Security System Layanan Internet Banking PT BANK MANDIRI (Persero) Tbk.

Rialda Annisya[1], Maynina Norshela Hastuti[2]

Abstrct - ***How many banking services that bank provide to their clients for customer satisfaction. One of the services who begant to demand nowadays is Internet Banking. With this service, customer can perform many kind of banking transaction easier, as simple as browsing they only need Internet Access. It is easier for customer especially for those who are very busy to maintain their finance. In this service, Internet Access must be safe from people whom irresponsible. Therefore, this type of service using a variety of security methods to take cares the privasi and customer data. Security System usually involves Secure Socet Layer (SSL, cryptography Public Key and Digital Signature). However, do all this security service is 100% safe?In this case, the author will analyze the security data and methods that used by Bank Mandiri in Mandiri Internet Banking, so it will be conclude based on theory and analysis, the quality of security is applied to this service.***

Index – Term : internet banking, security, reduce risk

I. Pendahuluan

1.1 Latar Belakang

Dewasa ini Teknologi informasi sudah merupakan suatu kebutuhan yang sangat penting, bahkan sebagai tuntutan yang mendesak bagi setiap orang untuk menyelesaikan semua permasalahan dengan cepat serta meringankan semua pekerjaannya.Seiring dengan situasi seperti ini, perkembangan teknologi informasi terutama peranan komputer mendapatkan perhatian yang sangat serius.Teknologi informasi ini memberi dampak luar biasa dalam dunia perbankan saat ini.

Akhir-akhir ini banyak sekali perubahan pada teknologi informasi, demikian juga di bidang telekomunikasi, kebanyakan disebabkan karena adanya desakan dan dasyatnya kompetisi di dunia perbankan saat ini. Perkembangan teknologi ini semakin hari semakin pesat, akan tetapi apakah kita siap atau tidak dalam mengikuti perkembangan teknologi tersebut.

Perkembangan teknologi informasi menciptakan jenis-jenis dan peluang-peluang bisnis yang baru dimana transkasi-transaksi bisnis makin banyak dilakukan secara elektronika.Berkaitan dengan perkembangan teknologi informasi tersebut memungkinkan setiap orang dengan mudah melakukan transaksi perbankan. Perkembangan internet memang cepat dan memberi pengaruh signifikan dalam aspek kehidupan kita.

Penggunaan internet tidak hanya terbatas pada pemanfaatan informasi yang dapat diakses melalui media , melainkan juga dapat digunakan sebagai sarana untuk melakukan transaksi perbankan. Bank indonesia mulai memasuki dunia maya yaitu *internet banking* atau yang lebih dikenal *E-Banking,* yang merupakan bentuk layanan perbankan secara elektronik melalui media *E-Banking*pada dasarnya merupakan susatu kontrak trasaksi antara pihak bank dan nasabah yang memberikan manfaat berganda dengan menggunakan media internet.Transaksi perbankan dapat dilakukan kapan dan dimana saja tanpa dibatasi tempat dan waktu. Semakin relevannya teknologi internet di dunia bisnis, maka Perbankan Nasional dapat mengadopsi dan mengeksploitasi keunggulan internet dalam menjawab tantangan yang ada saat ini.

Melihat hal tersebut, maka PT. Bank Mandiri (Persero) Tbk.mencoba menjaring nasabah dan mempertahankan nasabah yang ada dengan meluncurkan suatu fasilitas Internet Banking.Penggunaan Internet Banking ini diharapkan dapat memenuhi kebutuhan layanan yang baik bagi nasabah, dengan dukungan SDM Perbankan yang profesional serta kemampuan menguasai dan melayani nasabah dengan produk-produk inovatif tersebut.

Strategi untk menghadapi persaingan dalam dunia perbankan pada umumnya serta sebagai peningkatan mutu layanan kepada nasabah pada khususnya, maka dengan ini penulis akan membahas *security*layanan *internet banking*Mandiri sebagai salah satu pemenuhan tanggung jawab Mandiri dalam memberikan layanan yang unggul yang di terapkan oleh Mandiri, dan kami menetapkan **"Security System Layanan Internet Banking PT BANK MANDIRI (Persero) Tbk"** sebagai tema dan sekaligus menjadi judul dalam penyusunan *paper* ini.

Internet Banking kini bukan lagi istilah yang asing bagi masyarakat Indonesia khususnya yang tinggal di wilayah perkotaan.Hal tersebut disebabkan semakin banyaknya perbankan nasional yang menyelenggarakan layanan tersebut.Di masa mendatang, layanan ini tampaknya sudah bukan lagi sebuah layanan yang akan memberikan *competitive advantage* bagi bank yang

1. rialdaannisya@gmail.com
2. mayninanorshela@yahoo.com
Institut Manajemen Telkom

menyelenggarakannya.Keadaannya akan sama seperti pemberian fasilitas ATM. Semua bank akan menyediakan fasilitas tersebut.

Penyelenggaraan Internet Banking yang sangat dipengaruhi oleh perkembangan teknologi informasi, dalam kenyataannya pada satu sisi membuat jalannya transaksi perbankan semakin mudah, akan tetapi di sisi yang lain membuatnya juga semakin berisiko. Dengan kenyataan seperti ini, faktor keamanan harus menjadi faktor yang paling perlu diperhatikan. Bahkan mungkin faktor keamanan ini dapat menjadi salah satu fitur unggulan yang dapat ditonjolkan oleh pihak bank.Diskusi ini mencoba mengidentifikasi berbagai permasalahan tersebut dan alternatif pemecahannya.

1.2 Rumusan Masalah

Setelah melihat latar belakang masalah dan berdasarkan penelitian yang dilakukan, maka penulis dapat mengidentifikasi permasalahan yang sedang dihadapi oleh Bank Mandiriyaitu :

1. Ancaman keamanan atau resiko apa saja yang berkaitan dengan aktivitas *Internet Banking*Mandiri?
2. Bagimanasistem keamanan *Internet Banking*Mandiri?
3. Penanggulangan ancamanapa yang dapat digunakan untuk mengurangi resiko sistem keamanan *Internet Banking* Mandiri?

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini adalah sebagai berikut:

1. Untuk mengetahui ancaman keamanan atau resiko yang berkaitan dengan aktivitas *Internet Banking* Mandiri.
2. Untuk mengetahui sistem keamanan *Internet Banking* Mandiri.
3. Untuk mengetahui penanggulangan ancaman yang digunakan untuk mengurangi resiko sistem keamanan *Internet Banking* Mandiri.

2.1 Teori Pendukung

Dalam pembahasan mengenai *Security System* Layanan Internet Banking PT Bank Mandiri (Persero) Tbk. ini digunakan beberapa teori penunjang:

2.1.1 Pengertian *Internet Banking*

Persaingan dalam perbankan harus dapat diimbangi dengan peninfgkatan pelayanan bank kepada para nasabah, sehingga nasabah tersebut tidak tertarik untuk menggunakan jasa bank lain. Salah satu jenis pelayanan yang dapat bank berikan adalah *internet banking*, walupun saat ini internet banking bukanlah menjadi satu-satunya keunggulan bersaing sebab semua perbankan telah menggunakan layanan *internet banking.*

Menurut David Whiteley (Harahap, Khairil Aswan : 43), *Internet Banking* disefinisikan sebagai salah satu jasa pelayanan yang diberikan bank kepada nasabahnya dengan maksud agar nasabah dapat mengecek saldo rekeningnya dan membayar tagihan selama 24 jam tanpa perlu datang ke kentor cabang.

Internet Banking merupakan salah satu produk perbankan elektronik yang ditawarkan untuk memberikan kemudahan bagi nasabah dalam melakukan transaksi perbankan non-tunai melalui komputer dan jaringan internet. Pada prinsipnya layanan internet banking hamper serupa dengan layanan ATM.

2.1.2 Sistem Keamanan *Internet Banking*

Kesempatan Indonesia untuk mengembangkan *internet banking* sangat terbuka luas.Hal itu dimungkinkan karena pertumbuhan penggunaan internet di kawasan Asia sangat tinggi dan nasabah perbankan memerlukan layanan yang lebih lagi.

Salah satu isu yang menjadi permasalahan dalam penggunaan *internet banking* adalah sistem kemanan bertransaksi perbankan dengan menggunakan internet.Masalah yang sering muncul adalah adanya pencurian nomor kredit dan MITM Attack. MITM attack adalah serangan dimana attacker berada di tengah bebas mendengarkan dan mengubah percakapan antara dua pihak.Sedangkan pencurian dalam nomor kredit, nomor curian kemudian dimanfaatkan oleh orang yang sesungguhnya tidak berhak.Nasabah harus diyakinkan oleh pihak bank bahwa transaksi perbankan berjalan aman karena bank bersangkutan memiliki perangkat keamanan untuk mencegah para hacker mengganggu transaksi mereka.

Menurut Gary Lewis dan Kenneth Thygerson (Harahap, Khairil Aswan : 52), ada dua jenis sistem keamanan yang dipakai dalam internet banking, antara lain:

1. **Sistem *Cryptography***

   Sistem ini menggunakan angka-angka yang dikenal dengan kunci *(key)*.Sistem ini disebut juga dengan sistem sandi.Ada dua tipe *cryptography*, yaitu simetris dan asimetris. Pada sistem simestris menggunakan kode kunci yang sama bagi penerima dan pengirim pesan. Kelemahan dari *cryptography simestris* adalah kunci ini harus dikirim pada pihak penerima dan hal ini memungkingkan seseorang untuk mengganggu di tengah jalan.Sistem *cryptography asimetris* juga mempunyai kelemahan yaitu jumlah kecepatan pengiriman data menjadi berkurang karena adanya tambahan kode.Sistem ini biasanya digunakan untuk mengenali nasabah dan melindungi informasi finansial nasabah.

2. Sistem *Firewall*

Firewall merupakan sistem yang digunakan untuk mencegah pihak-pihak yang tidak diijinkan untuk memasuki daerah yang dilindungi dalam unit pusat kerja perusahaan. *Firewall* berusaha untuk mencegah pihak-pihak yang mencoba masuk tanpa ijin dengan cara melipatgandakan dan mempersulit hambatan-hambatan yang ada. Namun, yang perlu diingatkan adalah bahwa sitem *firewall* ini tidak dapat mencegah masuknya virus atau gangguan yang berasala dari dalam perusahaan itu sendiri.

Aspek keamanan komputer mempunyai beberapa lingkup yang penting, yaitu:

a. Privacy & Confidentiality

Hal yang paling penting dalam aspek ini adalah usaha untuk menjaga data dan informasi dari pihak yang tidak diperbolehkan mengkasesnya.*Privacy* lebih mengarah kepada data-data yang sifatnya privat.Sebagai contoh, email pengguna yang tidak boleh dibaca admin.Sedangkan *confidentiality*berhubungan dengan data yang diberikan kepada suatu pihak untuk hal tertentu dan hanya diperbolehkan untuk hal itu saja. Contohnya, daftar pelanggan sebuah ISP.

b. Integrity

Aspek ini mengutamakan data atau informasi tidak boleh diakses tanpa seizin pemiliknya. Sebagai contoh, sebuah email yang dikirim pengirim seharusnya tidak dapat dibaca orang lain sebelum sampai ke tujuannya.

c. Authentication

Hal ini menekankan mengenai keaslian suatu data/informasi, termasuk juga pihak yang memberi data atau mengaksesnya tersebut merupakan pihak yang dimaksud.Contohnya seperti penggunaan PIN atau *password.*

d. Availability

Aspek yang berhubungan dengan ketersediaan informasi ketika dibutuhkan.Sebuah sistem inofrmasi yang diserang dapat menghambat ketersediaan informasi yang diberikan.

e. Access Control

Aspek ini berhubungan dengan cara pengaksesan informasi. Hal ini biasanya berhubungan dengan klasifikasi data *(public, private confidential, top secret)*&*user* (*guest, admin, top manager*, dsb.), mekanisme authentication dan juga *privacy.* Seringkali dilakukan dengan menggunakan kombinasi *user ID* atau *password*dengan metode lain seperti kartu atau *biometrics.*

f. Non-Repudiation

Hal ini menekankan agar sebuah pihak tidak dapat menyangkal telah melakukan transaksi atau pengaksesan data tertentu.Aspek ini sangat penting dalam hal *e-commerce.* Sebagai contoh, seseorang yang mengirim email pemesanan barang tidak dapat disangkal telah mengirim email tersebut.

2.1.3 Pengaturan Internet Banking di Indonesia

UU ITE kini mampu mengatuir sistem internet banking sebagai salah satu layanan perbankan yang merupakan wujud perbankan teknologi informasi.Kendala seperti aspek teknologi dan aspek hukum kini bukan lagi menjadi faktor penghambat sistem *internet banking* di Indonesia.

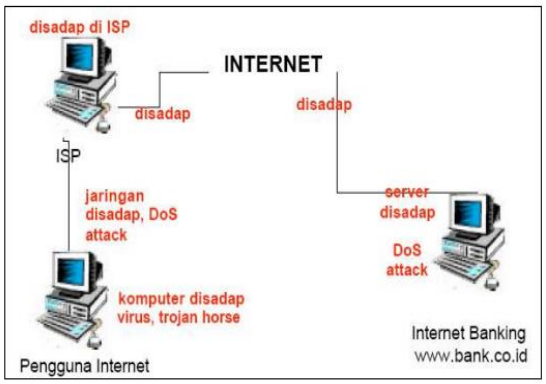
Dalam surat keputusan Direksi Bank Indonesia No. 27/164/KEP/DIR dan surat edaran Bank Indonesia No. 27/9/UPPB tanggal 31 Maret 1995 mengenai pengguanan sistem informasi oleh bank dapat dilihat bahwa pelaksanaan tenologi sistem informasi diserahkan kepada masing-masing bank. Bank Indonesia hanya memberikan pedoman sehingga di dalam pelaksanaannya tidak merugikan nasabah dan bank itu sendiri. Pada bagian III pasal 1 surat edaran Bank Indonesia No. 27/9/UPPB tanggal 31 Maret 1995, disebutkan bahwa tujuan pengamanan teknologi sistem informasi adalah untuk mengurangi resiko penyelenggaraan teknologi sistem informasi yang dapat merugikan yang dapat merugikan kepentingan bank dan masyarakat.

2.1.4 Ancaman pada Internet Banking

Pada dasarnya layanan *Internet Banking*menggunakan Internetsebagai media komunikasi, maka keamanan dari layanan *Internet Banking* bergantung kepada keamananan dari Internet. Internet pada mulanya dikembangan di lingkungan akademis (pendidikan dan penelitan).

Teknologi Internet yang digunakan saat ini bergantung kepada sebuah teknologi yang disebut IP *(Internet Protocol)* versi 4.IPv4 ini memiliki beberapa kelemahan ditinjau dari segi keamanan yang sudah diperbaiki di versi 6 (IP v6).Namun sayangnya IPv6 belum lazim dipergunakan.

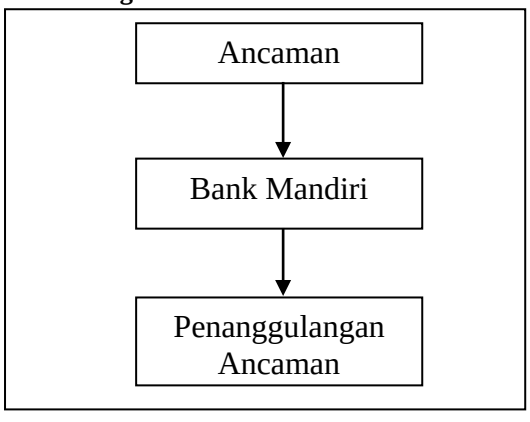
Gambar 2.1
Titik rawan dalam hubungan internet



Dapat dilihat pada gambar 2.1, pengguna terhubung dengan jaringan internet melalui layanan *Internet Service Provider (ISP).* Biasanya, koneksi menggunakan modem, DSL, kabel modem, wireless, maupun dengan *leased line*. Lalu ISP akan menghubungakan pengguna ke internet melalui penyedia jaringan *(network provider).*Hal ini juga berlaku pada layanan *Internet Banking.*Server akan terhubung ke internet melalui ISP atau penyedia jaringan lainnya.

Dari gambar 2.1, dapat ditunjukkan pula potensi celahkeamanan yang yang dapat terjadi. Dari sisi pengguna, komputer miliknya dapat disisipkan virus atau Trojan sehingga data – data di dalamnya dapat diubah atau diambil. Dari sisi ISP, apabila sistem keamanannya rentan, maka seorang cracker dapat menbobolnya dan dapat mengambil data pelanggan ISPnya. Dari sisi penyedia layanan *Internet Banking*-pun juga terdapat potensi celah keamanan.Salah satu yang terjadi kasus di Amerika seorang *cracker*menjebol institusi keuangan dan mengambil data nasabah dari berbagai bank. Begitu pula dari sisi jalur ISP dan pengguna, biasanya hal ini terjadi di tempat umum, seperti warnet. Pengguna warnet dapat disadap informasinya dari pemilik warnet yang tidak bertanggung jawab.

2.2 Kerangka Pemikiran



Gambar 2.2
Kerangka Pemikiran

3.1 Analisis dan Pembahasan

3.1.1 Ancaman Internet Banking Mandiri

Secara umum, hal yang paling sering diserang para penyusup untuk masuk ke dalam sebuah situs yang terproteksi adalah dengan mendapatkan akses masuknya, atau sisi Autentikasi.Karena hanya dengan mengetahu user ID dan password kita dapat melakukan apapun yang kita inginkan. Dalam pengujian keamanan layanan ini, penulis akan mencoba melakukannya dengan dua cara, yaitu dengan menggunakan perangkat lunak *keylogger*dan proses *sniffing.*

a. Active dan Passive Snifing

Snifing merupakan sebuah aksi penyadapan paket data yang dikirimkan sebuah komputer ke server tertentu. Terdapat dua jenis aksi *sniffing*, yaitu *passive* dan *active*. Perbedaannya hanyalah jika *active* melakukan aksi perubahan paket data dalam melakukan *sniffing*, sedangkan *passive* tidak.

Perlu diperhatikan bahwa metode *sniffing*jenis ini dapat dikategorikan sebagai *cyberlaw*, jika penggunaannya tidak pada tempatnya.

b. Keylogger

*Keylogger*merupakan sebuah produk yang dapat mengetahui aktivitas apa saja yang terjadi pada komputer yang isisipinya. Pembuat produk ini berargumen bahwa *keylogger* sangat berguna untuk memantau perkembangan kerja karyawan perusahaan, mengetahui apa yang dilakukan anak ketika brosing di Internet dan sebagainya.

Jenis *keylogger* ada 2 yaitu, perangkat lunak &*hardware*. Keduanya mempunyai tujuan yang sama dengan karakteristik yang berbeda. Jenis *hardware* biasanya dipasang secara fisik pada komputer, merekam segala aktivitas yang diketikkan *keyboard*.Sedangkan jenis perangkat lunak, diinstal di sistemoperasi kompueter dan dijalankan, biasanya secara tersembunyi.

c. Typo site

Pelaku membuat nama situs palsu yang sama persis dengan situs asli dan membuat alamat yang mirip dengan situs asli. Pelaku menunggu kesempatan jika ada seseorang korban salah mengetikan alamat dan sirus palsu buatannya. Jika hal ini terjadi maka pelaku akan mudah memperoleh informasi *user* dan *password* korbannya dan dapat dimanfaatkan untuk merugikan korban.

d. Brute force attacking

Brute force attack atau dalam bahasa Indonesia disebut juga dengan serangan brute force ini adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci password yang memungkinkan atau istilah gampangnya mungkin menggunakan Random password atau password acak. Pendekatan inipada awalnya merujuk pada sebuah program komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia.

e. Web deface

Sistem *exploitation* dengan tujuan menggantikan tampilan halaman muka semua situs. Cara kerja *web deface* adalah dengan melakukanperubahan pada halaman web depan pada situs-situs tertentu, dilakukan oleh para hacker atau cracker untuk mengganggu informasi yang dimunculkan pada halaman situs yang dimaksud. Contohnya adalah dengan menambahkan gambar, tulisan ke suatu web milik orang lain tanpa sepengetahuan adminnya.

f. Phissing

Suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi peka seperti kata sandi dan *username* dengan menyamar sebagai orang atau bisnis yang terpercaya dalam sebuah komunikasi resmi, seperti *email.*

g. Denial of service

Denial of service(DoS) *attack* merupakan sebuah usaha (dalam bentuk serangan) untuk melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan servis-servisnya*(denial of servis).* Cara untuk melumpuhkan dapat bermacam-macam dan akibatnyapun dapat beragam. Sistem yang diserang dapat menjadi *hang* atau *crash*, tidak berfungsi, atau menurunnya kinerja sistem karena beban CPU menjadi tingi.

h. Virus, worm, Trojan

Menyebarkan *virus, worm,* maupun *Trojan* dengan tujuan untuk melumpuhkan sistem komputer, memperoleh data-data dari sistem korban.

3.1.2 Keamanan *Internet Banking* Mandiri

Aplikasi *Internet Banking* Mandiri dijamin kerahasiaan dan keamanannya, dalam hal ini Bank Mandiri menggunakan teknologi enkripsi *Secure Socket Layer (SSL)* 128 bit, yang akan melindungi komunikasi antara komputer nasabah dengan server Bank Mandiri. Untuk menambah keamanan digunakan metode *time outsession*, dimana setelah 10 menit tanpa aktivitas Nasabah, maka akses akan tidak aktif lagi.

Selain itu Bank Mandiri akan menjaga kerahasian data pengguna *Internet Banking* Mandiri, dan hanya orang tertentu yang berhak untuk mengakses informasi tersebut untuk digunakan sebagaimana mestinya (dalam hal ini Bank Mandiri akan selalu mengingatkan karyawan akan pentingnya menjaga kerahasian data Nasabah). Bank Mandiri tidak akan memperlihatkan/menjual data tersebut kepada pihak ke tiga.

Bank Mandiri juga tidak secara otomatis mengumpulkan informasi data pengunjung *Internet Banking* Mandiri, hanya beberapa informasi umum yang akan dikumpulkan dan digunakan antara lain :

a. Nama domain yang akan digunakan Nasabah untuk mengakses internet
b. *Internet address* yang digunakan untuk mengakses *web site* Bank Mandiri
c. *Browser* yang digunakan
d. Hari, tanggal & waktu mengakses internet
e. Pilihan yang ditentukan oleh Nasabah untuk memberikan informasi kepada Bank, antara lain jenis rekening.

Untuk dapat mengakses *Internet Banking* Mandiri Nasabah harus memasukkan terlebih dahulu User ID dan PIN, dan untuk keamanan Nasabah diharuskan memasukkan kembali PIN untuk setiap transaksi yang bersifat finansial.

Mengingat banyaknya variasi *internet browser* yang ada, dan *internet banking* harus mengikuti keamanan masing-masing browser, maka saat ini Bank Mandiri menyediakan sarana *internet banking* yang lebih cocok diakses dengan menggunakan *Netscape Communicator 4.7* atau *Microsoft Internet Explorer* versi 5 .01 atau versi terakhir.

Internet Banking menggunakan beberapa metode keamanan terkini seperti:

a. Penggunaan protokol *Hyper Text Transfer Protokol Secure (HTTPS),* yang membuat pengiriman data dari server ke ISP dan klien berupa data acak yang terenkripsi.
b. Penggunaan teknologi enkripsi *Secure Socket Layer (SSL)* 128 bit, dari Verisign. Dengan SSL inilah, transfer data yang terjadi harus melalui enkripsi SSL pada komunikasi tingkat *socket.*
c. Penggunaan *user ID* dan PIN untuk login ke layanan Internet Banking ini.
d. Penggunaan metode *time out session,* yang menyebabkan bila setelah 10 menit nasabah tidak melakukan aktivitas apapun, akses tidak berlaku lagi.

e. Penggunaan PIN Mandiri untuk setiap aktivitas perbankan. PIN ini di-generate dari Token PIN Mandiri.

3.1.3 Penanggulangan Ancaman pada Sistem Internet Banking Mandiri

Ada usaha pengamanan yang dapat digunakan untuk meningkatkan tingkat keamanan dan pada saat yang samameningkatkan kepercayaan *(trust)* dari nasabah. Secara teknis sistem dapat diproteksi dengan menggunakan *firewall, Intrusion Detection System (IDS),* dan produk *cryptography* (untuk *encryption* dan *decryption* seperti penggunaan SSL). Selain hal teknis yang tidak kalah pentingnya adalah usaha untuk meningkatkan *awareness* (baik dari pihak *management,* operator, penyelenggara jasa, sampai ke nasabah), membuat *policy (procedure)* yang baik dan mengevaluasi sistem secara berkala.

Penanggulangan potensi penyerangan keamanan sitem *internet banking*, diantaranya;

a. IP spoofing diantisipasi dengan penyaringan oleh *router.*

b. *User name spoofing*, sistem otentikasi mencegah seseorang dari
berpura-pura menjadi user lain dengan memerlukan sandi untuk mengakses bank, transmisi semua password terenkripsi, dan menggunakan *encrypted one-time"cookies"* untuk mempertahankan state yang telah disahkan

c. Upaya untuk *Crack Database Otentikasi (Attempts to Crack Authentication Database),*Informasi account pelanggan yang disimpan pada database server yang terlindungi di belakang *firewall* dan database tidak dapat di *download* dari Internet.

d. Serangan berbasis web server *(Web Server Based Attacks),*Serangan terhadap *Netscape Commerce Server* adalah digagalkan karena lingkungan *chroot-ed* dan karena proses *"outside"* yang tidak bisa melihat apa-apa pada proses *"inside".Firewall* hanya mengizinkan mail untuk melewati dan menggunakan SMTP filter. Setiap mesin minimal dikonfigurasi untuk hanya melakukan tugasnya, dan tidak lebih. Pengamanan di atas pada prinsipnya merupakan usaha untuk memenuhi aspek keamanan seperti *authentication,confidentiality / privacy*, *non-repudiation*, dan *availability.* Adanya pengamanan ini tidak membuat sistem menjadi 100% aman akan tetapi dapat membuat sistem dipercaya *(trusted).* Potensi lubang keamanan dapat dianggap sebagai resiko. Maka masalah ini dapat diubah menjadi masalah *riskmanagement.*

Pada intinya, aspek keamanan komputer mempunyai beberapa lingkup yang penting, yaitu:

a. ***Privacy & Confidentiality***
Hal yang paling penting dalam aspek ini adalah usaha untuk menjaga data dan informasi dari pihak yang tidak diperbolehkan mengaksesnya.*Privacy* lebih mengarah kepada data-data yang sifatnya privat. Sebagai contoh email pengguna yang tidak boleh dibaca admin. Sedangkan *confidentialy* berhubungan dengan data yang diberikan kepada suatu pihak untuk hal tertentudan hanya diperbolehkan untuk hal itu saja.Contohnya adalah daftar pelanggan sebuah ISP.

b. ***Integrity***
Aspek ini mengutamakan data atau informasi tidak boleh diakses tanpa seizing pemiliknya. Sebagai contoh, sebuah email yang dikirim pengirim seharusnya tidak dapat dibaca orang lain sebelum sampai ke tujuannya.

c. Authentication
Hal ini menekankan mengenai keaslian suatu data atau informasi, termasuk juga pihak yang memberi data atau mengaksesnya tersebut merupakan pihak yang dimaksud.Contohnya seperti penggunaan PIN atau *password.*

d. Availability
Aspek yang berhubungan dengan ketersediaan informasi ketika dibutuhkan.Sebuah sistem informasi yang diserang dapat menghambat ketersediaan informasi yang diberikan.

e. Access Control
Aspek ini berhubungan dengan cara pengaksesan informasi. Hal ini biasanya berhubungan dengan klasifikasi data *(public, privat confidential, top secret)* dan *user (guest, admin, top manager,* dan sebagainya), mekanisme *authentication* dan juga *privacy.*Seringkali dilakukan dengan menggunakan kombinasi *user ID* atau *password* dengan metode lain seperti kartu atau *biometrics.*

f. Non-Repudiation
Hal ini menekankan agar sebuah pihak tidak dapat menyangkal telah melakukan transaksi atau pengaksesan data tertentu.Tiga aspek ini sangat penting dalam hal *e-commerce.*Sebagai contoh, seseorang yang mengirim *email* pemesanan barang tidak dapat disangkal telah mengirim email tersebut.
Sebagai contoh, seseorang yang mengirim email pemesanan barang tidak dapat disangkal telah mengirim email tersebut.

4.1 Kesimpulan

Berdasarkan uraian serta analisis yang telah dikemukakan pada bab-bab sebelumnya, maka dapat ditarik kesimpulan sebagai berikut:

a. Ancaman yang terjadi pada Internet Banking Mandiri antara lain *Active Snifing*, *Passive Snifing*, *Keylogger*, *Typo Site*, *Brute Force Attacking*, *Web Deface*, *Phissing*, *Denial of Service*, dan *Virus Worm Trojan.*

b. Keamanan yang digunakan pada sistem Internet Banking Mandiri antara lain dengan penggunaan protokol *Hyper Text Transfer Protokol Secure (HTTPS),* penggunaan teknologi enkripsi *Secure Socket Layer (SSL)* 128 bit, Penggunaan *user ID* dan PIN untuk *login* ke layanan *Internet Banking,* penggunaan *metode time out session* selama 10 menit,dan penggunaan PIN Mandiri yang di *generate*dari Token PIN Mandiri untuk setiap aktivitas perbankan.

c. Penanggulangan ancaman pada sistem *Internet Banking* Mandirisecara teknis diproteksi dengan menggunakan *firewall, Intrusion Detection System (IDS),* dan produk *cryptography* (untuk *encryption* dan *decryption* seperti penggunaan SSL). Selain itudengan usaha untuk meningkatkan *awareness* (baik dari pihak *management*, operator, penyelenggara jasa, sampai ke nasabah), membuat policy *(procedure)* yang baik dan mengevaluasi sistem secara berkala.

4.2 Saran

Beberapa saran dari penulis untuk meminimalisir celah ancaman antara lain:

a. Untuk mencegah *hardware keylogger*, pengguna atau penyedia layanan *Internet Banking* dapat memaksimalkan fitur virtual keyboard. Karena dengan fitur ini, *keylogger* tidak dapat merekam hasil ketikan karena tidak melalui *port* atau kabel keyboard.

b. Untuk mencegah perangkat lunak *keylogger*, dapat menggunakan perangkat lunak antivirus dan *firewall* yang selalu terupdate. Karena jika tidak ter-update, akan percuma. Karena beberapa *keylogger* dapat mematikan anti virus.

c. Untuk mencegah terjadinya *poisoning ARP*, maka solusi yang dapat dilakukan dengan mengimplementasi *security* pada *switch*, tetapi hanya *switchmanageable* yang dapat melakukannya bukan *switch* jenis biasa. Cara lainnya dengan mencegah *ARP cache* pada computer berubah, dengan cara mengubahnya menjadi *ARP cache static* seperti menggunakan perintah arp-s pada *command prompt.*

d. Hindari untuk mengakses *Internet Banking*dari tempat–tempat umum, seperti warnet, dll. Karena aspek keamanan yang biasanya minimalis.

e. Untuk meminimalisir terjadinya proses *sniffing,* gunakan protokol yang mengenkripsi data pada transfer datanya seperti HTTPS, IPSec, SMB Signing, dll.

Daftar Pustaka

Harahap, Aswan Khairil. *Perlindungan Hukum Nasabah Bank dalam Cyber Crime terhadap Internet Banking Dikaitkan dengan UU No.11 Tahun 2008 tentang Transaksi Informasi dan Transaksi Elektronik.*Universitas Sumatera Utara. 2009.

Haryanto.*Media Internet Banking.*http://www.dudung.net

Mukhlish, Fata. *Analisis Keamanan Internet Banking Bank Mandiri.*Institut Teknologi Bandung.

Thygerson, Kenneth. *Financial Institution Internet Source Book.*Mc Graw Hill, 1997 hal 100-101

http://www.bankmandiri.co.id

http://www.ebizzasia.com/