METODE KEAMANAN E-COMMERCE

Kartika Imam Santoso[1]
[1]Jurusan Sistem Informasi, STMIK BINA PATRIA Magelang
E-mail : kartikaimams@gmail.com[1]

Abstract

Many companies sell and promote the products via E-Commerce and E-Business. The sale is done electronically by we application. Beside that network security is the most important issue when we build web situs oriented to support the activities of E-Commerce.Nevertheless, many owner of business don"t realize because of limited information and capabilities. On the other hand, if we would like to do transaction of sale and buying in the situd of E-Commerce web must be equipped with the facility of data enscription. The purpose of the research is to know the methods to protect the security of E-Commerce. To limit the possibility of victim must be better than to improve the damage after the attack which is impossible to be improved. There are 24 security of E-Commerce as follows: Security standar, ISO 17799, Security public, Physic security, Controlacccess, Monitoring, Outhentication, Biometric, *Usernames and Passwords*, Smartcard, Wireless Security, 802.1X Standard, Cryptography, Hashing, Simetric enscription, Asimetric encsription, EAP-TLS, EAP-TTLS, PEAP (Protected EAP), WPA2 AES Passphrase, Digital Certificates, Firewalls, Computer Intrusion Detection and Prevention Systems, Encrypting For E-Mail, Use Filter, Payment security.The methode can be usedone orcombined in the system of E-Commerce for the network security and protect the system.

Keyword: E-Commerce, E-Commerce security**,** Protection Methods

Abstrak

Banyak perusahaan yang menjual produk dan promosi produk melalui E-Commerce dan E-Bussiness. Penjualan tersebut dilakukan secara elektronik dengan aplikasi web. Di samping itu, keamanan jaringan adalah isu paling penting saat kita membangun sebuah situs web yang ditujukan untuk mendukung aktivitas E-Commerce. Namun demikian, banyak sekali pemilik bisnis yang tidak menyadari hal tersebut karena terbatasnya informasi dan seringkali karena terbenturnya oleh minimnya kapabilitas pihak pengembangnya. Padahal jika menginginkan adanya transaksi pemesanan dan pembelian dalam situs web E-Commerce, minimal harus dilengkapi fasilitas enkripsi data. Tujuan dari penelitian ini adalah untuk mengetahui metode-metode untuk melindungi *(Protection Methods)* atau lapisan mana saja yang bisa dilakukan untuk keamanan e-Commerce. Membatasi kemungkinan menjadi korban adalah lebih baik daripada mencoba untuk memperbaiki kerusakan setelah serangan, yang mungkin tidak dapat diperbaiki. Metode Pengamanan e-Commerce ada 24 antara lain : Standar Keamanan, ISO 17799, Kebijakan keamanan, Keamanan fisik, Akses kontrol, Pemantauan (*Monitoring*), Otentikasi, Biometrik, *Usernames and Passwords*, Smartcard, Wireless Security, 802.1X Standard, Cryptography, Hashing, Enkripsi Simetrik, Enkripsi Asimetrik, EAP-TLS, EAP-TTLS, PEAP (Protected EAP), WPA2 AES Passphrase, *Digital Certificates*, Firewalls, *Computer Intrusion Detection and Prevention Systems*, *Encrypting For E-Mail*, Penggunaan Filter (*Use Filter*), Keamanan Pembayaran. Metode tersebut bisa digunakan satu atau digabungkan dalam sisttem e-Commerce untuk keamanan jaringan dan melindungi sistem.

Keyword : e-Commerce, keamanan e-Commerce***, Protection Methods***

1. Pendahuluan

Dewasa ini, perkembangan teknologi dan informasi semakin pesat. Teknologi Internet merupakan salah satu media informasi yang saat ini paling banyak digunakan karena memiliki banyak keunggulan terutama dalam efesiensi waktu serta murah. Salah satu contoh dari pemanfaatan Internet adalah aplikasi web. Aplikasi web adalah suatu aplikasi yang diakses menggunakan penjelajah web melalui suatu jaringan seperti Internet atau Intranet. Aplikasi web sangat bermanfaat dalam mempromosikan ataupun melakukan transaksi jual beli pada sebuah perusahaan melalui media Internet. Sebagai contoh, banyaknya perusahaan yang menjual produk dan promosi produk melalui E-Commerce dan E-Bussiness. Penjualan tersebut dilakukan secara elektronik.

Di samping itu, keamanan jaringan adalah isu paling penting saat kita membangun sebuah situs web yang ditujukan untuk mendukung aktivitas E-Commerce. Namun demikian, banyak sekali pemilik bisnis yang tidak menyadari hal tersebut karena terbatasnya informasi dan seringkali karena terbenturnya oleh minimnya kapabilitas pihak pengembangnya. Padahal jika menginginkan adanya transaksi pemesanan dan pembelian dalam situs web E-Commerce, minimal harus dilengkapi fasilitas enkripsi data.

Fasilitas enkripsi data yang standar yang digunakan di Internet saat ini adalah SSL (Secure Socket Layer) yang diterbitkan oleh

penerbit terpercaya berdasarkan CA (Certificate Authority) yang diakui. Dalam hal ini protokol HTTP (Hypertext Transfer Protocol) adalah protokol baku yang digunakan dalam web. Demi mendukung kemudahan komunikasi antar perangkat yang beragam maka protokol HTTP dirancang bersifat memiliki platform terbuka. Kemudahan rancangan ini ternyata dimanfaatkan oleh beberapa oknum untuk mencuri informasi yang dikirimkan oleh pengakses suatu situs web.

Untuk melindungi paket informasi yang dikirimkan melalui protokol terbuka HTTP maka dirancanglah sebuah protokol HTTPS (Hypertext Transfer Protocol Secure) dengan sistem enkripsi data yang dinamakan SSL. Dengan demikian, pada saat seorang pengakses situs web mengirimkan data secara elektronik, SSL yang dikonfigurasi dalam situs web tersebut akan mengenkripsinya dan mendistribusikannya melalui lapisan khusus yang sulit diakses oleh pihak ketiga.

Kelemahan dari layanan web e-Commerce antara lain pada saluran komunikasi data, target pada client, target pada server, target pada database serta pada transaksi pembayaran.

2. Landasan Teori

2.1. E-Commerce

E-commerce merupakan kepanjangan dari Electronic Commerce yang berarti perdagangan yang dilakukan secara elektronik. Seperti halnya e-mail (Electronic Mail) yang artinya sudah diketahui yaitu pengiriman surat secara elektronik. E-commerce berarti perdagangan elektronik yang mencakup proses pembelian, penjualan, transfer, atau pertukaran produk, layanan, atau informasi melalui jaringan komputer, termasuk Internet [1].

Dalam sebuah perusahaan e-commerce bisa bertahan atau tidak hanya mengandalkan kekuatan produk saja, tapi dengan adanya tim manajemen yang handal, pengiriman yang tepat waktu, pelayanan yang bagus, struktur organisasi bisnis yang baik, jaringan infrastruktur dan keamanan, desain situs web yang bagus, beberapa faktor yang termasuk:

a. Menyediakan harga kompetitif
b. Menyediakan jasa pembelian yang tanggap, cepat, dan ramah.
c. Menyediakan informasi barang dan jasa yang lengkap dan jelas.
d. Menyediakan banyak bonus seperti kupon, penawaran istimewa, dan diskon.
e. Memberikan perhatian khusus seperti usulan pembelian.
f. Menyediakan rasa komunitas untuk berdiskusi, masukan dari pelanggan, dan lain-lain.
g. Mempermudah kegiatan perdagangan

2.2. Keamanan Komputer

Keamanan komputer meliputi beberapa aspek diantaranya:

a. *Authentication*: agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi. Dengan kata lain informasi tersebut benar-benar dari orang yang dikehendaki.
b. *Integrity*: keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut.
c. *Nonrepudiation*: merupakan hal yang bersangkutan dengan si pengirim. Si pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
d. *Authority*: informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
e. *Confidentiality*: merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Confidentiality* biasanya berhubungan dengan informasi yang diberikan kepada pihak lain.
f. *Privacy*: merupakan lebih ke arah data-data yang sifatnya pribadi.
g. *Availability*: aspek *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.
h. *Acces control*: aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal itu biasanya berhubungan dengan masalah *authentication* dan juga *privacy*. *Access control* seringkali dilakukan menggunakan kombinasi user id dan *password* atau dengan menggunakan mekanisme lainnya [2].

2.3. Berdasarkan bagaimana cara dan posisi seseorang mendapatkan pesan-pesan dalam saluran komunikasi, penyerangan dapat dikategorikan menjadi:

a. *Sniffing*; secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum maupun yang sudah dienkripsi) dalam suatu saluran komunikasi. Hal tersebut umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekam pembicaraan yang terjadi.
   Pencegahannya : enkripsi data dengan algoritma yang kuat seperti AES, RSA dll
b. *Replay Attack*; jika seseorang bisa merekam pesan-pesan *handshake*

(persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.

Pencegahan : enkripsi data dengan algoritma yang kuat seperti AES, RSA dll

c. *Spoofing*; Penyerang, misalnya C, bisa menyamar menjadi A. semua orang dibuat percaya bahwa C adalah A. penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada yang salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. PIN ke dalam *Card Acceptance Device* (CAD) – yang benar-benar dibuat seperti CAD asli – tentu sang penipu bisa mendapatkan PIN pemilik *smartcard*. Pemilik *smartcard* tidak tahu bahwa telah terjadi kejahatan.

Pencegahan : Membuat ciri khas dari web atau id kita, misal dengan *digital signature*.

d. *Man-in-the-middle*; jika *spoofing* terkadang hanya menipu satu pihak, maka dalam skenario ini saat A hendak berkomunikasi dengan B, C di mata A seolah-olah adalah B, dan C dapat pula menipu B sehingga C seolah-olah adalah A. C dapat berkuasa penuh atas jalur komunikasi dan bisa membuat berita fitnah.

Pencegahan : Membuat ciri khas dari web atau id kita, misal dengan *digital signature*

[2].

2.3. Serangan dan kerentanan *(Attacks And Vulnerabilities)*

Setiap hari, berbagai jenis kejahatan berteknologi sedang dilakukan, yang dapat menyebabkan banyak masalah bagi para korban. Teknologi kejahatan terjadi di sekitar kita, tetapi kurang terlihat dan lebih sedikit pelaku dibandingkan kejahatan lainnya. Hal ini memperkecil kemungkinan pelaku kriminal untuk terjebak karena mereka tidak harus mengambil risiko terlihat oleh tetangga mereka atau sampai alarm terdengar. Anonimitas dan ketersediaan internet mempermudah bagi hacker jahat untuk melakukan kejahatan dan tidak terjebak .

Kejahatan teknologi juga memiliki hasil yang lebih besar dibandingkan kejahatan tradisional. " Teknik canggih dan cerdik telah memungkinkan penjahat ini pada jaman modern menggunakan ribuan identitas yang dicuri untuk mengalirkan miliaran dari bank dan lembaga keuangan lainnya. Sementara itu, rata-rata pria *stickup* mendapat sekitar $ 7.200 dalam pencurian bank [3]. Hal ini penting untuk memahami metode serangan agar dapat secara efektif mengetahui dan memahami bagaimana untuk melindungi terhadap mereka. Metode serangan yang terus berubah, sehingga sangat penting untuk tetap mengikuti alat terbaru dan teknik hacker jahat gunakan untuk menembus pertahanan jaringan serta sebagai kebutuhan perlindungan terbaru .

a. Ancaman pada Web Server (*Web Server Threats*)

Perangkat lunak server web dirancang untuk memberikan halaman web dengan menanggapi permintaan HTTP. Perangkat lunak server web biasanya dirancang untuk kegunaan dan kenyamanan, bukan keamanan. "Perangkat lunak yang lebih kompleks, semakin besar probabilitas bahwa ia mengandung kesalahan coding atau kelemahan keamanan" (Schneider, 2009). Semakin banyak baris kode, semakin besar kesempatan ada akan menjadi kesalahan. "Perkiraan umum digunakan dalam industri adalah bahwa ada antara 5-50 bug per 1.000 baris kode. Jadi perkiraan akan bahwa Microsoft Windows 7 memiliki sekitar 1,200,000 bug "[4].

Web server dapat diserang oleh penyerang untuk memperoleh nama pengguna dan password dari salah satu pengguna. Setelah penyerang memiliki nama pengguna dan password, ia kemudian bisa mendapatkan akses dan hak istimewa sehingga ia dapat memiliki akses tak terbatas ke server. Penyerang kemudian dapat menginstal *backdoor* sehingga dia bisa mendapatkan akses di masa depan.

Web server juga menjadi target terhadap serangan fisik. Seseorang bisa mendapatkan akses ke ruang di mana server berada dan menyebabkan kerusakan itu. Setelah seseorang memiliki kontrol fisik atas server, ia mampu melakukan hampir semua hal dengan itu.

b. Ancaman pada Database *(Database Threats)*

E-Commerce Sistem menyimpan data pengguna dan mengambil informasi produk dari database yang terhubung ke server web. Database juga mengandung informasi berharga yang merupakan target besar untuk sebuah serangan. *Trojan horse* dapat mengubah hak akses atau menghapus kontrol akses untuk digunakan pengguna sebagai akses tak terbatas.

c. Pengintaian *(Reconnaissance)*

Mendapatkan sebanyak mungkin informasi tentang jaringan target

penting untuk melakukan serangan yang efektif. Anda akan perlu tahu apa jenis sistem operasi mesin yang digunakan, port apa yang terbuka dan kerentanan dari sistem target. Mengetahui semua informasi yang akan membuat lebih mudah untuk mengeksekusi serangan.

d. *Social Engineering* (Rekayasa Sosial)
Dalam konteks ini 'rekayasa sosial' adalah istilah yang digunakan untuk menggambarkan penggunaan trik psikologis, manipulasi perilaku sering melalui penipuan, oleh penjahat cyber pada pengguna yang tidak curiga untuk mendapatkan 'akses informasi'. Cyber-penjahat bisa orang-orang yang kita already'label 'sebagai hacker dan penipu yang menggunakan rekayasa sosial dalam menghindari mereka dari sarana teknis yang rumit untuk mengakses komputer untuk melakukan kejahatan. Para pengguna menjadi target utama yang terkait dengan sasaran sekunder penjahat cyber ', seperti sistem komputer organisasi; yang pada gilirannya dapat menyebabkan target tersier atau utama seperti program pengendalian sistem, database, sistem keuangan atau telekomunikasi. Penjahat cyber akan mencoba untuk mendapatkan ini 'akses informasi' memungkinkan mereka untuk memotong keamanan. Hal ini dapat mencakup username dan password, PIN (nomor identifikasi pribadi), token dan informasi kartu kredit. Begitu mereka telah mendapatkan akses ke sistem mereka kemudian dapat menghapus, memodifikasi atau menyalin informasi yang sesuai dengan kebutuhan serangan mereka [5].

e. Port Scanning
Setelah semua informasi tentang sistem telah diambil melalui s*ocial engineering* atau cara lain, port scanning digunakan untuk menentukan port yang terbuka pada sistem. Setiap protokol TCP / IP memiliki ribuan port, yang membantu berkomunikasi ke internet. *Port* terbuka seperti pintu terbuka atau jendela untuk rumah Anda. Sebuah *port scanner* yang digunakan untuk memindai *port* sistem dan menghasilkan laporan kepada pengguna tentang status *port* yang ada. *Port scanner* mengirimkan pesan ke komputer untuk meminta akses ke masing-masing *port*. *Port* kemudian mengirimkan sinyal kembali ke *port scanner* dan pemindai dapat menentukan status port tersebut dengan pesan itu. Hal ini mirip dengan pemeriksaan pada semua pintu atau jendela di rumah Anda dalam upaya untuk menemukan satu yang tidak terkunci sehingga ia dapat memperoleh akses ke rumah Anda.

f. Kerentanan Pemindaian *(Vulnerability Scanning)*
Kerentanan pemindaian adalah bagian penting dari serangan karena menunjukkan kelemahan yang berbeda dari sistem target. "Setelah serangkaian diakses jaringan "penyadap" (port) telah diidentifikasi untuk satu set sistem sasaran dan informasi aplikasi yang terkait, berikutnya 'langkah' dalam pelaksanaan serangan biasanya untuk memulai proses identifikasi operasi tertentu sistem dan aplikasi kerentanan [6]. Program komputer yang dibangun sesuai dengan kegunaan dan tetapi tidak terpikirkan dan kehilangan fokus dari masalah keamanan. Setiap program memiliki beberapa kelemahan yang membuatnya rentan terhadap serangan. Setelah kelemahan ditentukan, seorang hacker dapat mengambil keuntungan dan memodifikasi, yang dapat menyebabkan kerusakan pada program atau sistem.

g. Serangan pada server e-Commerce *(E-Commerce Server Attacks)*
Setelah semua informasi telah dikumpulkan, serangan yang sebenarnya dapat berlangsung. Penyerang harus merencanakannya atau serangan yang didasarkan pada keterampilan, peralatan, dan pengetahuan yang dia memiliki. *Hacker* memiliki banyak motif yang berbeda untuk menyerang jaringan dan tidak semua berbahaya. Beberapa *hacker* menyerang jaringan untuk mengeksploitasi kelemahan dan kemudian memperbaiki kelemahan untuk kompensasi. *Hacker* menyerang jaringan lain untuk menguji kemampuan mereka, sementara yang lain ingin mencuri informasi.

h. Serangan secara fisik (*Physical Attacks*)
Serangan fisik tidak memerlukan banyak pengetahuan teknis tapi bisa sama merusak seperti serangan lainnya. Serangan fisik memerlukan akses fisik ke jaringan, yang biasanya dilakukan oleh orang dalam atau s*ocial engineering*. Setelah seseorang memperoleh akses fisik ke server, ia dapat memiliki kontrol penuh atas sistem tersebut. Mencegah seseorang dari mendapatkan akses fisik ke server mungkin yang paling penting, tapi hampir mustahil. *Hacker* jahat juga mungkin karyawan yang memiliki dendam terhadap perusahaan dan ingin merugikan perusahaan itu, mereka bahkan orang yang sebelumnya

menangani jaringan atau administrator keamanan.

i. Malware

Program malware, juga dikenal sebagai perangkat lunak berbahaya, yang dibangun untuk diam-diam menginfeksi komputer target saat membuka program. Malware termasuk virus, *trojan horse*, worm, dan rootkit dan perangkat lunak lain dengan niat jahat. Program Malware dapat menyamar sebagai perangkat lunak yang sah tetapi dapat menyebabkan kerusakan setelah instalasi .

Virus komputer dan worm adalah jenis yang paling umum dari malware . Virus adalah program yang menginfeksi perangkat lunak dieksekusi dan menyebar ke software executable lain ketika program dijalankan. " Secara tradisional, sebuah worm komputer dianggap sebuah aplikasi yang dapat mereplikasi diri melalui koneksi tetap atau jaringan dial - up. Tidak seperti virus, yang masuk ke dalam hard disk komputer atau file sistem, worm adalah program mandiri [7].

Trojan horse dan *rootkit* adalah software yang tidak merusak, yang memungkinkan hacker mengakses secara *remote* dan mendapatkan hak akses administrator. *Trojan horse* memungkinkan pengguna akses terus-menerus ke sistem dan hanya hacker mendapatkan hak user. *Rootkit* memungkinkan *hacker* untuk memiliki akses terus-menerus ke sistem target dan hak akses administrator. *Trojan horse* dan *rootkit* digunakan untuk serangan *denial of service*, pencurian data, memodifikasi file, penyadapan keyboard atau komputer pemantau. Mereka juga digunakan untuk membuat komputer zombie, yang digunakan untuk menyerang komputer lain .

j. *Denial of Service* (DoS)

Banyak perusahaan menjalankan dan bergantung pada jaringan mereka untuk kebutuhan bisnis mereka. Beberapa perusahaan menggunakan jaringan mereka untuk mengirim file dan lain-lain menggunakannya untuk menjual produk. Dalam serangan *denial of service* (DoS), seorang hacker membanjiri jaringan dengan begitu banyak informasi yang menyebabkan kelebihan beban dan menutup sistem. Nama serangan mengatakan itu semua dan menjelaskan apa tujuan dari serangan DoS, yaitu untuk menutup layanan perusahaan.

3. Pembahasan

Komputer dan keamanan informasi sangat penting untuk bisnis, keluarga dan individu untuk tetap dilindungi dari hacker jahat, pelaku penipuan, dan predator online. Dengan semua kejahatan yang mungkin terjadi, keamanan jaringan harus menjadi perhatian utama bagi semua orang, tanpa memandang status. Jika informasi sengaja dihapus, dimodifikasi atau dicuri, bisa menempatkan bisnis keluar dari layanan untuk jangka waktu lama atau bahkan selamanya.

Menjaga kerahasiaan, integritas dan ketersediaan (*Control, Integration and Available* CIA) merupakan tujuan utama dari keamanan jaringan. Berbagai jenis keamanan yang diperlukan untuk mencapai tujuan CIA dan menyediakan sistem perlindungan yang menyeluruh. Metode tersebut mungkin mahal tapi bisa menjadi sia-sia tergantung pada risiko serangan. Meskipun tidak mungkin untuk membuat patch untuk program perlindungan lengkap, masih perlu untuk menerapkan update terbaru dan menginstal patch untuk membuatnya lebih sulit bagi hacker untuk melakukan serangan .

Metode-metode untuk melindungi (*Protection Methods*) sistem e-Commerce antara lain :

3.1. Standar Keamanan

Bisnis, kecil dan besar, diwajibkan untuk mematuhi hukum dan peraturan tertentu yang terkait dengan kegiatan mereka. Perhatian untuk keamanan telah menyebabkan pengembangan standar dan peraturan untuk melindungi data yang berharga.

3.2. ISO 17799

ISO mengadopsi standar awalnya diterbitkan oleh Standard British Institute (BSI). BSI mengeluarkan BS7799 pada tahun 1998 dan kemudian diadopsi oleh ISO sebagai 17799. ISO 17799 memberikan rekomendasi sebagai berikut:

a. Klasifikasi Aset dan Pengendalian Semua aset informasi harus dipertanggung jawabkan dan memiliki klasifikasi keamanan untuk menunjukkan perlunya dan prioritas untuk perlindungan.
b. Personil keamanan Personil harus memberikan pendidikan keamanan yang sesuai dan menyadari prosedur pelaporan insiden.
c. Keamanan Fisik dan Lingkungan
d. Keamanan Jaringan
e. Access Control

3.3. Kebijakan keamanan

Setiap organisasi berkaitan dengan melindungi aset perdagangan elektronik harus memiliki kebijakan keamanan di tempat. Kebijakan keamanan harus menjelaskan dimana aset untuk melindungi dan mengapa, siapa yang bertanggung

jawab untuk perlindungan mereka, dan apa yang diterima dan apa yang tidak. Kebijakan keamanan bertindak sebagai panduan bagi karyawan sehingga mereka tahu apa yang harus dilakukan sebelum, selama dan setelah kejadian. Karyawan semua harus menyadari kebijakan, dan tes dapat dilakukan untuk memastikan kompetensi mereka. Tes bisa dalam berbagai bentuk, seperti tertulis, tes lisan dan berbasis skenario. Pengujian harus dirancang sedemikian rupa sehingga karyawan merasa nyaman dengan informasi dalam kebijakan dan nyaman menanggapi berbagai situasi.

3.4. Keamanan fisik

Keamanan fisik harus jenis pertama keamanan yang diimplementasikan. Ini tidak masuk akal untuk mengamankan komputer Anda dan meninggalkan tempat Anda aman, yaitu hampir sama dengan mengunci pintu rumah Anda, tetapi meninggalkan jendela terbuka. Keamanan fisik bahkan dapat berupa sistem pemantauan video dan perangkat kontrol akses. Meskipun tidak ada cara untuk benar-benar aman, yang terbaik adalah untuk membatasi kemungkinan menjadi korban.

3.5. Akses kontrol

Mengontrol akses ke fasilitas atau daerah di fasilitas merupakan bagian penting dari keamanan. Penjaga keamanan harus digunakan untuk keliling patroli dan verifikasi ID karyawan. Masalah dengan penjaga keamanan adalah bahwa mereka rekayasa manusia dan sosial dapat digunakan untuk memanipulasi mereka. Karena kepedulian sosial rekayasa, kunci, biometrik scanner, dan password juga harus dipertimbangkan untuk kontrol akses.

3.6. Pemantauan (*Monitoring*)

Pemantauan sangat penting karena hacker bisa menyelinap masuk tanpa mengetahui perusahaan dan menyebabkan banyak kerusakan. Fasilitas dan jaringan perlu dipantau untuk mencegah hacker dari penetrasi pertahanan dan menyebabkan kerusakan ireversibel. Dengan pemantauan konstan, keamanan akan mampu mendeteksi serangan dan menghentikannya sebelum terjadi kerusakan. Hal ini lebih baik untuk mengambil langkah-langkah untuk mencegah sesuatu dari terjadi daripada mencoba untuk memperbaiki kerusakan kemudian. Beberapa hal yang dapat rusak diperbaiki dan informasi penting bisa hilang selamanya.

3.7. Otentikasi

Berbagai metode verifikasi yang digunakan oleh lembaga yang berbeda untuk mencegah pengguna yang tidak sah dari mengakses fasilitas mereka, sistem, dan jasa.

3.8. Biometrik

Biometrik menggunakan tubuh seseorang untuk verifikasi akses. Scan retina, jari dan pembaca cetak telapak, dan scanner tubuh lainnya digunakan untuk kontrol akses untuk memverifikasi identitas seseorang. Biometrics adalah baik karena menggunakan bagian tubuh yang unik untuk individu tersebut. Masalah dengan biometrik datang ketika seseorang merusak bagian mereka dari tubuh yang digunakan untuk verifikasi. Jika seseorang merusak bagian tubuh yang digunakan untuk verifikasi, itu akan membutuhkan kerja ekstra dan administrator harus menggunakan sarana yang berbeda untuk memungkinkan orang akses.

3.9. *Usernames and Passwords*

Username dan password pengguna memilih identitasnya, yang biasanya memiliki persyaratan tertentu yang ditetapkan oleh administrator. Persyaratan harus diatur karena orang akan menggunakan password yang umum dan hacker dapat istirahat mereka. "The password yang paling aman adalah minimal 8 karakter dengan campuran atas dan huruf kecil dan simbol dan angka. Semakin panjang password, dan lebih acak pemilihan karakter dan angka, semakin kuat password "[8].

Masalah dengan password dan username adalah bahwa orang baik melupakan mereka atau mereka menuliskannya dan menempatkan mereka di tempat di mana orang dapat menemukan mereka.

3.10. Smartcard

Smartcard digunakan dalam banyak fasilitas untuk mengontrol akses ke daerah tertentu, sistem, atau jasa. Smartcard memungkinkan akses seseorang tanpa harus mengingat password. Masalah dengan banyak smartcard adalah bahwa orang kehilangan mereka dan orang lain mungkin bisa menggunakannya.

3.11. Wireless Security

Pengguinaan jaringan komputer dengan kabel sudah jarang digunakan, sekarang bisnis menggunakan koneksi nirkabel untuk mengirim, menerima dan akses informasi. Mengirim dan menerima informasi secara nirkabel membuatnya rentan untuk ditangkap. Sistem dapat mengirim dan menerima informasi melalui router nirkabel yang terhubung ke modem yang terhubung ke Internet. Komputer mengirimkan paket ke router nirkabel, yang kemudian transfer yang ke modem dan melalui Internet.

3.12. 802.1X Standard

802.1x menyediakan akses nirkabel ke jaringan kabel. "Keseluruhan kerangka kerja untuk menyediakan kontrol akses untuk jaringan adalah apa yang disebut sebagai sistem otentikasi berbasis pelabuhan, yang sebagian orang sebut sebagai 802.1X". Karena keamanan ditingkatkan, 802.1x adalah standar nirkabel yang dianjurkan. "Jenis terkuat otentikasi nirkabel yang tersedia saat ini, IEEE 802.1x otentikasi menyediakan otentikasi yang paling kuat untuk WPA2 Perusahaan Model WLAN" (Ciampa, 2009). 802.1x menyediakan fitur kontrol akses seperti penyaringan Alamat MAC, kunci enkripsi WPA2 akses, dan kemampuan untuk mematikan broadcast SSID. Meskipun 802.1x adalah standar nirkabel yang dianjurkan karena masalah keamanan, masalah dengan 802.1x adalah biaya untuk menerapkan dan memelihara [9].

3.13. Cryptography

Kriptografi digunakan untuk mengubah plaintext menjadi algoritma yang dikenal sebagai ciphertext, yang merupakan urutan matematika yang kompleks terbaca bagi siapa pun tanpa kode untuk memahaminya. Setelah data dienkripsi menjadi ciphertext, itu diberikan password dan password yang dibutuhkan untuk mendekripsi data dan mengubahnya kembali menjadi plaintext. Data yang dapat dikirim ke orang lain selama orang yang memiliki password untuk mendekripsi informasi. Jenis algoritma menentukan kekuatan enkripsi dan dapat membuatnya lebih atau kurang sulit untuk mendekripsi tanpa kunci yang tepat. Kriptografi juga digunakan untuk membuat tanda tangan untuk dokumen, yang membantu untuk menentukan keaslian dokumen itu [10].

3.14. Hashing

Hashing adalah cara untuk menciptakan tanda tangan unik untuk sebuah dokumen untuk membuktikan bahwa dokumen tersebut adalah dokumen asli. Hal ini penting untuk mencegah seseorang dari menyalin dokumen. Jika seseorang melakukan copy dokumen, hash yang sama dari aslinya tidak akan di copy. Hashing digunakan untuk membandingkan dokumen untuk memastikan itu adalah asli. Jenis yang paling aman dari hash adalah Secure Hash Algorithm (SHA), yang menggunakan enkripsi 160 bit [11].

3.15. Enkripsi Simetrik

Enkripsi simetris menggunakan kunci tunggal untuk mengenkripsi dan mendekripsi data dan menggantikan setiap huruf dan angka dalam dokumen dengan yang lain dalam urutan acak sehingga hampir tidak mungkin untuk memecahkan kode tanpa kunci. Advanced Encryption Standard (AES) adalah enkripsi simetris terbaru dan paling aman di pasar. "Setelah proses panjang yang memerlukan kerja sama dari pemerintah AS, industri, dan pendidikan tinggi, lima finalis terpilih, dengan pemenang akhir yang algoritma yang dikenal sebagai Rinjdael, yang lebih sering disebut sebagai AES" [9]. Masalah dengan enkripsi simetris adalah bahwa ia menggunakan kunci tunggal, yang lulus sekitar dan diharapkan akan terus aman.

3.16. Enkripsi Asimetrik

Meskipun keduanya masih digunakan sampai sekarang, kriptografi asimetris jauh lebih aman daripada kriptografi simetrik. "Cipher asimetris jauh lebih matematis kompleks daripada cipher simetris". Berbeda dengan kriptografi simetrik, kriptografi asimetris memiliki lebih dari satu kunci, yang dikenal sebagai kunci publik dan *private*. Penggunaan banyak kunci baik untuk alasan keamanan tetapi bisa membingungkan mana yang akan digunakan [10].

3. 17. EAP-TLS (Transport Layer Security)

EAP - TLS umumnya dianggap sebagai yang terkuat yang tersedia dan yang paling mahal untuk diterapkan. Ini menyediakan otentikasi sertifikat timbal balik antara klien dan server, menggunakan protokol TLS standar (keturunan dari protokol SSL digunakan untuk mengamankan sebagian besar transaksi Web). " Ini adalah protokol *client / server* yang ditumpuk di atas sebuah protokol lapisan transport yang dapat diandalkan, seperti TCP dalam kasus TCP / IP dan terdiri dari dua lapisan yang sama dan protokol SSL sebagai " [12]. Server menggunakan TLS untuk menunjukkan bahwa ia memegang sertifikat digital dan meminta yang sama dari klien. Klien menggunakan sertifikat untuk membuktikan identitas dan material kunci dipertukarkan. The TLS terowongan berakhir setelah otentikasi telah selesai. Tombol disampaikan oleh EAP-TLS dapat digunakan untuk mengenkripsi data dengan *Advanced Encryption Standard* (AES), *Temporal Key Integrasi Protocol* (TKIP) atau *Wired Equivalent Privacy* (WEP). EAP-TLS adalah cocok di mana klien WLAN telah memiliki sertifikat digital atau di mana keamanan yang tinggi perlu membenarkan investasi dalam infrastruktur kunci publik untuk mengelola sertifikat tersebut.

3.18. EAP-TTLS (Tunneled TLS)

Ini jenis EAP menyeimbangkan biaya keamanan vs penyebaran dengan mengganti sertifikat client-side dengan metode otentikasi password legacy seperti PAP, CHAP dan MSCHAPv2. EAP - TTLS memerlukan server untuk mengotentikasi diri dengan sertifikat dan membangun melalui terowongan TLS yang diakses oleh klien. Terowongan TLS digunakan untuk melindungi metode otentikasi yang kurang aman. Bahkan ketika password teks yang jelas dikembalikan, terowongan TLS mengaburkan respons klien. Untuk menghindari mengekspos nama klien, EAP-TTLS harus dikonfigurasi untuk mengirim " anonim " identitas ketika 802.1X dimulai, kemudian mengirim identitas yang sebenarnya melalui terowongan TLS. terowongan yang berakhir ketika otentikasi selesai dan tombol disampaikan. " EAP - TTLS telah banyak digunakan, dan itu mungkin ditemui di banyak perusahaan WLAN. Sementara EAP-TTLS hampir identik dengan EAP-PEAP, tidak menikmati dukungan asli untuk sistem operasi Ms Windows, yang telah menghasilkan penetrasi pasar yang relatif jauh lebih sedikit " [13].

3.19. PEAP (Protected EAP)

PEAP sangat mirip dengan EAP-TTLS tetapi menggunakan protokol otentikasi klien yang berbeda. Seperti EAP-TTLS, PEAP membentuk terowongan TLS melalui sertifikat server-side. Meskipun kredensial pengguna yang sama dapat digunakan dengan EAP-TTLS, server otentikasi PEAP harus mampu mengurai baik EAP dan protokol otentikasi sebelumnya terkandung. Hari ini, PEAP lebih luas didukung dari EAP-TTLS karena dianggap sangat aman. Pilihan terbaik untuk jaringan Anda tergantung pada jenis klien yang digunakan dalam WLAN dan anggaran Anda.

3.20. WPA2 AES Passphrase

Modus Kunci pra-berbagi (PSK) tidak memerlukan kompleksitas sebuah server otentikasi 802.1x. Setiap perangkat jaringan nirkabel mengenkripsi lalu lintas jaringan menggunakan kunci 256-bit. Kunci ini dapat dimasukkan baik sebagai string dari 64 digit hex, atau sebagai passphrase 8 sampai 63 karakter ASCII. "Dalam kriptografi, *Advanced Encryption Standard* (AES) adalah standar enkripsi kunci simetris yang diadopsi oleh pemerintah AS. Standar ini terdiri dari tiga blok cipher, AES-128, AES-192 dan AES-256, diadopsi dari koleksi yang lebih besar awalnya diterbitkan sebagai Rijndael. Masing-masing cipher ini memiliki ukuran blok 128-bit, dengan ukuran kunci 128, 192 dan 256 bit, masing-masing "(McBewster, Miller, & Vandome, 2009). AES cipher telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya *Data Encryption Standard* (DES) [14].

3.21. *Digital Certificates*

Sertifikat digital mengesahkan kepemilikan kunci publik dengan nama subjek sertifikat. Hal ini memungkinkan orang lain untuk bergantung pada tanda tangan atau pernyataan yang dibuat oleh kunci pribadi yang sesuai dengan kunci publik yang disertifikasi. Dalam model ini hubungan kepercayaan, sebuah CA adalah pihak ketiga yang terpercaya yang dipercaya oleh kedua subjek (pemilik) sertifikat dan pihak mengandalkan sertifikat (IBM). Sertifikat digital digunakan untuk berkomunikasi melalui Internet menggunakan protokol aman seperti HTTPS.

3.22. Firewalls

Firewall adalah sebuah perangkat lunak atau konfigurasi hardware. Tujuan utama dari firewall adalah untuk mengontrol lalu lintas jaringan internal inbound dan outbound. Hal ini seharusnya memberikan atau menolak akses ke jaringan pribadi. Firewall dapat digunakan untuk membatasi sistem dari hanya menyediakan satu set kecil jasa. Tiga jenis *firewall* adalah :

a. *Packet-filtering, firewall* ini memeriksa sumber dan alamat tujuan paket. Mereka memastikan paket yang diterima dari luar dalam menanggapi yang dikirim.
b. *Gateway Proxy, firewall* ini bertindak sebagai gateway untuk pengguna di luar menghubungkan ke jaringan. Pengguna di luar harus terlebih dulu menyambung ke firewall gerbang sebelum dapat terhubung ke jaringan.
c. *Proxy* Aplikasi, *firewall* ini memeriksa permintaan pengguna untuk terhubung ke server aplikasi. Mereka memastikan bahwa permintaan pengguna sesuai dengan protokol aplikasi.

Komponen-komponen sistem e-commerce harus dikonfigurasi untuk memungkinkan sistem atau server di jaringan internal untuk memulai koneksi dengan jaringan. *Firewall* dapat digunakan untuk membatasi server atau sistem pada jaringan dari memulai koneksi ke jaringan internal [14].

3.23. *Computer Intrusion Detection and Prevention Systems*

Computer Intrusion Detection dan Sistem Pencegahan yang mirip dengan memiliki

detektor gerakan pada bangunan dan kunci di pintu dan jendela. *Computer Intrusion Detection* (IDS) *System*, mirip dengan detektor gerakan, dimaksudkan untuk mendeteksi penyerang potensial dan seseorang waspada untuk mengambil tindakan. *The Intrusion Prevention System* (IPS), mirip dengan kunci di pintu dan jendela, dimaksudkan untuk menjaga penyerang keluar. Nama-nama dari kedua sistem untuk meringkas apa yang mereka masukkan. Untuk memiliki program keamanan yang baik, Anda perlu kedua sistem perlindungan di tempat, satu untuk deteksi dan yang lainnya untuk pencegahan aktivitas berbahaya. Banyak sistem hari ini menggabungkan kedua deteksi dan pencegahan ke dalam satu sistem dan dikenal sebagai *Intrusion Detection* and *Prevention Systems* (IDPS) [16].

4.22. *Encrypting For E-Mail*

E-mail adalah salah satu yang diintip pada kunjungan ke inbox Anda. Untuk memastikan keamanan, Anda dapat menggunakan program seperti *Hush mail* atau surat M Ute yang secara otomatis mengenkripsi semua email yang Anda terima dan dikirim. Bisa juga diamankan dengan PGP (*Pretty Good Privacy*).

4.23. Penggunaan Filter (*Use Filter*)

Beberapa perusahaan seperti Vent, Web sense dan VeriTest dan perusahaan lain menawarkan sistem untuk tujuan pemantauan dimana data dari jaringan Anda, dan kemudian secara otomatis mencegah data sensitif [17].

4.24. Keamanan Pembayaran

Rekber (rekening bersama) adalah suatu instansi yang berperan sebagai perantara dalam terjadinya transaksi online. Sebenarnya rekber itu cuma istilah saja. Diluar negeri istilah ini dikenal dengan nama *ESCROW SERVICE*.

Dalam hal ini, rekber berperan sebagai pihak ketiga dalam arah pergerakan uang antara pembeli dan penjual. Berarti, arah pergerakan uang yang semula dari pembeli langsung ke penjual kini diperantarai oleh rekber, agar penjual tidak langsung menerima uang dari pembeli. Setelah produk diterima dan disetujui oleh si pembeli, maka rekber yang akan mengirimkan uangnya ke penjual [18].

4. Kesimpulan

E-commerce adalah cara yang efektif untuk melakukan bisnis. Hal ini memungkinkan perusahaan untuk menyediakan produk dan layanan kepada populasi yang lebih luas daripada yang mereka lakukan dengan cara tradisional. Namun, e-commerce juga memiliki berbagai risiko yang perlu dikurangi untuk beroperasi dengan aman. Tindakan pencegahan sebanyak mungkin untuk melindungi sistem, bahkan itu berarti menghabiskan uang ekstra untuk melakukannya. Sebenarnya tidak ada cara benar-benar mengamankan jaringan, tetapi ada cara untuk meminimalkan kemungkinan menjadi korban. Membatasi kemungkinan menjadi korban adalah lebih baik daripada mencoba untuk memperbaiki kerusakan setelah serangan, yang mungkin tidak dapat diperbaiki. Metode Pengamanan e-Commerce ada 24 antara lain : Standar Keamanan, ISO 17799, Kebijakan keamanan, Keamanan fisik, Akses kontrol, Pemantauan (*Monitoring*), Otentikasi, Biometrik, *Usernames and Passwords*, Smartcard, Wireless Security, 802.1X Standard, Cryptography, Hashing, Enkripsi Simetrik, Enkripsi Asimetrik, EAP-TLS, EAP-TTLS, PEAP (Protected EAP), WPA2 AES Passphrase, *Digital Certificates*, Firewalls, *Computer Intrusion Detection and Prevention Systems*, *Encrypting For E-Mail*, Penggunaan Filter (*Use Filter*), Keamanan Pembayaran. Metode tersebut bisa digunakan satu atau digabungkan dalam sisttem e-Commerce untuk keamanan jaringan dan melindungi sistem.

Daftar Pustaka

[1] Turban, E., Rainer, R.K.Jr., and Potter, R.E. (2005). *Introduction to Information Technology*, New York: John Wiley & Sons, Inc

[2] Ariyus, Doni. (2006). *Computer Security*, Penerbit Andi, Yogyakarta.

[3] Segal, A. & Thorne, J., (2006). Identity Theft: The New Way to Rob Banks. URL:http://articles.cnn.com/2006-05-18/us/identity.theft_1_identity-theft-bank-employee-bank-heist?_s=PM:US diakses tanggal 20 Dec 2015

[4] Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G., and Williams, T. (2011). Gray Hat Hacking, The Ethical Hacker's Handbook, Third Edition, McGraw Hill

[5] Guenther M. (2001) 'Social Engineering – Security Awareness Series'; Information Warfare Site U.K. URL : (http://www.iwar.org.uk/comsec/resources/sa-tools/Social-Engineering.pdf) diakses tanggal 20 Dec 2015

[6] Young, S. (2004). Hacker's Handbook: The Strategy Behind Breaking Into and Defending Networks.Boca Raton, FL: Auerbach Publications

[7] Brenton, C. (2003). *Mastering Network Security. 2nd ed*. Alameda, CA: Sybex

[8] Failor, D. (2009). InsidersChoice to CompTIA Security+ Certification Exam SY0-201 and Exam BRO-001. Friendswood, TX: TotalRecall Publications, Incorporated

[9] Ciampa, M. (2009). *CompTIA Security+ 2008 In Depth*. Boston, MA: Course Technology.

[10] Dent, A., Mitchell, C. (2005). *User's Guide to Cryptography and Standards. Norwood*, MA: ArtechHouse, Incorporated.

[11] Mcbewster, J., Miller, F., & Vandome, J.(2009). *Advanced Encryption Standard*. Alphascript Publishing.

[12] Oppliger, R. (2009). SSL and TLS: *Theory and Practice. Artech House.*

[13] *Wescott, D. (2010). CWSP Certified Wireless Security Professional Official Study Guide*. Sybex Publishing.

[14] Strebe, M. (2004). *Network Security Foundations*. Alameda, CA: Sybex, Incorporated.

[15] Nahari, H., & Krutz, R. (2011). *Web Commerce Security: Implementation and Design.* Wiley Publishing

[16] Rahman, S.M. & Lackey, R. (2013). *E-Commerce Systems Security For Small Businesses, Proceding International Journal of Network Security & Its Applications* (IJNSA), Vol.5, No.2, March 2013 page 193-210

[17] Juncai, Shen and Shao, Qian. (2011), *Based on Cloud Computing E-commerce Models and Its Security, International Journal of e-Education, e-Management and e-Learning*, Vol.1.No.2

[18] Crowguard. (2011), URL:http://blog.crowguard.com/pengertian-definisi-lengkap-rekber-rekeningbersama/ diakses tanggal 20 Dec 2015