PERTEMUAN 4 :
SECURITY ECOMMERCE

A. TUJUAN PEMBELAJARAN

Pada pertemuan ini akan dijelaskan mengenai Pengantar security eCommerce, Tujuan security eCommerce, Konsep security eCommerce dan Jenis-Jenis security dalam eCommerce. Anda harus mampu

4.1. Menjelaskan Pengertian security dalam eCommerce
4.2. Menjelaskan Tujuan Security dalam eCommerce
4.3. Mengimplementasikan konsep Security dalam eCommerce
4.4. Mengaplikasikan Metode Security dalam eCommerce

B. URAIAN MATERI

Tujuan Pembelajaran 4.1:

Menjelaskan Pengertian Security eCommerce

Keamanan adalah kekhawatiran bagi organisasi karena menghadapi masalah ganda untuk melindungi data yang disimpan dan pesan yang dikirim. Organisasi selalu memiliki data sensitif yang ingin membatasi akses ke beberapa orang yang berwenang. Secara historis data tersebut disimpan di daerah terlarang atau disandikan. Ecommerce menimbulkan tambahan masalah keamanan.

Pertama, maksud dari Internet adalah untuk memberi orang-orang remote akses informasi. Sistem ini pendekatan inheren terbuka, secara tradisional membatasi akses kepada pengguna dimana merupakan hambatan fisik yang kurang layak, meskipun organisasi masih perlu untuk membatasi akses fisik ke server.

Kedua, karena perdagangan elektronik didasarkan pada komputer dan jaringan, teknologi ini dapat digunakan untuk menyerang sistem keamanan. Hacker dapat menggunakan komputer untuk mencegat lalu lintas jaringan dan me-scan rahasia informasi. Mereka dapat menggunakan komputer untuk menjalankan serangan berulang-ulang pada sistem untuk pelanggaran keamanan (misalnya, mencoba semua kata dalam kamus untuk password account).

Faktor keamanan meliputi :

- pengelolaan dan penjagaan keamanan secara fisik
- penambahan perangkat-perangkat elektronik (perangkat lunak dan perangkat keras) untuk melindungi data, sarana komunikasi serta transaksi

Faktor Pendorong Kemunculan dan Perkembangan Keamanan e-Commerce:

- ❖ Kemajuan infrasutruktur sistem komunikasi
- ❖ Meledaknya sistem perdagangan global
- ❖ Sistem perdagangan real time
- ❖ Meningkatkan rasa pengertian/penghargaan terhadap segala resiko yang mungkin terjadi
- ❖ Tersedianya teknologi sistem keamanan (security)
- ❖ Sistem keamanan sebagai aset yang berharga
- ❖ Politik
- ❖ Pengakuan terhadap pernyataan sah

Tujuan Pembelajaran 4.2:

Menjelaskan Tujuan Security dalam eCommerce

Sistem Keamanan Informasi: Merupakan penerapan teknologi untuk mencapai tujuan-tujuan keamanan sistem informasi dengan menggunakan bidang-bidang utama yaitu:

- Sistem Keamanan Komunikasi (Communications security) merupakan perlindungan terhadap informasi ketika di kirim dari sebuah sistem ke sistem lainnya.
- Keamanan Komputer (Computer security) adalah perlindungan terhadap sistem informasi komputer itu sendiri.
- Keamanan secara fisik seperti pengamanan oleh penjaga keamanan, pintu yang terkunci, sistem control fisik lainnya, dan sebagainya.
- Keamanan Personal meliputi kepribadian orang-orang yang mengoperasikan atau memilki hubungan langsung dengan sistem tersebut.

- Keamanan administrative contohnya mengadakan control terhadap perangkat-perangkat

  lunak yang digunakan, mengecek kembali semua kejadian-kejadian yang telah diperiksa sebelumnya dan sebagainya.
- Keamanan media yang digunakan meliputi pengontrolan terhadap media penyimpanan yang ada dan menjamin bahwa media penyimpanan yang mengandung informasi sensitive tersebut tidak mudah hilang begitu saja.

Tujuan-tujuan Sistem Keamanan Informasi:

- *Confidentially* : Menjamin apakah informasi yang dikirim tersebut tidak dapat dibuka atau tidak dapat diketahui oleh orang lain yang tidak berhak.
- *Integrity*: Menjamin konsistensi data tersebut apakah masih utuh sesuai aslinya atau tidak, sehingga upaya orang-orang yang tidak bertanggung jawab untuk melakukan penduplikatan dan perusakan data bisa dihindari.
- *Availability* : Menjamin pengguna yang sah agar dapat mengakses informasi dan sumber miliknya sendiri.

  Legitimate Use : Menjamin kepastian bahwa sumber tidak digunakan oleh orang-orang yang tidak bertanggung jawab

Tujuan Pembelajaran 4.3:

Mengimplementasikan konsep Security dalam eCommerce

Konsep Security e-Commerce:

1. Security Policy (Kebijaksanaan keamanan yang digunakan) merupakan satu set aturan yang diterapkan pada semua kegiatan-kegiatan pengamanan dalam security domain. Security domain merupakan satu set sistem komunikasi dan computer yang dimiliki oleh organisasi yang bersangkutan.
2. Authorization (Otorisasi) berupa pemberian kekuatan secara hukum untuk melakukan segala aktifitasnya
3. Accountability (kemampuan dapat diakses) memberikan akses ke personal security.
4. A Threat (Ancaman yang tidak diinginkan) merupakan kemungkinan-kemungkinan munculnya seseorang, sesuatu atau kejadian yang bisa

membahayakan aset-aset yang berharga khususnya hal-hal yang berhubungan dengan *confidentiality*, *integrity*, a*vailability* dan *legitimate use*.

5. *An Attack* (Serangan yang merupakan realisasi dari ancaman), pada sistem jaringan computer ada dua macam attack, yaitu passive attack (misalnya monitoring terhadap segala kegiatan pengiriman informasi rahasia yang dilakukan oleh orang-orang yang tidak berhak) dan active attack (misalnya perusakan informasi yang dilakukan dengan sengaja dan langsung mengena pada sasaran).
6. *Safeguards* (Pengamanan) meliputi control fisik, mekanisme, kebijaksanaan dan prosedur yang melindungi informasi berharga dari ancaman-ancaman yang mungkin timbul setiap saat.
7. *Vulnerabilitie*s (Lubang-lubang keamanan yang bisa ditembus)
8. *Risk* (Resiko kerugian) merupakan perkiraan nilai kerugian yang ditimbulkan oleh kemungkinan adanya attack yang sukses.
9. *Risk Analysis* (Analisa Kerugian) merupakan proses yang menghasilkan suatu keputusan apakah pengeluaran yang dilakukan terhadap *safeguards* benar-benar bisa menjamin tingkat keamanan yang diinginkan.

***Threats* (Ancaman):**

- System Penetration : orang-orang yang tidak berhak, mendapatkan akses ke sistem computer dan diperbolehkan melakukan segalanya.
- *Authorization Violation*: Ancaman berupa pelanggaran atau penayalahgunaan wewenang legal yang dimiliki oleh seseoarang yang berhak.
- *Planting*: Ancaman yang terencana misalnya Trojan horse yang masuk secara diam-diam yang akan melakukan penyerangan pada waktu yang telah ditentukan.
- Communications Monitoring: penyerang dapat melakukan monitoring semua informasi rahasia.
- *Communications Tampering*: penyerang mengubah informasi transaksi di tengah jalan pada sebuah jaringan komunikasi dan dapat mengganti sistem server dengan yang palsu.
- *Denial of Service* (DoS): Penolakan service terhadap client yang berhak.

- *Repudiation*: Penolakan terhadap sebuah aktivitas transaksi atau sebuah komunikasi yang terjadi dikarenakan sesuatu yang bersifat senagja, kecelakaan ataupun kesalahan teknis lainnya.

***Safeguards*:**

Yang dilakukan *safeguards* yaitu:

- Mencegah munculnya *threats* (ancaman) sebelum benar-benar terealisasi
- Meminimalisasikan kemungkinan terjadinya ancaman tersebut.
- Mengurangi akibat yang timbul karena ancaman yang sudah terealisasi.

Security service safe guards:

- *Authentication Service*: Memberikan kepastian identitas pengguna.
  - Entity authentication: contohnya password.
  - Data origin authentication: membuktikan sah tidaknya identitas dalam bentuk pesna tertulis.
- *Access Control Services*: Melindungi semua fasilitas dan sumber-sumber yang ada dari akses-akses yang tidak berhak.
- *Confidentiality Service*: Memberikan perlindungan terhadap informasi yang berusaha disingkap oleh orang lain yang tidak berhak.
- *Data Integrity Srevice*: Perlindungan terhadap ancaman yang dapat mengubah data item seandainya ini terjadi di dalam lingkungan security policy.
- *Non-Repudiation Service*: Melindungi user melawan ancaman yang berasal dari user berhak lainnya. Ancaman tersebut dapat berupa kesalahan penolakan ketika transaksi atau komunikasi sedang terjadi

Tujuan Pembelajaran 4.3:

Mengaplikasikan Metode Security dalam eCommerce

Ada beberapa metode pengamanan yang digunakan dalam membangun E-Commerce, yaitu :

a) Metode Enkripsi

Metode enkripsi atau yang lebih dikenal dengan kriptografi (cryptograph) adalah metode penyandian suatu pesan atau data yang terkirim melalui jaringan publik dengan menggunakan kunci-kunci (keys) tertentu. Beberapa teknologi enkripsi yang cukup populer adalah:

1. Kombinasi *Public Key* dan *Private Key*

   Public Key merupakan kunci yang dikenal oleh umum, sedangkan Private Key merupakan kunci yang hanya dikenal oleh si pemiliknya.

   Kombinasi Public Key / Private key sebetulnya menghilangkan keinginan mencuri dengan cara meng-enkripsi nomor kartu kredit tersebut di server prusahaan, jadi pada sa'at pengiriman data, data telah di-enkripsi dengan menggunakan teknologi public key dan private key,

2. *Certificate Authority/Digital Signature*

   Pada penggunaan public key di atas masih dimungkinkan adanya pencurian atau pemalsuan public key. Contoh, saat Nia meminta public key dari Imam, bisa saja di tengah perjalanan permintaan tersebut disadap orang lain, sehingga yang mengirimkan jawaban bukannya Imam, melainkan Mr.X yang mengaku sebagai Imam dan memberikan public key miliknya kepada Nia. Akibatnya, Mr. X akan mampu mendekrip data-data yang ditujukan Nia kepada Imam. Oleh karenanya diperlukan adanya keterlibatan pihak ketiga yang dapat dipercaya (yang menjamin keabsahan dari suatu public key), yaitu Certification Authority (CA). CA inilah yang akan memberikan sertifikasi atas public key milik Imam. Sertifikasi yang diberikan kepada public key seseorang ini dikenal sebagai Digital Signature.

3. *Secure Electronic Transaction* (SET)

   SET pertama kali diperkenalkan oleh RSA Data Security, suatu lembaga independen yang mengeluarkan berbagai standarisasi dalam hal Internet Security. Teknologi yang digunakan dalam SET merupakan gabungan antara teknologi enkripsi public key/private key dengan teknologi digital signature. *Secure Electronic Transaction* (SET) tersebut akan mengen kode nomor kartu kredit yang ada di server vendor di internet dan yang hanya dapat membaca nomor kartu kredit tersebut hanya Bank dan Perusahaan kartu kredit, artinya pegawai vendor/ merchant tidak bisa membaca sama sekali sehingga kemungkinan terjadi pencurian oleh vendor menjadi tidak mungkin.

b) Metode *Virtual Private Network* (VPN)

Virtual Private Network atau Jaringan Pribadi Maya, pada umumnya, di mana satu jaringan komputer suatu lembaga atau perusahaan di suatu daerah atau negara terhubung dengan jaringan komputer dari satu grup perusahaan yang sama di daerah atau negara lain, dalam VPN, media penghubungnya adalah Internet. Pengamanan dan pembatasan diperlukan untuk menjaga agar tidak semua orang atau user dari jaringan pribadi dapat mengakses jaringan publik (internet).

Sesungguhnya konsep VPN inilah yang diadopsi kedalam E-Commerce. Karena user yang melakukan transaksi di Internet pada suatu situs Web telah membentuk suatu VPN antara user dan situs Web tersebut, di mana segala informasi atau data yang terkirim diantara keduanya tidak dapat disadap atau dibuka oleh user lain yang memang tidak berhak membukanya.

Secara garis besar, ada dua cara membentuk VPN, yaitu :

❖ *Tunneling*

Sesuai dengan arti tunnel atau lorong, dalam membentuk suatu VPN ini dibuat suatu tunnel di dalam jaringan publik untuk menghubungkan antara jaringan yang satu dan jaringan lain dari suatu grup atau perusahaan.yang ingin membangun VPN tersebut. Seluruh komunikasi data antar jaringan pribadi akan melalui tunnel ini, sehingga orang atau user dari jaringan publik yang

tidak memiliki izin untuk masuk tidak akan mampu untuk menyadap, mengacak atau mencuri data yang melintasi tunnel ini. Salah satu metode tunelling yang umum dipakai, di antaranya: IPX To IP Tunnelling

IPX To IP tunnelling biasa digunakan dalam jaringan VPN Novell Netware. Jadi dua jaringan Novell yang terpisah akan tetap dapat saling melakukan komunikasi data melalui jaringan publik Internet melalui tunnel ini tanpa kuatir akan adanya gangguan pihak ke-3 yang ingin mengganggu atau mencuri data. Pada IPX To IP tunnelling, paket data dengan protokol IPX (standar protokol Novell) akan dibungkus (encapsulated) terlebih dahulu oleh protokol IP (standar protokol Internet) sehingga dapat melalui tunnel ini pada jaringan publik Internet.

Saat ini beberapa vendor hardware router seperti Cisco, Shiva, Bay Networks sudah menambahkan kemampuan VPN dengan teknologi tunnelling pada hardware mereka.

❖ *Firewall*

Sebagaimana layaknya suatu dinding, Firewall akan bertindak sebagai pelindung atau pembatas terhadap orang-orang yang tidak berhak untuk mengakses jaringan kita.

Suatu jaringan yang terhubung ke Internet pasti memiliki IP address (alamat Internet) khusus untuk masing-masing komputer yang terhubung dalam jaringan tersebut. Apabila jaringan ini tidak terlindungi oleh tunnel atau firewall, IP address tadi akan dengan mudahnya dikenali atau dilacak oleh pihak-pihak yang tidak diinginkan. Akibatnya data yang terdapat dalam komputer yang terhubung ke jaringan tadi akan dapat dicuri atau diubah. Dengan adanya pelindung seperti firewall, hal ini bisa menyembunyikan (hide) address tadi sehingga tidak dapat dilacak oleh pihak-pihak yang tidak diinginkan.

Kemampuan yang dimiliki oleh firewall :

- IP Hiding/Mapping. Kemampuan ini mengakibatkan IP address dalam jaringan dipetakan atau ditranslasikan ke suatu IP address baru. Dengan demikian IP address dalam jaringan tidak akan dikenali di Internet.
- Privilege Limitation. Dengan kemampuan ini dapat membatasi para user dalam jaringan sesuai dengan otorisasi atau hak yang diberikan kepadanya. Misalnya, User A hanya boleh mengakses home page, user B boleh mengakses home page, e-mail dan news, sedangkan user C hanya boleh mengakses e-mail.
- Outside Limitation. Dengan kemampuan ini dapat membatasi para user dalam jaringan untuk hanya mengakses ke alamat-alamat tertentu di Internet di luar dari jaringan kita.
- Inside Limitation. Kadang-kadang masih memperbolehkan orang luar untuk mengakses informasi yang tersedia dalam salah satu komputer (misalnya Web Server) dalam jaringan kita. Selain itu, tidak diperbolehkan, atau memang sama sekali tidak dizinkan untuk mengakses seluruh komputer yang terhubung ke jaringan kita.
- Password and Encrypted Authentication. Beberapa user di luar jaringan memang diizinkan untuk masuk ke jaringan kita untuk mengakses data dan sebagainya, dengan terlebih dahulu harus memasukkan password khusus yang sudah terenkripsi.

Firewall yang tersedia saat ini dipasaran sangat banyak, ada yang tergantung pada suatu sistem operasi tertentu (Unix, Windows-NT, Novell) ada yang independen. Firewall yang tergantung pada sistem operasi umumnya berupa software, sedangkan yang independen berupa blackbox hardware.

Jika memikirkan tentang keamanan berbelanja, Sebenarnya yang harus di ketahui sebagian besar dari pencurian kartu kredit terjadi disebabkan oleh pegawai sales yang menghandle nomor kartu kredit tersebut, atau juga kemungkinan penyebab pembobolan kartu kredit itu terjadi bisa dikarnakan pada setiap kali anda membayar menggunakan kartu kredit di toko, di restoran, di glodok / mangga dua.

Pada setiap kali anda membuang resi pembelian kartu kredit, anda sebenarnya telah membuka informasi kartu kredit tersebut untuk dicuri.

Setelah apa yang anda ketahui tentang e-commers, yang lebih jelasnya e-commers merupakan cara yang aman untuk membuka toko/usaha bisnis karena meminimalkan kemungkinan dijarah, dirampok, dibakar, dan kebanjiran.

C. SOAL LATIHAN/TUGAS

1. Gambarkan metode Enkripsi dan Certification Authority/Digital Signature berikan penjelasan!
2. Gambarkan proses Enkripsi RSA berikan contoh dan penjelasannya!
3. Untuk melindungi kegiatan bisnis online atau eCommerce pelaku yang terlibat didalam mendapat perlindungan dari pemerintah dengan terbitnya UU TEI, cobalah anda cari UU TEI yang terkait dengan kegiatan eCommerce!
4. Selain kejahatan dalam dunia maya yang sudah dijelaskan sebelumnya, *cyber crime* apa saja yang bisa terjadi atau kemungkinan terjadi, jelaskan dan bagaimana penanggunalangannya, Anda dapat berdiskusi dalam kelompok. Presentasikan hasilnya pada kegiatan pembelajaran selanjutnya.
5. Sebutkan dan jelaskan apa saja standar keamanan untuk aplikasi web, Email dan jaringan!
6. Apa yang anda ketahui tentang SET (Security Elektronic Transaction), jelaskan proses kerjanya, dan berikan contoh!

D. DAFTAR PUSTAKA

Buku

Electronic Commerce : The Strategic Perspective **,** by Richard T. Watson, Pierre Berthon, Leyland F. Pitt, and George M. Zinkhan, Copyright © 2008 , The Global Text Project is funded by the Jacobs Foundation, Zurich, Switzerland.

eCommerce and eBusines**,** by Zorayda Ruth Andam, May 2003, e-Asean Task Force UNDP APDP.

Onno W. Purbo, Dkk, Mengenal eCommerce, Elex Media Komputindo, Jakarta,2001

Link and Sites:

staffsite.gunadarma.ac.id/lulu/index.php?stateid=download&id

http://www.crmbuyer.com/story/64103.html

http://www.ecommerce-web-hosting-guide.com/ecommerce-business-models.html

http://deris.unsri.ac.id/materi/deris/ecommerce_deris.pdf

GLOSARIUM

Confidentially adalah Menjamin apakah informasi yang dikirim tersebut tidak dapat dibuka atau tidak dapat diketahui oleh orang lain yang tidak berhak.

Integrity adalah Menjamin konsistensi data tersebut apakah masih utuh sesuai aslinya atau tidak, sehingga upaya orang-orang yang tidak bertanggung jawab untuk melakukan penduplikatan dan perusakan data bisa dihindari.

Availability adalah Menjamin pengguna yang sah agar dapat mengakses informasi dan sumber miliknya sendiri.

Legitimate Use adalah Menjamin kepastian bahwa sumber tidak digunakan oleh orang-orang yang tidak bertanggung jawab

Security Policy (Kebijaksanaan keamanan yang digunakan) adalah satu set aturan yang diterapkan pada semua kegiatan-kegiatan pengamanan dalam security domain. Security domain merupakan satu set sistem komunikasi dan computer yang dimiliki oleh organisasi yang bersangkutan.

Authorization (Otorisasi) adalah pemberian kekuatan secara hukum untuk melakukan segala aktifitasnya

Accountability (kemampuan dapat diakses) adalah memberikan akses ke personal security.

A Threat (Ancaman yang tidak diinginkan) adalah kemungkinan-kemungkinan munculnya seseorang, sesuatu atau kejadian yang bisa membahayakan aset-aset yang berharga khususnya hal-hal yang berhubungan dengan confidentiality, integrity, availability dan legitimate use.

An Attack adalah Serangan yang merupakan realisasi dari ancaman

Safeguards (Pengamanan) adalah pengamanan yang meliputi control fisik, mekanisme, kebijaksanaan dan prosedur yang melindungi informasi berharga dari ancaman-ancaman yang mungkin timbul setiap saat.

Vulnerabilities adalah Lubang-lubang keamanan yang bisa ditembus

Risk (Resiko kerugian) adalah perkiraan nilai kerugian yang ditimbulkan oleh kemungkinan adanya attack yang sukses.

Risk Analysis (Analisa Kerugian) adalah proses yang menghasilkan suatu keputusan apakah pengeluaran yang dilakukan terhadap safeguards benar-benar bisa menjamin tingkat keamanan yang diinginkan.