracker* berhasil masuk lewat tiga *IP Address* yang berbeda. Saat itu *cracker* masih tercatat sebagai seorang mahasiswa jurusan hubungan internasional di sebuah universitas swasta di Yogyakarta dan bekerja sebagai konsultan di sebuah perusahaan Jakarta.

G. Metodologi Penelitian

1. Bentuk Penelitian

Dalam penelitian ini penulis menggunakan metode deskriptif analisis. Alasan pemilihan metode deskriptif analisis ini dikarenakan karena metode ini tidak hanya berusaha untuk meneliti suatu proyek penelitian dengan mencari dan menemukan fakta yang ada, tetapi juga memberikan deskripsi atau gambaran

secara sistematis, kemudian menguraikannya melalui analisis dan pengertian mengenai data akurat.

2. Variable Pengukuran

Untuk memberikan penjelasan mengenai variable – variable dalam penelitian ini digunakan pengukuran kinerja sistem keamanan dalam pembelian dan pembayaran melalui *e-Commerce* yaitu :

1. Prosedur Sistem Pembelian dan Pembayaran melalui *e-Commerce*, merupakan suatu komponen bisnis yang segala aktifitasnya dilaksanakan atas infrastruktur sistem informasi secara online.
2. Sistem Pengendalian Intern Pembelian dan pembayaran

   Pengendalian intern sistem keamanan merupakan prosedur mekanis tindakan pengendalian dan pengamanan atas suatu proses dalam pembelian dan pembayaran melalui *e-Commerce* yang meliputi :

   a. Kerahasiaan dan privacy dari permintaan

      Pengendalian kerahasiaan dan privacy ini dilakukan untuk memeriksa kebenaran akan data transaksi pelanggan sebagai suatu tindakan pengamanan bahwa transaksi tersebut memang dilakukan oleh pihak yang sah dan yang bersangkutan.

   b. Authorisation, authentication dan access control

      Pengendalian ini dilakukan untuk memeriksa ketelitian dan kebenaran data – data transaksi yang valid apakah telah lengkap, dan terkumpul

semuanya, yang kemudian diperiksa agar bebas dari segala kesalahan, sebelum dilakukan proses pengolahan transaksi lebih lanjut.

c. Identitas pelanggan dan authorisation profile

Pengendalian identitas ini dilakukan untuk memeriksa kebenaran akan identitas pelanggan dan authorisation profile sebagai suatu tindakan pengamanan bahwa transaksi tersebut memang dilakukan oleh pihak yang sah dan yang bersangkutan.

d. Cryptographic key management

Untuk menjaga intergrasi dan keamanan data yang tersimpan agar tidak hilang, rusak, atau diakses oleh orang yang tidak berhak maka segi keamanan situs juga menjadi perhatian utama

e. Firewalls

Dapat berupa sebuah komputer, *router*, atau peralatan komunikasi yang menyaring akses untuk melindungi jaringan dari mudah diserang, gangguan ilegal, kecelakaan, atau tindak kejahatan, misalnya untuk melindungi jaringan perusahaan dari pengacau ilegal saat pengguna komputer perusahaan mengakses ke layanan internet.

f. Pendeteksian dan pencegahan virus

Sistem yang digunakan untik mendeteksi virus yang menyerang dan pencegahan yang dilakukan pleh sistem keamanan secara otomatis dan merupakan bagian dari sistem firewall.

g. Pelatihan penggunaan bagi pelanggan

Program yang diberikan bagi pelanggan untuk memberikan petunjuk cara menggunakan layanan situs secara mudah dan cepat.

h. Tools untuk mengawasi komplain dari pelanggan, segala gangguan dan pelaporan

Merupakan program tools bagi para pelanggan untuk menyampaikan segala macam komplain yang dialami dalam bertransaksi, gangguan – gangguan tekhnis serta ketidakpuasan para pelanggan dalam bertransaksi.

i. Penanganan kejadian, pelaporan, dan cara mengatasinya

Cara yang digunakan perusahaan untuk mengatasi segala macam kendala yang terjadi, pelaporannya serta cara mengatasinya.

3. Teknik Pengumpulan Data

Data sangatlah penting untuk mendukung dalam melakukan analisis dan terhadap suatu masalah yang akan diteliti. Di dalam menyusun teknik pengumpulan data dikenal dua jenis, yaitu :

a. ***Field Search***

Merupakan suatu metode yang ditujukan untuk mengumpulkan data primer. Data primer adalah data yang dikumpulkan dan diolah sesuai dengan tujuan dan desain penulis sebagai referensi, atau apabila digunakan, menggunakan hasil research sumber lain, tetapi yang mengolah adalah penulis sendiri.

b. *Library Search*

Merupakan metode dalam usahanya mengumpulkan data sekunder. Data sekunder adalah data yang sudah diambil, diproses, dan dikumpulkan serta diolah oleh orang lain untuk tujuan – tujuan tertentu yang sesuai dengan tujuan penelitian. Penulis mengumpulkan berbagai ragam informasi yang dibutuhkan, baik berupa tesis, laporan maupun publikasi lainnya baik yang bersifat umum maupun internal.

4. Metode Analisis Data

Analisis data merupakan aktifitas untuk menemukan jawaban atas pertanyaan perihal rumusan – rumusan yang diperoleh dalam penelitian. Metode yang digunakan penulis dalam menganalisa data yang dikumpulkan adalah metode analisis deskriptif atau kualitatif, yaitu menjelaskan dan menjabarkan mengenai sistem keamanan dalam pembelian dan pembayaran melalui *e-Commerce*. Selanjutnya hasil penelitian dari kepustakaan yang ada dibandingkan dengan kenyataan yang ada pada perusahaan yang diteliti oleh penulis yaitu *eBay.com* untuk dianalisis dan ditarik suatu kesimpulan.