TEKNOLOGI SEKURITAS E-COMMERCE

Ekabrata Yudhistyra

Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI
Jl. Ir. H. Juanda 96 Bandung 40132

ABSTRAK

E-commerce merupakan bagian dari *e-business* yang mengkolaborasikan mitra bsinis, pelayanan nasabah, lowongan pekerjaan, dan lain-lain. Saat ini banyak perusahaan yang mengalihkan usahanya menjadi usaha berbasis internet (*e-commerce*) dengan pertimbangan melalui *e-commerce* ini pemasaran dan penjualan produk tidak akan terbatasi lagi oleh jarak, ruang, dan waktu. Untuk mengelola suatu usaha di internet, diperlukan teknologi basis data, surat elektronik, dan satu faktor penting yaitu peranan EDI (*Electronic Data Interchange*) untuk melakukan pertukaran data secara elektronik.

E-commerce juga memberikan kemudahan bagi konsumen untuk melakukan transaksi penjualan maupun pembelian, konsumen dapat membeli produk secara *on line* dan pembayaran dapat dilakukan baik dengan transfer dana maupun melalui kartu kredit.

Pada awalnya banyak terjadi kecurangan dalam bertransaksi on-line, diantaranya pencurian data dan informasi serta seringnya penyalah gunaan kartu kredit dalam melakukan transaksi pembayaran. Tetapi saat ini masyarakat luas tidak perlu khawatir lagi bertransaksi melalui internet karena teknologi sekuritas sudah dapat ditingkatkan dan terlebih lagi pemerintah khususnya pemerintah Indonesia sudah mengeluarkan UU ITE yaitu Undang-undang Informasi dan Transaksi Elektronik (dikeluarkan pada tahun 2008) yang mengatur berbagai perlindungan hukum atas seluruh kegiatan yang memanfaatkan internet sebagai medianya, baik untuk transaksi maupun untuk pemanfaatan informasinya guna memberikan kepastian hukum bagi penggunanya.

Kata-kata kunci: *e-commerce*, sekuritas, transaksi elektronik, internet

1. PENDAHLUAN

E-commerce atau perdagangan elektronik melibatkan transfer dana secara elektronik, pertukaran data elektronik, sistem manajemen persediaan otomatis, dan sistem pengumpulan data otomatis.

Karakteristik pengaksesan data dalam suatu jaringan atau network dalam melaksanan *e-commerce* adalah:

1. Identifikasi yang unik untuk setiap komputer di jaringan, maksudnya adalah setiap komputer diidentifikasikan secara unik dan ditangani dengan IP *address* secara spesifikasi.
2. Pengalamatan yang mudah

   DNS (*Domain Name System*) memberikan alamat jaringan yang mudah digunakan untuk mengelola kata dan tulisan di dalam IP *address*.
3. Paket Switching

   Untuk memperbaiki hal-hal yang tertunda seperti ukuran data yang ditransfer tidak sama, pengiriman data, file yang rusak dalam paket data sebelum dikirim melalui jaringan.
4. Routing

   Router melayani antar *network* dan membangun blok di internet.
5. Reliabilitas dan Protokol Pengendalian Transmisi (*Reliability* and TCP)

   IP *Software* menangani pengiriman paket dan TCP menangani keamanan pengiriman paket.
6. Standarisasi

   Tanpa standarisasi TCP/IP, ada beberapa kelemahan seperti tidak fleksibel dan peningkatan fungsional serta biaya.

Dengan melaksanakan *e-commerce* ada beberapa kelemahan terutama di bidang keamanan, diantaranya:

1. Lebih banyak potensi penyerang sebab internet mengijinkan suatu situs web (*website*) diakses dengan basis yang lebih luas bagi pelanggan dan masyarkat luas.
2. Skala kejahatan lebih tinggi, banyak potensi perusaknya.
3. Pembayaran dengan kartu kredit sering disalahgunakan oleh pihak luar. Jika seseorang telah memasukkan nomor dari kartu kredit maka orang lain dapat menggunakannya kembali tanpa sepengetahuan dari si pemegang kartu.

4. Penipuan dengan cara pencurian identitas dan membohongi pelanggan, yang disebabkan karena kurangnya hukum dalam bidang *e-commerce* ini.

Untuk mengendalikan dan terhindar dari kejahatan bertransaksi melalui internet, ada beberapa cara yang dapat dilakukan diantaranya adalah:

1. Meningkatkan teknologi sekuritas dalam bertransaksi
2. Mendaftarkan usahanya kepada Badan Pengawasan dan Pengendalian Certification Authority (CA)

2. TEKNOLOGI SEKURITAS E-COMMERCE

Teknologi dapat digunakan untuk membantu mengurangi resiko perusahaan dan pelanggannya ketika melakukan transaksi *e-commerce*. Beberapa hal yang dapat dilakukan adalah:

1. *Password*

   Yaitu identifikasi siapa yang mencoba mengakses sebuah situs *web*. Untuk membuat *password,* pilihlah karakter yang mudah diingat oleh diri sendiri tetapi tidak mudah ditebak oleh orang lain. Dianjurkan menggunakan *password* yang berbeda untuk setiap jaringan atau *station, password* diubah setiap jangka waktu tertentu.

2. Enkripsi

   Yaitu proses mengacak data sehingga tidak dapat dibaca oleh pihak lain. Pada umumnya, harus disertakan sebuah kunci sehingga data yang dienkripsi dapat didekripsikan kembali. Ilmu yang mempelajari teknik enkripsi disebut kriptografi. Contohnya adalah mengganti huruf b dengan m, huruf g dengan s dan seterusnya. Program yang banyak dipergunakan sampai saat ini adalah ROT-13 yang mengubah huruf menjadi 23 huruf didepannya. Misalnya b menjadi o dan seterusnya. Pembahasan enkripsi akan terfokus pada enkripsi password dan enkripsi komunikasi data.

3. *Public Key Infrastructure*

   Yaitu suatu perangkat lunak enkripsi yang menggunakan beberapa bagian dalam *software* tambahan yang disebut kunci untuk meyakinkan bahwa hanya pembuat dan penerima yang diijinkan untuk mengaksesnya. PKI merupakan kumpulan perangkat keras, perangkat lunak, orang, kebijakan dan prosedur yang dibutuhkan untuk menciptakan, mengatur, mendistribusikan, menggunakan, dan menyimpan.

Identifikasi pengguna haruslah unik untuk setiap daerah/batasan (*domain*) dari CA (*Certificate Authority*).

4. *Screening routers*

   Yaitu dapat mencetak paket dan perbedaannya, tidak hanya apa yang dapat mereka ikut sertakan pada paket tersebut tapi juga apa yang harus mereka ikutsertakan. *Screening routers* digunakan juga sebagai sebuah *firewall*. Pada banyak kasus, suatu *screening router* tunggal digunakan sebagai seluruh solusi *firewall*.

5. *Proxy servers*

   Tujuan utamanya adalah melewatkan paket pada suatu sisi jaringan internal di internet.

6. *Firewalls*

   Firewall atau tembok api merupakan suatu sistem yang memperbolehkan lalu lintas jaringan yang dianggap aman untuk dilalui. Biasanya *firewall* ini diterapkan di suatu mesin yang terdeteksi yang berjalan pada pintu *gateway* (pintu gerbang) antara jaringan lokal dengan jaringan lainnya. *Firewall* ini dimanfaatkan untuk mengendalikan kontrol terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dan jaringan lainnya. Singkatnya, *firewall* ini merupakan suatu sistem yang mengatur komunikasi antar dua jaringan yang berbeda.

   Fungsi *firewall*:

   a. Mengatur dan mengontrol lalu lintas jaringan
   b. Melakukan autentikasi terhadap akses
   c. Melindungi sumber daya dalam jaringan privat
   d. Mencatat semua kejadian, dan melaporkan kepada administrator

7. *Digital signature authentication*

   Yaitu pengesahan atau otentikasi digital misalnya *finger print*. Suatu tanda tangan digital bergantung pada tipe enkripsi yang berbeda.

   Banyak cara yang dapat digunakan untuk proses otentikasi ini. Cara yang pertama adalah data dapat dienkripsi dengan pemaksaan dari nama *user* dan *password*-nya. Selanjutnya adalah memeriksa apakah data yang dimasukkan tadi valid atau invalid. Metode sinyal digital lain menggunakan sertifikasi digital, tetapi itu tidaklah mudah untuk diterapkan pada suatu enkripsi umum dalam skala yang besar. Itu alasannya mengapa sertifikasi digital digunakan. Sertifikasi digital

merupakan bagian dari informasi yang menempatkan *web server* dipercaya oleh CA. Metode *signature digital* lainnya adalah:

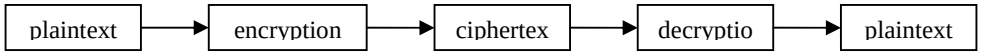
a. Penggunaan dari *Cyclic Redundancy Check* (Pemeriksaan redundansi berulang)
b. *The private key encryption* (enkripsi kunci pribadi)
c. *The private key encryption* (enkripsi kunci umum/publik)

8. Enkripsi

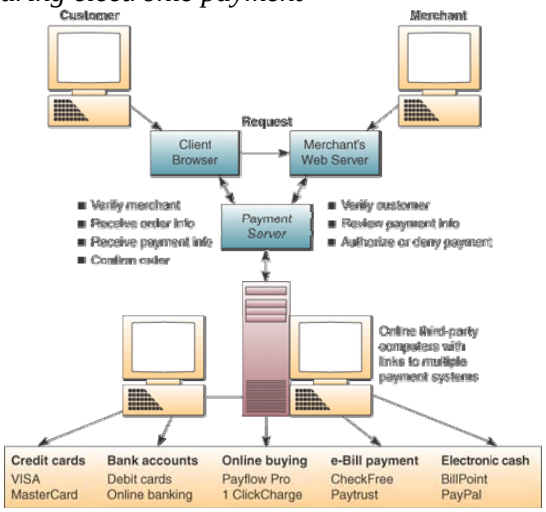
Enkripsi ini dilakukan oleh masing-masing pihak yang memiliki sepasang kunci/*key*, yaitu:

a. kunci publik (dapat diketahui oleh orang lain)
b. kunci privat (hanya diketahui diri sendiri)

Enkripsi ini membangun satu sistem yang dikenal dengan *Public Key Infrastructure* (PKI)



9. *Securing electronic payment*



Network sniffers merupakan perangkat lunak yang dapat mengenali dan mencegat format nomor kartu kredit.

Cara Penanggulangannya :

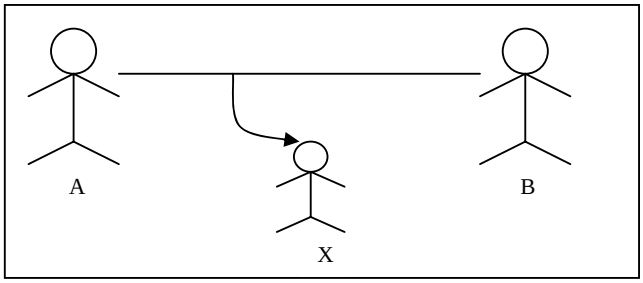
a. Enkripsi data antara penjual dan pembeli
b. Enkripsi kartu kredit
c. Informasi yang penting dilakukan secara *off-line*

Ada empat kriteria keamanan informasi dan transaksi bisnis elektronik, yaitu:

1. Kerahasiaan (*confidentiality*)

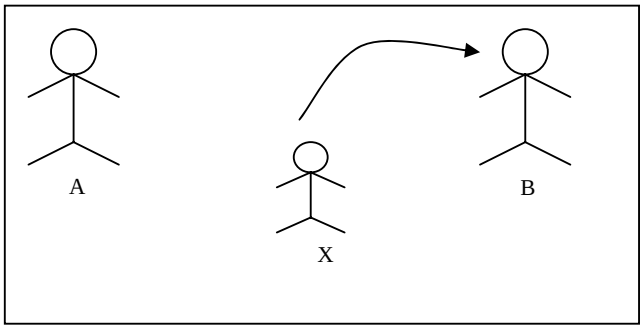
   Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka atau mengupas informasi yang telah disandi.

   Ancaman yang mungkin mengancam kerahasiaan ini adalah penyadapan, pencurian arsip atau bukti transaksi, pengaksesan oleh pihak yang tidak berwenang.



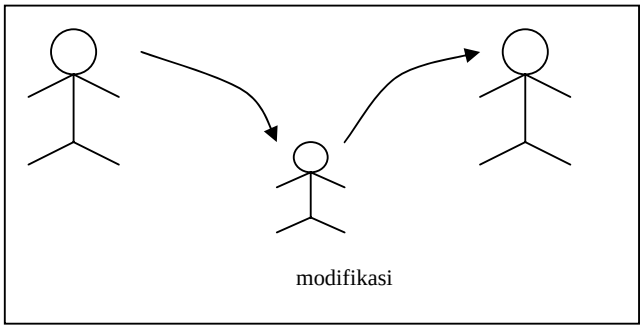
2. Otentitas (*authenticity*)

   Autentikasi, adalah berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain. Ancamannya adalah terjadinya pemalsuan identitas oleh pihak lain.



3. Integritas (*integrity*)

   Integritas data berhubungan dengan penjagaan dari perubahan data yang dilakukan secara tidak sah. Agar integritas data terjamin, maka sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak. Ancaman yang mengganggu integritas data antara lain penyisipan, penghapusan, dan pensubstitusian data lain kedalam data yang sebenarnya.



4. Nir-sangkal (*non repudiation*)

   Maksudnya adalah pihak pengirim tidak dapat menyangkal telah mengirimkan informasi tertentu pada waktu tertentu. Ancamannya adalah pengirim dapat mudah menyangkal telah mengirimkan informasi tertentu.

Beberapa tips melakukan transaksi *on line* secara aman:

1. ***Secure Surfing***

   Dapat menangani *Secure Socket Layer* (SSL), yang merupakan suatu metode enkripsi yang dapat mengambil informasi pribadi yang dikirimkan melalui ruang *cyber*. SSL ini merupakan hal yang paling umum dan mudah dimanfaatkan untuk mengumpulkan data. Ada 2 cara untuk mengetahui apakah suatu situs menggunakan SSL atau tidak. Pada *Internet Explorer*, lihat di ujung kiri atas pada tampilan dimana kata ”*Address*” muncul. Pada *Netscape*, lihat di sebelah kanan sekitar tombol ”stop” yang menggunakan simbol ”X”.

   Contoh: https://www.google.com/

   Huruf “s” pada “http” menunjukkan penggunaan SSL dan ini merupakan salah satu sekuritas. Jika icon tidak terkunci, artinya halaman *web* tersebut tidak aman, tetapi jika berada pada keadaan aman, maka *lock* akan mudah ditutup.

   SSL adalah protokol berlapis, mengambil data untuk dikirimkan, dipecahkan kedalam blok-blok yang teratur, dikompres jika diperlukan, dienkripsi, dan hasilnya dikirimkan. Di tempat tujuan, data didekripsi, verifikasi, dekompres, dan disusun kembali. Hasilnya dikirimkan ke klien di atasnya. SSL hanya mengenkripsikan data yang dikirim lewat http. Cara kerja SSL dapat digambarkan sebagai berikut :

   a. Pada saat koneksi mulai berjalan, klien dan server membuat dan mempertukarkan kunci rahasia, yang dipergunakan untuk mengenkripsi data yang akan dikomunikasikan. Meskipun sesi antara klien dan server diintip

pihak lain, namun data yang terlihat sulit untuk dibaca karena sudah dienkripsi.

b. SSL mendukung kriptografi *public key*, sehingga server dapat melakukan autentikasi dengan metode yang sudah dikenal umum seperti *RSA* dan *Digital Signature Standard (DSS)*.

c. SSL dapat melakukan verifikasi integritas sesi yang sedang berjalan dengan menggunakan algoritma *digest* seperti MD5 dan SHA. Hal ini menghindarkan pembajakan suatu sesi.

2. *Establishing Identity*

Suatu situs *web* yang menggunakan teknologi SSL, harus menunjukkan sertifikasi dari perusahaan tersebut yang memberikan identitasnya. Di Indonesia sekarang sudah ada badan sertifikasi. Konsumen dianjurkan untuk selalu melihat tanggal berlakunya sertifikasi tersebut, jika masih dalam batas waktu, maka situs tersebut aman digunakan.

3. ***Protecting Your Privacy***

Seseorang seharusnya mudah menentukan seberapa banyak dan bagaimana suatu perusahaan menggunakan informasi tentang diri orang tersebut. Jika sebuah perusahaan tidak secara terus terang menyebutkan dari mana dan bagaimana mereka mendapatkan data diri pribadi seseorang, maka berhati-hatilah. *Cookies* adalah sebuah tempat penyimpanan data yang kecil pada komputer yang mengijinkan perusahaan dapat menelusuri bagaimana sesorang anda dapat menjelajah situs mereka. Untuk perusahaan yang baik, maka tidak akan menggunakannya untuk menyimpan informasi identitas pribadi.

4. Returns and Customer Service

Jika suatu perusahaan *on line* yang reputasinya baik, maka mereka akan memberikan kebijakan-kebijakan yang masuk akal dan mudah untuk diketahui oleh masyarakat luas. Usahakan untuk selalu mencetak halaman *web* yang mengkonfirmasikan pesanan. Layanan pelanggan mudah dihubungi baik lewat telepon maupun lewat e-mail, lebih baik lagi jika keduanya mudah dilakuakn.

5. Legal Stuff

Lembaga keuangan maupun perusahaan kartu kredit memberikan jaminan dan dapat mempertanggung jawabkan atas seluruh transaksi, sebagai contohnya, selalu memberitahukan apakah suatu transaksi telah berhasil dilakukan atau tidak.

6. *Good Communication Goes Both Ways*

Anda harus memeriksa apakah seluruh pesanan dan informasi yang diberikan telah benar. Perusahaan yang baik akan memberitahukan jika ada data atau informasi yang salah. Jika sebuah perusahaan umumnya menggunakan SSL, dan memberikan kontak informasi secara jelas, kebijakan-kebijakan dan pernyataan-pernyataan personal, tentulah aman bertransaksi.

3. KESIMPULAN

Dengan berbagai teknologi yang semakin canggih, maka keamanan dalam bertransaksi di dunia maya tidak perlu dikawatirkan lagi.Saat ini banyak *software* yang memprioritaskan keamanan data dan jaraingan, bahkan pemerintah Indonesia sudah menerbitkan UUITE tahun 2008 yaitu Undang-undang Internet dan Transaksi Elektronik, didirikannya Badan Pengawasan dan Pengendalian yang mengatur pembuatan sertifikasi dan pengajuan akreditasi untuk perdagangan internet yang menjamin baik perusahaan maupun konsumen dalam melakukan transaksi jual beli.

4. DAFTAR PUSTAKA

[1]. Chaudhury, Abijit & Jean-Pierre Kuilboer (2002), *"e-Business and e-Commerce Infrastructure"*, McGraw-Hill, ISBN 0-07-247875-6

[2]. Kessler, M. (2003). "*More shoppers proceed to checkout online*". Retrieved January 13, 2004

[3]. Seybold, Pat (2001), *Customers.com*, Crown Business Books (Random House), ISBN 0-609-60772-3

[4]. http:/EzineArticles.com

[5]. http://www.go-digital.net/whitepapers/securecomm.html