ISSN 2085-2576
VOL II-NO.1 – MARET 2010

JURNAL MANAJEMEN INFORMATIKA

Penerapan eLearning Sebagai Media Pembelajaran Dalam Meningkatkan Mutu Pendidikan
Dewi Irmawati

Merancang Sistem Informasi Website Untuk Database Monitoring Dan Reporting CDR
Henny Madora

Pengembangan Aplikasi Berbasis Konsep Smart Classroom Sebagai Sarana Pendukung Interaksi Pembelajaran
Hetty Meileni

Simulasi Multimedia Interaktif Untuk Menunjang Pemahaman Mahasiswa Dalam Komunikasi Visual
Maivi Kusnandar, Indra Satriadi, Sony Oktapriandi

Pemanfaatan Wireless Aplication Sebagai Perangkat Untuk Mengakses Web Address
Sony Oktapriandi

Pembangunan Perangkat Lunak Menggunakan Sistem Data Terdistribusi (Studi Kasus: Sistem Informasi Akademik Politeknik Negeri Sriwijaya)
Zulkarnaini

Resiko Dan Pengamanan eCommerce
Ridwan Effendi

Pengaruh Faktor Intrinsik Dan Ekstrinsik Terhadap Motivasi Belajar Mahasiswa (Studi Pada Mahasiswa Jurusan Administrasi Niaga Politeknik Negeri Sriwijaya)
Heri Setiawan

Faktor-Faktor Yang Mempengaruhi Investasi Untuk Mendorong Pertumbuhan Ekonomi (Jurusan Manajemen Informatika Politeknik Negeri Sriwijaya)
Muhammad Noval

Pentingnya Komunikasi Verbal Dalam Proses Pembelajaran (Kajian Perspektif Komunikasi Efektif Pada Pembelajaran)
Nita Novita

JURUSAN MANAJEMEN INFORMATIKA
POLITEKNIK NEGERI SRIWIJAYA

ISSN 2085-2576

Jurnal Manajemen Informatika Politeknik Negeri Sriwijaya

Vol. II. No. 1 – Maret 2010

DAFTAR ISI

1. *Penerapan eLearning Sebagai Media Pembelajaran Dalam Meningkatkan Mutu Pendidikan*
   Dewi Irmawati 1-12

2. Merancang Sistem Informasi Website Untuk *Database Monitoring Dan Reporting CDR*
   Henny Madora 13-17

3. Pengembangan Aplikasi Berbasis Konsep Smart Classroom *Sebagai Sarana Pendukung Interaksi Pembelajaran*
   Hetty Meileni 18-22

4. *Simulasi Multimedia Interaktif Untuk Menunjang Pemahaman Mahasiswa Dalam Komunikasi Visual*
   Maivi Kusnandar, Indra Satriadi, Sony Oktapriandi 23-27

5. *Pemanfaatan Wireless Aplication Sebagai Perangkat Untuk Mengakses Web Address*
   Sony Oktapriandi 28-35

6. *Pembangunan Perangkat Lunak Menggunakan Sistem Data Terdistribusi (Studi Kasus: Sistem Informasi Akademik Politeknik Negeri Sriwijaya)*
   Zulkarnaini 36-41

7. *Resiko Dan Pengamanan eCommerce*
   Ridwan Effendi 42-46

8. *Pengaruh Faktor Intrinsik Dan Ekstrinsik Terhadap Motivasi Belajar Mahasiswa (Studi Pada Mahasiswa Jurusan Administrasi Niaga Politeknik Negeri Sriwijaya)*
   Heri Setiawan 47-53

9. *Faktor-Faktor Yang Mempengaruhi Investasi Untuk Mendorong Pertumbuhan Ekonomi (Jurusan Manajemen Informatika Politeknik Negeri Sriwijaya)*
   Muhammad Noval 54-56

10. *Pentingnya Komunikasi Verbal Dalam Proses Pembelajaran (Kajian Perspektif Komunikasi Efektif Pada Pembelajaran)*
    Nita Novita 57-64

RESIKO DAN PENGAMANAN eCOMMERCE

Ridwan Effendi
Staf Pengajar Jurusan Manajemen Informatika Politeknik Negeri Sriwijaya
Jalan Srijaya Negara Bukit Besar – Palembang 30139
e-mail: ridwan_effendi_mi@polsri.ac.id

ABSTRAK

Artikel ilmiah ini, akan memberikan gambaran tentang apakah resiko dan bagaimana pengamanan dalam electronic commerce (eCommerce). eCommerce merupakan satu set dinamis teknologi, aplikasi dan proses bisnis yang menghubungkan perusahaan, konsumen, dan komunitas tertentu melalui transaksi elektronik dan perdagangan barang, pelayanan, dan informasi yang dilakukan secara elektronik. Meskipun eCommerce merupakan sistem yang menguntungkan karena dapat mengurangi biaya transaksi bisnis dan dapat memperbaiki kualitas pelayanan kepada pelanggan, namun sistem eCommerce ini beserta semua infrastruktur pendukungnya mudah sekali disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab, dan bisa juga terkena kesalahan-kesalahan yang mungkin timbul melalui berbagai cara. Kerusakan hebat bisa terjadi pada semua elemen yang berkaitan dengan sistem ini baik itu dalam sistem perdagangan komersial, institusi finansial, service provider, bahkan konsumen sekalipun. Harus diakui, sesuatu yang dibuat oleh manusia itu memang tidak ada yang sempurna. Untuk itu perlu dikaji pengamanannya.

Kata Kunci : eCommerce, Resiko, Pengamanan.

PENDAHULUAN

Sebuah situs internet (*website)* secara otomatis dapat membawa sebuah perusahaan ke pasar global, tetapi tidak dapat dengan mudah merealisasikan atau mengkondusifkan bisnis perusahaan itu menjadi sebuah bisnis internasional. Karena banyak sekali faktor yang mempengaruhi, berhasil tidaknya sebuah bisnis internasional. Budaya, sistem bisnis, dan infrastruktur yang berbeda-beda di masing-masing negara membuat masalah pemasaran, penjualan, dan perkembangan hubungan bisnis menjadi semakin kompleks. Kekuatan internet untuk meningkatkan perdagangan global sudah tidak bisa dipungkiri lagi.

Dunia semakin canggih. Teknologi semakin berkembang. Perkembangan tersebut secara langsung maupun tidak langsung mempengaruhi sistem perdagangan, transaksi, dan peredaran uang manusia selama ini. Sebelumnya, transaksi secara tradisional dilakukan dan tangan ke tangan secara langsung, antara pembeli dan penjual bertatap muka, melakukan persetujuan, dan akhirnya terjadi kesepakatan. Namun kini, dengan adanya kecanggihan teknologi komputer, semua keterbatasan sarana, jarak, dan waktu transaksi dapat teratasi dengan mudah. Hanya dengan klik saja Kita bisa mendapatkan barang yang diinginkan, bisa mengetahui apa saja yang kita inginkan, dan dapat melakukan transaksi dengan siapa saja tanpa dibatasi oleh waktu dan jarak. Kemudahan inilah yang merupakan faktor utama berkembangnya *electronic commerce*, yang selanjutnya lebih populer ditulis *eCommerce*.

eCommerce menggambarkan cakupan yang luas mengenai teknologi, proses dan praktek yang dapat melakukan transaksi bisnis tanpa menggunakan kertas sebagai sarana mekanisme transaksi. Hal ini bisa dilakukan dengan berbagai cara seperti melalui *e-mail*, *electronic data interchange (EDI)*, atau bisa juga melalui *World Wide Web*. e*Commerce* ini juga meliputi transaksi di dalam dan di antara sektor bisnis yang khusus dan umum, serta sistem yang melibatkan komunitas dalam negeri maupun internasional.

Dalam dunia modern ini, *eCommerce* telah memberikan pengaruh yang besar terhadap pertumbuhan tata sosial dan ekonomi masyarakat. e*Commerce* telah menjadi bagian yang penting dari sektor bisnis khusus dan umum. Hal ini memang diakui karena dengan adanya e*Commerce* ini, biaya operasional bisa dikurangi agar bisa bersaing dan berjuang dengan semakin banyaknya permintaan yang mengharuskan pelayanan yang cepat dan akurat. Ini merupakan gejala perkembangan informasi sosial yang bertambah pesat. (Raharjo, 1998).

Kenyataannya, *eCommerce* tidak hanya menjadi mekanisme yang tepat dan membutuhkan biaya yang murah untuk diterapkan, tetapi juga akan menjadi sebuah sistem sosial yang dapat diterima dan dapat diharapkan untuk digunakan. e*Commerce* demikian gencar dibicarakan dimana-mana. Kebutuhan akan pengetahuan global tentang *eCommerce* menjadi menarik dan penting bagi pemula yang berkeinginan untuk terjun dan menggeluti bidang ini.

Memang artikel ilmiah ini tidak diarahkan untuk memberikan gambaran lengkap tentang *eCommerce*. Tulisan ini lebih diarahkan untuk memberikan gambaran secara umum, resiko apa saja yang ada dan bagaimana pengamanan *eCommerce*.

Permasalahan dalam artikel ilmiah ini adalah, apakah resiko dan bagaimana pengamanan dalam *electronic commerce*?.

Tujuan penulisan artikel ilmiah ini adalah memberikan gambaran terhadap resiko e*Commerce* dan memberikan petunjuk pengamanan *eCommerce*.

Manfaat penulisan artikel ilmiah ini adalah menyumbangkan pengetahuan sekilas tentang *eCommerce* yang berkembang pesat di dalam masyarakat.

Data dikumpulkan dengan melakukan studi perpustakaan, yaitu menggali dan menelusuri pengetahuan melalui buku pelajaran, majalah dan menjelajah situs internet, untuk membahas kajian ilmiah ini.

TINJAUAN PUSTAKA

Electronic commerce (*eCommerce*) merupakan satu set dinamis teknologi, aplikasi dan proses bisnis yang menghubungkan perusahaan, konsumen, dan komunitas tertentu melalui transaksi elektronik dan perdagangan barang, pelayanan, dan informasi yang dilakukan secara elektronik. (Purbo dan Wahyudi, 2000)

eCommerce menggambarkan cakupan yang luas mengenai teknologi, proses, dan praktek yang dapat melakukan transaksi bisnis tanpa menggunakan kertas sebagai sarana mekanisme transaksi. Hal ini bisa dilakukan dengan berbagai cara seperti melalui *e-mail, Electronic Data Interchange* (EDI), atau bisa juga melalui *World Wide Web* (situs di internet), *Electronic Commerce* ini juga meliputi transaksi di dalam dan di antara sektor bisnis yang khusus (*private*) dan umum (*public*), serta sistem yang melibatkan komunitas dalam negeri maupun internasional.

Dalam dunia modern ini, *eCcommerce* telah memberikan pengaruh yang besar terhadap pertumbuhan tata sosial dan ekonomi masyarakat. e*Commerce* telah menjadi bagian yang penting dari sektor bisnis khusus (*private*) dan umum (*public*). Keberadaan e*Commerce* ini, dapat mengurangi biaya operasional agar bisa bersaing dan berjuang dalam situasi yang mengharuskan pelayanan yang cepat dan akurat. Hal ini merupakan gejala perkembangan informasi sosial yang bertambah pesat. e*Commerce* tidak hanya mejadi mekanisme yang tepat dan membutuhkan biaya yang murah untuk diterapkan, tetapi juga akan menjadi sebuah sistem sosial yang dapat diterima dan bermanfaat.

Jenis *Electronic Commerce*

Secara umum kita bisa mengklasifikasikan *eCommerce* menjadi 2 (dua) jenis yaitu, *Business to Business* dan *Business to Consumer*.

Business to Business, karakteristiknya adalah: (Purbo dan Wahyudi, 2000), pertama *trading partners* yang sudah saling mengetahui diantara mereka sudah terjalin hubungan yang berlangsung cukup lama. Pertukaran informasi hanya berlangsung di antara mereka dan karena sudah sangat mengenal, maka pertukaran informasi tersebut dilakukan atas dasar kebutuhan dan kepercayaan. Kedua, pertukaran data dilakukan secara berulang dan berkala dengan format data yang telah disepakati. Jadi jasa yang digunakan antar kedua sistem tersebut sama dan menggunakan standar yang sama pula. Ketiga, Salah satu pelaku tidak harus menunggu partner mereka lainnya untuk mengirimkan data. Keempat, model yang umum digunakan ada *peer-to-peer*, di mana *processing intelligence* dapat didistribusikan di kedua pelaku bisnis.

Business to Consumer karakteristiknya adalah: (Purbo dan Wahyudi, 2000), pertama, terbuka untuk umum, dimana informasi disebarkan secara umum pula. Kedua, jasa yang dilakukan juga bersifat umum, sehingga mekanismenya dapat digunakan oleh orang banyak. Sebagai contoh, karena sistem web sudah umum di kalangan masyarakat make sistem yang digunakan adalah sistem web pula. Ketiga, jasa yang diberikan adalah berdasarkan pemintaan konsumen berinisiatif, sedangkan produsen harus siap memberikan respon terhadap inisiatif konsumen tersebut. Keempat, sering dilakukan sistem pendekatan *client-server*, di mana konsumen di pihak *client* menggunakan sistem yang minimal (berbasis web) dan penyedia barang/jasa *(business procedure*) berada pada pihak server.

Kegiatan yang Berhubungan dengan e*Commerce*

Teknologi semakin berkembang, sehingga perkembangan tersebut secara langsung maupun tidak langsung mempengaruhi sistem perdagangan dan transaksi selama ini Sebelumnya, transaksi secara tradisional dilakukan dan tangan ke tangan secara langsung, antara pembeli dan penjual bertatap muka, melakukan persetujuan, dan akhimya terjadi kesepakatan. Namun kini, dengan adanya kecanggihan teknologi komputer, semua keterbatasan sarana, jarak, dan waktu transaksi dapat teratasi dengan mudah. Hanya dengan klik saja kita bisa mendapatkan barang yang diinginkan, bisa mengetahui apa saja yang kita inginkan, dan dapat melakukan transaksi dengan siapa saja tanpa dibatasi oleh waktu dan jarak. Kemudahan inilah yang menjadi faktor utama berkembangnya *eCommerce*.

Banyak sekali yang bisa dilakukan melalui *eCommerce*. Namun pada umumnya orang menganggap *eCommerce* sebagai kegiatan seperti kita membeli sebuah buku di toko *online*. *eCommerce* lebih luas dari dari hal itu, ketepatan, kemudahan, dan kecepatan menjadi ciri kegiatan e*Commerce*.

Hal-hal bisa dilakukan didalam *eCommerce*, antara lain: (Andriana, 2003) pertama, perdagangan online melalui *world wide web* (*personal computer*) merupakan contoh yang paling gampang dan umum diketahui orang. Kedua, transaksi *online* bisnis antar perusahaan. Ketiga, internet bank yang saat ini sedang berkembang di Indonesia dimana kita dapat memeriksa lewat internet berapa saldo kita, mengganti nomor PIN ATM kita, transfer antar rekening, dan berbagai macam kemudahan sistem pembayaran tagihan lainnya. Semua itu dikembangkan tidak lain hanya untuk memudahkan manusia dalam menjalankan aktivitas sehari-harinya yang semakin padat dan sibuk. Keempat, televisi interaktif dimana melalui televisi kita bisa melihat daftar acara secara interaktif Internet lewat TV, dan akses *web* lewat TV yang berkembang pesat di Eropa. Keempat, *WAP* (*Wireless Applivation Protocol*), melalui Handphone kita dapat melakukan segala macam transaksi kita inginkan. Mulai dari pembelian tiket pesawat terbang, memesan makanan di restoran dan sebagainya. Semua itu dilakukan hanya dalam sekejap dan tidak mengharuskan kita duduk di depan komputer yang terhubung dengan Internet. Bisa-bisa, berdasarkan fakta yang menunjukkan bahwa penetrasi *Personal Computer* (PC) yang terhubung ke internet masih kecil dan biaya yang dibutuhkan masih relatif lebih mahal, maka telepon selular akan menjadi sarana sistem belanja online yang relatif lebih murah dan efisien jika dibandingkan dengan PC.

PEMBAHASAN

Resiko e*Commerce*

Dari segi pandangan bisnis resiko yang dapat timbul terdiri atas: Pertama, kehilangan segi finansial secara langsung karena kecurangan. Seseorang atau scorang penipu yang berasal dari dalam atau dari luar mentransfer sejumlah uang dari rekening yang satu ke rekening yang lainnya atau dia telah menghancurkan, menganti semua data finansial yang ada. Kedua, pencurian informasi rahasia yang berharga. Pada umumnya banyak organisasi maupun lembaga-lembaga yang menyimpan data rahasia yang sangat penting bagi kelangsungan hidup mereka. Misalnya, kepemilikan teknologi atau informasi pemasaran maupun informasi yang berhubungan dengan kepentingan konsumen/*client* mereka. Gangguan yang timbul bisa menyingkap semua informasi rahasia tersebut kepada pihak-pihak yang tidak berhak dan dapat mengakibatkan kerugian yang besar bagi si korban. Ketiga, kehilangan kesempatan bisnis karena gangguan pelayanan. Bergantung pada pelayanan elektonik dapat mengakibatkan gangguan selama periode waktu yang tidak dapat diperkirakan. Kesalahan ini bersifat kesalahan yang nonteknis, seperti aliran listrik tiba-tiba padam, atau jenis gangguan tak terduga lainnya. Keempat, penggunaan akses ke sumber oleh pihak yang tidak berhak. Pihak luar mendapatkan akses yang sebenarnya bukan menjadi haknya dan dia gunakan hal itu untuk kepentingan pribadi. Misalnya, seorang *hacker* yang berhasil membobol sebuah sistem perbankan. Setelah itu, dengan seenaknya sendiri dia memindahkan sejumlah rekening orang lain ke dalam rekeningnya sendiri. Kelima, kehilangan kepercayaan dari para konsumen. Kepercayaan konsumen terhadap sebuah perusahaan/ lembaga/institusi tertentu dapat hilang karena berbagai macam faktor, seperti usaha yang dilakukan dengan sengaja oleh pihak lain yang berusaha menjatuhkan kesalahan-kesalahan fatal yang dilakukan oleh perusahaan itu yang mengakibatkan kepercayaan konsumen berkurang. Keenam, Kerugian-kerugian yang tidak terduga. Gangguan terhadap transaksi bisnis, yang disebabkan oleh gangguan dari luar yang dilakukan dengan sengaja, ketidakjujuran, praktek bisnis yang tidak benar, kesalahan faktor manusia, atau kesa-lahan sistem elektronik, mengakibatkan kerugian transaksi bisnis yang tidak bisa dihindarkan. Terutama dari segi finansial, sebagai contohnya, konfirmasi sebuah transaksi tidak diterima dengan baik seperti sebagaimana mestinya. Kehilangan kesempatan bisnis, hilangnya kredibilitas dan reputasi, dan kerugian biaya yang besar merupakan resiko yang sewaktu-waktu bisa saja terjadi, namun kita harus siap-siap mengantisipasi atau mencegahnya.

Pengamanan e*Commerce*

Sistem Pengamanan *eCommerce* memiliki empat macam tujuan yang sangat mendasar, yaitu: pertama, *confidentiality*. Menjamin apakah informasi yang dikirim tersebut tidak dapat dibuka atau tidak dapat diketahui oleh orang lain yang tidak berhak. Memang, untuk data yang teramat penting, dibutuhkan sekali tingkat kerahasiaan yang tinggi, yang hanya bisa diakses oleh orang-orang tertentu saja (orang-orang yang berhak). Kedua, integritas. Menjamin konsistensi data tersebut apakah dia itu masih utuh sesuai aslinya atau tidak (palsu atau tidak), sehingga upaya orang-orang yang tidak bertanggung jawab untuk melakukan penduplikatan dan perusakan data bisa dihindari. Keempat, pengggunaan. Menjamin pengguna yang sah agar bisa mengakses informasi dan sumber miliknya sendiri. Jadi tujuannya adalah untuk memastikan bahwa orang-orang yang memang berhak tidak ditolak untuk mengakses informasi yang memang menjadi haknya. Kelima, legitimasi Pengguna. Menjamin kepastian bahwa sumber tidak digunakan (informasi tidak diakses)

oleh orang-orang yang tidak bertanggung jawab (orang-orang yang tidak berhak).

Pada penerapan teknologi yang sebenarnya, bidang-bidang utama yang digunakan untuk mencapai tujuan-tujuan tadi adalah sistem keamanan komunikasi (*communications security*) dan keamanan komputer (*computer security*). Keamanan komunikasi merupakan perlindungan terhadap informasi ketika dia dikirim dari sebuah sistem ke sistem lainnya. Keamanan komputer adalah perlindungan terhadap sistem informasi komputer itu sendiri, seperti keamanan pada perangkat lunak sistem operasi komputer dan keamanan terhadap perangkat lunak manajemen database komputer.

Namun dua kategori keamanan tersebut harus bisa digabungkan dengan faktor keamanan lainnya dan kita tidak boleh mengabaikannya. Menurut Jogianto H.M., dalam bukunya Pengenalan Komputer, ada beberapa faktor pengamanan yang perlu diperhatikan, seperti: pertama, keamanan secara fisik. Keamanan sistem fisik di sekitar kita, seperti pengamanan oleh penjaga keamanan, pintu yang terkunci, sistem kontrol fisik lainnya, dan sebagainya. Kedua, keamanan Personal. Sistem keamanan ini meliputi kepribadian orang-orang yang mengoperasikan atau memiliki hubungan langsung dengan sistem tersebut. Dalam hal ini kesadaran pribadi orang yang bersangkutan harus tinggi. Ketiga, keamanan administrative. Keamanan pada bidang tersebut adalah mengadakan kontrol terhadap perangkat-perangkat lunak yang dipakai, mengecek kembali semua kejadian-kejadian yang telah diperiksa sebelumnya, dan sebagainya. Keempat, keamanan media yang digunakan. Media *security* meliputi pengontrolan terhadap media penyimpanan yang ada dan menjamin bahwa media penyimpanan yang mengandung informasi sensitif tersebut tidak mudah hilang begitu saja.

Dalam membangun sebuah jaringan komputer (sebuah sistem) yang aman, maka kita juga harus mempelajari berbagai macam bentuk Ancaman yang mungkin timbul. Semuanya harus diketahui dan dipelajari dengan sebaik-baiknya agar segala investasi dan sumber daya informasi yang dimiliki dapat dilindungi atau diamankan secara efektif dan efisien. Ada beberapa macam bentuk ancaman yang bisa saja mengganggu atau bahkan membahayakan sistem informasi kita, antara lain: pertama, penetrasi ke Sistem. Orang-orang yang tidak berhak, mendapatkan akses ke sistem komputer dan diperbolehkan melakukan segala sesuatau sesuai dengan keinginannya, seperti memodifikasi file-file, mencuri informasi penting, dan penggunaan sumber-sumber atau aplikasi-aplikasi berharga lainnya yang terdapat dalam sistem tersebut. Bentuk-bentuk penetrasi ini bermacam-macam. Ada penyusup yang dengan segala upaya agar tampak seperti user yang sah, melakukan sesuatu dan masuk kesebuah sistem seperti layaknya user-user yang berhak lainnya. Ada pula yang berupa pengeksploitasian sistem yang diakibatkan karena memang sistem itu lemah, contoh mudahnya adalah seseorang yang berhasil memotong (*bypass*) prosedur untuk masuk. Kedua, penyalahgunaan wewenang. Ancaman bisa saja berupa pelanggaran atau penyalahgunaan wewenang legal yang dimiliki oleh seseorang yang berhak. Seseorang yang berhak mengakses sebuah sistem untuk tujuan tertentu bisa saja menyalahgunakan wewenangnya untuk memasuki sistem lain yang bukan menjadi haknya. Ketiga, planting. Gambarannya adalah sebagai berikut, bisa saja seseorang yang berniat melakukan serangan kedalam sebuah sistem tidak dilakukannya secara langsung, namun serangan yang akan dilakukan berupa serangan di masa yang akan datang. Secara diam-diam dia memasukkan sesuatu ke dalam sesuatu yang telah dianggap legal oleh sebuah sistem, namun dimasa yang akan datang sesuatu yang sebenarnya tidak legal tersebut, yang secara diam-diam bersembunyi di dalam hal lain yang legal itu, melakukan serangan uang mengejutkan. Contohnya adalah *Trojan Horse*. Keempat, pemantauan komunikasi. Tanpa melakukan penetrasi ke dalam sebuah sistem komputer, para penyerang bisa saja memantau atau memonitor semua informasi rahasia hanya dengan melakukan Pemantauan komunikasi sederhana di sebuah tempat pada sebuah jaringan komunikasi. Kelima, communication tampering. Tanpa melakukan penetrasi, para penyerang juga bisa melakukan hal-hal yang membahayakan kerahasiaan informasi kita. Misalnya saja dengan mengubah informasi transaksi di tengah jalan pada sebuah jaringan komunikasi. Bisa juga dengan membuat sebuah sistem *server* gadungan yang mungkin saja menipu user-user tertentu sehingga mereka dengan sukarela memberikan semua informasi rahasia yang dimilikinya (misalnya *username* dan *password* mereka). Keenam, menghalangi orang lain. User-user berhak,yang ingin mengakses informasi, sumber dan fasilitas-fasilitas lainnya bisa saja dihalang-halangi dengan sengaja.ini juga merupakan gangguan. Sebagai contoh, *port* untuk mengakses service tertentu dengan sengaja dibebani, sehingga service terhadap user lain dihalangi atau bisa juga dengan membanjiri internet *address* dengan paket-paket yang besar. Keenam, penolakan. Penolakan terhadap sebuah aktivitas transaksi atau sebuah komunikasi yang terjadi bisa saja dikarenakan sesuatu yang bersifat sengaja, kecelakaan, ataupun kesalahan teknis lainnya. Ini juga merupakan bentuk ancaman yang harus dipelajari dan tidak bolah diremekan begitu saja.

Ada beberapa hal yang dapat dilakukan dalam mengamankan sistem Komputer dan sistem

komunikasi, yaitu: pertama, mencegah munculnya ancaman di atas sebelum benar-benar terealisasi. Kedua, meminimalisasikan kemungkinan terjadinya ancaman tersebut. Ketiga, mengurangi akibat yang timbul karena ancaman yang sudah terealisasi.

Pada sistem keaman komunikasi dan keamanan komputer, menurut Onno W. Purbo dan Aang Arif Wahyudi dalam bukunya Mengenal *eCommerce*, ada lima bentuk utama jasa Pengamanan, yaitu antara lain: pertama, authentication services. Jasa ini memberikan kepastian identitas pengguna. Ketika seseorang ada atau sesuatu mengkliam sebuah identitas tertentu, maka *authentication services* ini yang memberikan konfirmasi bahwa klaim tersebut adalah sah. Ada dua macam jenis authentication services yaitu: *Entity authentication dan Data origin authentication*. *Entity authentication di*anggap sebagai pintu gerbang yang digunakan dalam rangka menunjukan sahnya identitas dalam sebuah konisi yang terjadi. *pasword* adalah contoh yang paling mudah dalam jenis *authentication services* ini. *Data origin authentication*, membutikan sah atau tidaknya identitas yang diklaim tersebut, misalnya dalam bentuk pesan tertulis. Kedua, *Access Control Services*. Jasa ini bertujuan untuk melindungi semua fasilitas dan sumber-sumber yang ada dari akses-akses yang tidak berhak. Pengaksesan tidak berhak bisa saja meliputi penggunaan yang tidak berhak, pembokaran informasi rahasia, pemodifikasian, perusakan dan pemberian perintah yang dilakukan oleh akses ilegal. *Access control services* ini merupakan bagian utama yang melaksanakan sistem *authorization* (otorisasi). Kedua, *Confidentiality Services*. Jasa ini memberikan perlindungan terhadap informasi yang berusaha disingkap oleh orang lain yang tidak berhak, yang berusaha untuk mendapatkan informasi tersebut secara umum servis ini bisa digambarkan dalam bentuk upaya untuk menyembunyikan sesuatu yang berisi informasi berharga.sebagai contohnya adalah enkripsi. Ketiga, Data *Integrity Service*. Jasa ini berupa perlindungan terhadap ancaman yang dapat mengubah data item seandainya ini terjadi didalam *security policy*. Pengubahan data ini bisa saja meliputi penyisipan data, dan modifikasi data. *Data integrity services* ini juga berfungsi untuk memberikan perlindungan seandainya terjadi pembuatan atau penghapusan data item tanpa melaui otirisasi. Keempat, *Non-Repudiation Services*. Jasa ini secara fundametal berbeda dengan jenis-jenis jasa pengamanan lainnya. Jasa ini utamanya ditujukan untuk melindungi user melawan ancaman yang berasal dari user berhak lainnya. Ancaman tersebut dapat berupa kesalahan penolakan ketika transaksi atau komunikasi sedang terjadi. Untuk mempermudah pemahaman bentuk ancaman tersebut, kita lihat contoh berikut ini: pertama, penerima mengklaim bahwa dia menerima pesan tetapi sipengirim mengklaim bahwa dia tidak mengirim pesan. Kedua, penerima mengklaim bahwa dia menerima pesan yang berbeda dengan apa yang klaim oleh sipengirim. Ketiga, penerima menerima pesan dengan data tanggal dan waktu tertentu, tetapi sipengirimnya tidak mengakui data tanggal dan waktu yang diklaim tersebut.

Berdasarkan uraian diatas, terlihat bahwa sistem pengamanan benar-benar sangat diperlukan untuk menghindari hal-hal yang tidak diinginkan, khususnya pada pelaksanaan *eCommerce* yang penuh dengan transaksi yang melibatkan finansial.

KESIMPULAN DAN SARAN

Kesimpulan

Pertama, Resiko *eCommerce* dapat dibagi menjadi resiko akibat penyalahgunaan dan resiko akibat kegagalan sistem, yang keduanya dapat menimbulkan kerugian. Kedua, Pengamanan *eCommerce* meliputi segala aspek atau bidang disiplin keamanan yang beraneka ragam, antara lain sistem keamanan komunikasi, keamanan komputer, keamanan dari segi fisik, keamanan individu yang terlibat, keamanan secara administratif, dan keamanan media yang digunakan.

Saran

Walaupun *eCommerce* telah berkembang pesat di dalam kehidupan masyarakat, namun untuk melakukan atau menyusun kegiatan *eCommerce* tidaklah mudah. Kita perlu mempertimbangkan resiko yang mungkin timbul dan pengamanannya, sehingga keuntungan akan dapat diraih.

DAFTAR PUSTAKA

Budi Raharjo. 1998. *Keamanan Sistem informasi berbasis Internet*. Bandung: PT Insan Indonesia.

Budi Raharjo. 1998. *Mengimplementasikan Electronic Commerce di Indonesia*. Bandung: PT Insan Indonesia.

Dian Andriana. 2003. *Pengenalan Pemrograman eCommerce dengan PHP dan MySQL*. Jakarta: Ilmu Komputer.com.

Jogianto H.M. 1999. *Pengenalan Komputer*. Jakarta: PT. Elex Media Komputindo.

Onno W. Purbo dan Aang Arif Wahyudi. 2000. *Mengenal eCommerce*. Jakarta PT. Elex Media Komputindo.