KEAMANAN DALAM ELECTRONIC COMMERCE

Andre M. R. Wajong; Carolina Rizki Putri

Jurusan Teknik Industri, Fakultas Sains dan Teknologi, Bina Nusantara University
Jln. KH Syahdan No 9, Palmerah, Jakarta Barat 11480
awajong@binus.ac.id

ABSTRACT

The objective of this paper is to give information and understanding about security threat that could happen in security system in e-commerce. The approach used is how the transaction system is, how the security is applied, and also the possible security threat in e-commerce. The result of this research is that there are still gaps in e-commerce. It is hoped that the business actors will be more realized about the security importance and more aware about the possible threat.

Keywords: *e-commerce, security, threat*

ABSTRAK

Tujuan dari paper ini adalah memberikan informasi serta pemahaman mengenai ancaman keamanan yang dapat terjadi dalam sistem keamanan yang biasa digunakan dalam e-commerce. Pendekatan yang dilakukan adalah bagaimana sistem transaksi berlangsung, sistem keamanan yang diterapkan, serta ancaman keamanan yang mungkin terjadi pada E-Commerce. Hasil dari paper ini adalah masih banyak terdapat celah keamanan pada E-Commerce dan para pelaku bisnis E-Commerce diharapkan lebih sadar akan pentingnya keamanan serta lebih waspada terhadap ancaman yang mungkin terjadi.

Kata kunci: *e-commerce, keamanan, ancaman*

PENDAHULUAN

Latar Belakang

Bisnis lewat internet cukup menguntungkan, karena dengan menggunakan *internet*, produk usaha tidak hanya dapat dilihat di dalam kota, atau dalam negeri saja, melainkan lingkupnya mencapai lingkup nasional, bahkan internasional. Beberapa keuntungan juga ditawarkan dalam menjalankan bisnis lewat internet, seperti dikenalnya produk lebih luas lagi, efisiensi perusahaan meningkat, tidak dibatasi ruang dan waktu, dan lain sebagainya.

E-commerce merupakan bentuk perdagangan secara elektronik melalui media internet. Bisnis ini bisa berjalan selama 24 jam sehari, 7 hari seminggu, dan luas pangsa pasarnya menjangkau dari tingkat lokal hingga mancanegara. Dengan E-Commerce memungkinkan pelanggan bertransaksi dengan cepat dan biaya yang murah tanpa melalui proses yang berbelit-belit, di mana pihak pembeli cukup mengakses internet ke website perusahaan yang mengiklankan produknya di internet, yang kemudian pihak pembeli cukup mempelajari *term of condition* (ketentuan-ketentuan yang diisyaratkan) pihak penjual.

E-commerce selain memiliki sisi positif juga memiliki sisi negatif yaitu rawan tindak pidana kejahatan dunia maya (*cybercrime*) misalnya penipuan dengan cara pencurian identitas dan membohongi pelanggan, kejahatan kartu kredit, *phising*, *spammer*, dll. Ancaman akan keamanan tersebut akan mengakibatkan pelanggan takut melakukan transaksi dan kemudian kembali ke metode tradisional dalam melakukan bisnis. Masalah-masalah yang telah disebutkan akan dapat diantisipasi apabila sebelumnya telah terdapat kesadaran akan pentingnya keamanan oleh para pelaku bisnis E-Commerce.

Ruang Lingkup

Dalam penulisan paper ini, ruang lingkup pembahasannya mencakup penjelasan mengenai metode transaksi pada e-commerce, penjelasan mengenai penerapan sistem keamanan pada e-commerce, penjelasan mengenai ancaman keamanan yang mungkin terjadi pada e-commerce, dan contoh kasus bagaimana eBay sebagai e-commerce membantu keamanan para pelanggannya.

Tujuan dan Manfaat

Tujuan penulisan paper ini yaitu untuk memahami ancaman keamanan yang mungkin terjadi pada E-Commerce, serta memahami sistem keamanan yang biasa diterapkan pada E-Commerce. Selain itu, manfaat penulisan paper ini adalah agar pembaca memahami dan menyadari pentingnya keamanan pada E-Commerce.

METODE

Secara ringkas, metodologi dapat diartikan sebagai cara atau metode untuk mencapai tujuan. Metode penulisan yang digunakan dalam pembuatan paper ini adalah dengan mencari bahan dan informasi yang berhubungan dengan topik dari sumber-sumber literatur, baik dari buku, jurnal, maupun artikel-artikel dari situs.

PEMBAHASAN

Sistem Transaksi pada Website E-Commerce

Administrator melakukan manipulasi data di database menggunakan Admin Interface, yang merupakan halaman dimana administrator dapat menginputkan data, mengubah data, dan menghapus data, baik itu data mengenai shipping atau pengiriman barang, data produk atau jasa yang dijual, dan juga data mengenai informasi pembayaran.

Data pada database ini nanti berhubungan langsung dengan e-commerce website, produk yang ditampilkan diambil dari database, sedangkan data *shipping*, data *payment* dan validasinya menggunakan data *shipping* dan *payment*. Dari sisi client atau customer, pertama kali client melakukan penelusuran produk, kemudian memilih produk, dan membeli produk melalui e-commerce website. Setelah client setuju untuk melakukan pembayaran, maka data pembayaran disimpan dan kemudian data pengiriman pun juga disimpan, kemudian sampailah di sisi admin, dimana admin dapat melihat data transaksi terbaru lewat halaman administrator.

Dimensi dan Metode yang Digunakan pada Keamanan E-Commerce

Dua hal yang utama yang harus diperhatikan dalam melakukan transaksi adalah hal apa saja yang dibutuhkan dalam rangka menciptakan keamanan bertransaksi dan metode yang digunakan untuk menciptakan keamanan tersebut. Dimensi keamanan pada E-Commerce adalah: (1) autentikasi, pembeli, penjual, dan institusi pembayaran yang terlibat harus dipastikan identitasnya sebagai pihak yang berhak terlibat dalam transaksi tersebut, seperti pada Gambar 1; (2) integritas, jaminan bahwa data dan informasi yang di transfer pada e-commerce tetap utuh dan tidak mengalami perubahan; (3) non-repudiation, pelanggan membutuhkan perlindungan terhadap penyangkalan dari penjual bahwa barang telah dikirimkan atau pembayaran belum dilakukan. Dibutuhkan informasi untuk memastikan siapa pengirim dan penerimanya; (4) privasi, pelanggan menginginkan agar identitas mereka aman. Mereka tidak ingin orang lain mengetahui apa yang mereka beli; (5) keselamatan, pelanggan menginginkan jaminan bahwa aman untuk memberikan informasi nomer kartu kredit di internet.

Gambar 1 Alur Kerja Website E-Commerce

Selain itu, terdapat beberapa metode dan mekanisme yang dapat digunakan untuk memenuhi dimensi keamanan e-commerce diatas, yaitu:

Public Key Infrastructure (PKI)

Memungkinkan para pemakai yang pada dasarnya tidak aman di dalam jaringan publik seperti Internet, maka dengan PKI akan merasa aman dan secara pribadi menukar uang dan data melalui penggunaan suatu publik.

Public Key Algorithm

Disebut juga dengan algoritma asimetris (*Asymmetric Algorithm*) yaitu algorima yang menggunakan kunci yang berbeda pada saat melakukan enkripsi dan melakukan deskripsi.

Digital Signature

Tanda tangan digital merupakan tanda tangan yang dibuat secara elektronik, dengan jaminan yang lebih terhadap keamanan data dan keaslian data, baik jaminan tentang indentitas pengirim dan kebenaran dari data atau paket data terebut.

Certificate Digital

Sertifikat Otoritas merupakan pihak ke-tiga yang bisa dipercaya (Trust Thrid Party/TTP). Sertifikat Otoritas yang akan menghubungkan kunci dengan pemiliknya. TTP ini akan menerbitkan sertifikat yang berisi identitas seseorang dan juga kunci privat dari orang tersebut.

Secure Socket Layer (SSL)

Suatu protokol yang membuat sebuah pipa pelindung antara *browser cardholder* dengan *merchant*, sehingga pembajak atau penyerang tidak dapat menyadap atau membajak informasi yang mengalir pada pipa tersebut. Pada penggunaannya SSL digunakan bersaman dengan protokol lain, seperti HTTP (*Hyper Text Transfer Protocol*), dan *Sertificate Autority*.

Transport Layer Security (TLS)

Adalah protokol cryptographic yang menyediakan keamanan komunikasi pada Internet seperti e-mail, internet faxing, dan perpindahan data lain.

Secure Electronic Transaction (SET)

Merupakan *gabungan antara teknologi public/private key dengan digital signature*. Pada enkripsi, public key menggunakan enkripsi 56 bit sampai dengan 1024 bit, sehingga tingkat kombinasi enkripsinya pun sangat tinggi. Didalam bertransaksi, CA membuatkan sertifikat digital yang berisi informasi jati diri dan kunci publik cardholder, berikut informasi nomor kartu kredit yang ‘disembunyikan’,sehingga cardholder seperti mempunyai “KTP” digital. Biaya pengembangan infrastruktur SET relative sangat mahal, sehingga ini merupakan salah satu kerugiannya.

Ancaman Keamanan pada E-Commerce

Beberapa ancaman keamanan yang sering terjadi pada website e-commerce, antara lain *credit card fraud* atau *carding. Carding* adalah aktifitas pembelian barang di Internet menggunakan kartu kredit bajakan. Ada beberapa tahapan yang umumnya dilakukan para *carder* dalam melakukan aksi

kejahatannya, yaitu (1) mendapatkan nomor kartu kredit yang bisa dilakukan dengan berbagai cara antara lain: *phising, hacking, sniffing, keylogging, worm,* dan lain-lain. Berbagi informasi antara *carder*, mengunjungi situs yang memang spesial menyediakan nomor-nomor kartu kredit buat *carding* dan lain-lain yang pada intinya adalah untuk memperolah nomor kartu kredit; (2) mengunjungi situs-situs e-commerce seperti Ebay, Amazon untuk kemudian *carder* mencoba-coba nomor yang dimilikinya untuk mengetahui apakah kartu tersebut masih valid atau limitnya mencukupi; (3) melakukan transaksi secara online untuk membeli barang seolah-olah *carder* adalah pemilik asli dari kartu tersebut; (4) menentukan alamat tujuan atau pengiriman; (5) pengambilan barang oleh *carder*.

Sebagaimana kita ketahui bahwa Indonesia dengan tingkat penetrasi pengguna internet di bawah 10 %, namun menurut survei AC Nielsen tahun 2001 menduduki peringkat keenam dunia dan keempat di Asia untuk sumber para pelaku kejahatan *carding*. Hingga akhirnya Indonesia di-*blacklist* oleh banyak situs-situs *online* sebagai negara tujuan pengiriman. Oleh karena itu, para *carder* asal Indonesia yang banyak tersebar di Jogja, Bali, Bandung dan Jakarta umumnya menggunakan alamat di Singapura atau Malaysia sebagai alamat antara di mana di negara tersebut mereka sudah mempunyai rekanan.

Dos (*Denial of Service attacks*) dan DDos (*Distributed Dos*)

Denial of Service attacks adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan resource yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut. Dalam sebuah serangan *Denial of Service*, si penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap sistem atau jaringan dengan menggunakan beberapa cara, seperti dengan *traffic flooding* atau *request flooding*. Sedangkan *Distributed Dos* adalah salah satu jenis serangan *Denial of Service* yang menggunakan banyak host penyerang (baik itu menggunakan komputer yang didedikasikan untuk melakukan penyerangan atau komputer yang "dipaksa" menjadi *zombie*) untuk menyerang satu buah host target dalam sebuah jaringan. Distributed Dos merupakan jenis serangan yang sering digunakan pada situs yang popular, seperti Yahoo!, Amazon, dan eBay.

Social Engineering

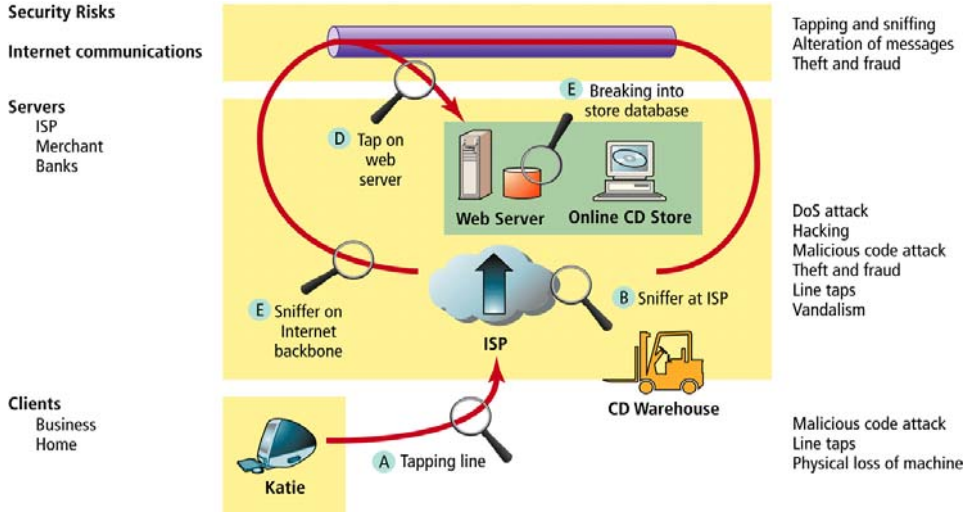
Serangan yang paling mudah dan paling menguntungkan adalah dengan menggunakan teknik social engineering. Attacker pemerolehan informasi rahasia/sensitif dengan cara menipu pemilik informasi tersebut. *Social engineering* umumnya dilakukan melalui telepon atau Internet. Skenario yang biasanya sering dipakai adalah *attacker* menelpon pembeli dan berpura-pura menjadi perwakilan dari website tempat dia membeli barang dan mengumpulkan beberapa informasi penting. Kemudian *attacker* menelpon customer service dari website tersebut dan berpura-pura menjadi pembeli dan memberi tahukan personal information yang sebelumnya telah dia dapatkan dari pembeli. Lalu attacker meminta customer service untuk mereset ulang password yang ada.

Sebagai contoh, seorang berpura-pura sebagai agen tiket yang menelepon salah satu pegawai perusahaan untuk konfirmasi bahwa tiket liburannya telah dipesan dan siap dikirim. Pemesanan dilakukan dengan nama serta posisi target di perusahaan itu, dan perlu mencocokkan data dengan target. Tentu saja target tidak merasa memesan tiket, dan penyerang tetap perlu mencocokkan nama, serta nomor pegawainya. Informasi ini bisa digunakan sebagai informasi awal untuk masuk ke sistem di perusahaan tersebut dengan account target.

Bentuk lainnya adalah *phising schemes*, apabila terjadi kesalahan pengetikan, maka pembeli akan memasuki situs yang tidak sah dan memberikan informasi rahasia yang dia miliki. Penyerang juga dapat berpura-pura mengirimkan email palsu yang terlihat datang dari situs yang sah kemudian mengumpulkan informasi yang ada.

Malicious Code

Suatu program, baik macro maupun script yang dapat dieksekusi dan dibuat dengan tujuan untuk merusak sistem computer. Bentuknya dapat berupa virus, worm, ataupun trojan. Apabila website e-commerce sudah disisipi malicious code ini maka kemungkinan besar computer pengunjung pun akan terinfeksi juga. Melalui malicious code ini lah pembajakan ID/password dapat terjadi.



Gambar 2 Celah Keamanan pada E-Commerce
Sumber: Laudon and Traver (2001)

Perencanaan Peningkatan Keamanan pada E-Commerce

Membuat perencanaan peningkatan keamanan tersebut, memiliki 5 tahapan, yaitu (1) *perform a risk assessment*, melakukan penilaian terhadap resiko yang dapat terjadi dan penilaian terhadap poin *vulnerability* yang ada; (2) *develop security policy*, *security policy* adalah sekumpulan pernyataan yang berisikan pernyataan yang memprioritaskan resiko informasi, identifikasi terhadap target yang beresiko, dan indentifikasi mekanisme untuk mencapai target tersebut; (3) *develop an implementation plan*, tahap selanjutnya adalah implementasi terhadap security policy yang telah direncanakan; (4) *create a security organization*, membuat sebuah organisasi yang bertanggung jawab atas keamanan. Selain itu mereka juga bertanggung jawab untuk membuat user dan manajemen lebih sadar akan ancaman keamanan serta melakukan pemeliharaan terhadap tools yang dipilih untuk mengimplementasikan *security*; (5) *perform a security audit*, untuk memeriksa dan mereview akses log secara rutin dan mengidentifikasi bagaimana outsiders menggunaka website sebaik *insiders* yang melakukan akses.

Bagaimana eBay Sebagai Website E-Commerce Membantu Keamanan Pelanggannya

eBay adalah ajang pasar online dunia, tempat bagi pembeli dan penjual berhimpun dan berdagang apa saja. Diluncurkan tahun 1995, eBay diawali sebagai tempat untuk berdagang barang

koleksi dan barang yang sulit ditemukan. Sejak itu, eBay telah berkembang menjadi ajang pasar tempat Anda dapat menemukan segala sesuatu, dari ponsel dan DVD hingga pakaian, barang koleksi dan mobil. Dengan daftar barang sebanyak 103,6 juta di seluruh dunia dan penambahan daftar barang sebanyak 6,1 juta yang dilakukan setiap hari, eBay menawarkan kesempatan yang tidak terhingga bagi semua orang untuk membeli dan menjual di seluruh dunia. eBay menerima beberapa bentuk pembayaran seperti : PayPal, Credit cards dan debit cards, Moneybookers, Paymate, ProPay, Pay upon pickup, Escrow.

Beberapa cara yang disarankan eBay kepada pelanggannya untuk melakukan proteksi terhadap account yang dimiliki yaitu (1) apabila pelanggan menerima email yang mencurigakan, eBay menyarankan untuk mengecek di menu Messages pada akun pelanggan. Lalu *forward* email tersebut ke spoof@ebay.com; (2) berhati-hati dengan website yang mengandung kata "eBay" pada URL-nya. Website eBay yang resmi adalah "ebay.com" sebelum slash (/) pertama. Jika alamat mengandung karakter tambahan seperti @, -, nomer, maka itu bukan merupakan website eBay. Contoh dari fake website eBay : http://signin.ebay.com@10.19.32.4/; (3) pelanggan dapat mengamankan akun yang dimiliki dengan cara: *login* ke dalam eBay account, apabila tidak berhasil pelanggan diharapkan secepatnya menghubungi customer service eBay, ubah password pada akun email pribadi pelanggan, pelanggan dapat meminta password yang baru, merubah pertanyaan rahasia berikut jawabannya, dan melakukan verifikasi informasi kontak pada akun pelanggan, pelanggan sebaiknya melakukan perlindungan computer terhadap virus online dan ancaman melalui internet lainnya. Hal ini dapat dilakukan, dengan melakukan update terhadap internet browser, gunakan dan lakukan update antivirus, menginstal firewall; (4) pelanggan dapat menghalangi pencurian identitas diantaranya dengan cara: selalu memonitor akun yang dimiliki dan jangan pernah me-reply email yang menanyakan informasi pribadi dan lakukan verifikasi email tersebut pada menu My Messages pada akun.

PENUTUP

Penerapan e-Commerce pada saat ini merupakan salah satu syarat yang layak dipenuhi oleh suatu perusahaan atau organisasi yang masih berkembang ataupun yang telah matang sekalipun agar dapat bersaing secara global dan dapat meningkatkan kinerja secara lebih baik. Dengan *E-Commerce* memungkinkan kita bertransaksi dengan cepat dan biaya yang murah tanpa melalui proses yang berbelit-belit. Walau dalam penerapannya masih banyak terdapat ancaman pada keamanannya, tetapi untuk kedepannya diharapkan bisnis E-Commerce dapat terus berkembang tentunya sejalan dengan perkembangan keamanannya. Diharapkan para pelaku bisnis E-Commerce dapat menyadari betapa pentingnya keamanan dalam bertransaksi dan bersikap waspada terhadap berbagai ancaman yang mungkin terjadi.

DAFTAR PUSTAKA

Laudon, K. C., & Traver, C. G. (2004). *E-Commerce, Business. Technology. Society* (2nd ed.). Addison-Wesley.

Potter. (2003). *Introduction to Information Technology* (2nd ed.). New Jersey: John Wiley & Sons, Inc.

Haryadi, H. (2009). Carding, di akses 15 Agustus 2010, dari http://www.tandef.net/carding

Muharami, E. (2010). E-Payment, diakses 14 Agustus 2010, dari http://www.ittelkom.ac.id/library/index.php?option=com_content&view=article&id=652:epayment&catid=6:internet&itemid=15

Purwanto, I. (2010). *Internet dan Jaringan Computer*, diakses 14 Agustus 2010, dari http://ridha.staff.gunadharma.ac.id

Agustiandar, Y. E. (2008). *Keamanan E-Commerce*, diakses 14 Agustus 2010, dari http://epolebusiness.wordpress.com/2008/06/04/keamanan-e-commerce/

Zolzer, D. (2002). *Security and Encryption*, diakses 17 Agustus 2010, dari http://www.csie.ntu.edu.tw/~ec/Laudon/Chapter5.pdf