Upaya Melindungi Data Perusahaan Pelayaran di Internet dari Hacker

Oleh

Iwan Mahendro

Staff Pengajar AMNI

Email : imahendro@gmail.com

Abstrak

Perusahaan pelayaran adalah badan hukum atau badan usaha yang mengusahakan jasa angkutan laut dengan menggunakan kapal. Saat ini perusahaan – perusahaan pelayaran sudah menggunakan internet untuk menjalankan berbagai aktivitas perusahaan. Hal ini dilakukan karena dengan adanya internet akan memudahkan komunikasi baik itu antar perusahaan pelayaran maupun dengan kapal yang sedang berlayar. Akan tetapi dengan adanya internet ini, maka tindak kejahatan melalui internetpun juga banyak terjadi, biasanya dilakukan oleh para hacker dengan cara membobol data perusahaan maupun menyerang data perusahaan dengan berbagai macam virus. Perusahaan – perusahaan akan melakukan berbagai upaya untuk melindungi datanya dari berbagai serangan lewat internet.

Kata kunci : *perusahaan pelayaran, internet, data*

ABSTRACT

The shipping company is a legal entity or entities who undertake marine transportation services by boat. Currently the company - the shipping company is already using the internet to run the various activities of the company. This is because with the internet will facilitate communication both between the shipping company and the ship was sailing. But with the internet, then crime through internetpun also occur, usually done by hackers to break into corporate data as well as ways to attack corporate data with a variety of viruses. Company - the company will take measures to protect its data from a variety of attacks via the Internet.

Keywords: *shipping companies, the Internet, the data*

I. PENDAHULUAN

A. Latar Belakang

Indonesia mulai menggiatkan perekonomian di bidang maritim, hal ini tentunya mendorong perusahaan – perusahaan pelayaran untuk lebih aktif dalam menjalankan usahanya. Apalagi dengan kemajuan teknologi yang sangat cepat terutama dalam bidang internet, akan lebih mendorong perusahaan pelayaran untuk lebih baik dalam memajukan perusahaannya baik itu untuk persaingan lokal maupun persaingan internasional.

Perusahaan mulai menggunakan internet karena internet mempunyai banyak kelebihan sehingga akan sangat membantu dalam pengoperasian perusahaan. Kelebihan internet antara lain sarana komunikasi murah, kecepatan, dan memudahkan pekerjaan. Selain kelebihan tentunya internet juga mempunyai kekurangan. Kekurangan internet antara lain ketergantungan pada jaringan telepon dan ISP, adanya virus, dan privasi mudah dibobol.

Perusahaan dengan adanya jaringan internet biasanya akan membayar gaji karyawannya melalui transfer sehingga gaji akan langsung masuk ke rekening karyawan. Masalah yang sering dihadapi perusahan pelayaran saat data – data terkoneksi ke jaringan internet adalah adanya serangan hacker yang mencoba untuk membobol data dengan tujuan untuk bisa mengambil uang perusahaan dengan jumlah sangat besar. Jadi jika perusahaan tidak siap maka akan mengalami kerugian yang sangat besar.

Perkembangan teknologi yang sangat cepat memungkinkan para pengguna internet untuk mencari cara agar data – data mereka tidak diserang oleh hacker. Perusahaan – perusahaan pelayaran juga mulai mencari cara agar bisa mengamankan data mereka dari serangan hacker dan virus yang menyerang.

B. Permasalahan

1. Internet
2. Serangan hacker ke data perusahaan pelayaran
3. Cara melindungi data dari serangan hacker
4. Aspek – aspek keamanan komputer

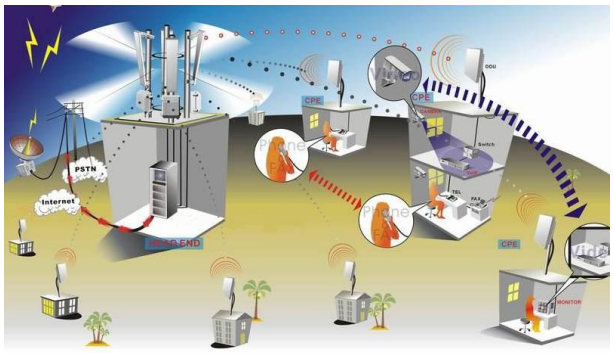
II. Pembahasan

1. Internet

a. Pengertian Internet

Internet adalah sebuah perpustakaan besar yang didalamnya terdapat jutaan (bahkan milyaran) informasi atau data yang dapat berupa teks grafik, audio maupun animasi dan lain lain dalam bentuk media elektronik. Semua orang

bisa berkunjung ke perpustakaan tersebut kapan saja serta dari mana saja, jika dilihat dari segi komunikasi, internet adalah sarana yang sangat efektif dan efesien untuk melakukan pertukaran informasi jarak jauh maupun jarak dekat, seperti di dalam lingkungan perkantoran, tempat pendidikan, atapun instansi terkait.



Gambar 1 Jaringan Internet

b. Fasilitas Internet

Ada 8 fasilitas internet yaitu :

1. WWW (World Wide Web)

   Banyak yang menyalahartikan WWW sebagai internet, padahal WWW hanyalah bagian dari fasilitas yang disediakan internet. WWW adalah sebuah fasilitas yang ada dalam internet yang bertugas untuk melakukan pencarian dan pemberian informasi dengan cepat menggunakan teknologi hypertext. Untuk membuat hypertext diciptakanlah HTML (Hypertext Markup Language). HTML berfungsi mengikat WWW ke dalam file yang berekstensi .htm ataupun .html. Untuk mengakses file HTML tersebut dibutuhkan sebuah metode pengiriman data yang disebut HTTP (Hypertext Transfer Protocol) kemudian diikuti dengan URL (Uniform Resource Locator) atau alamat web tersebut.

2. E-Mail

   E-Mail atau surat elektronik adalah sebuah fasilitas internet yang memungkinkan pengguna untuk mengirim surat ke pengguna lain melalui internet secara cepat. Tidak hanya untuk mengirim pesan teks saja, E-Mail memungkinkan pengguna untuk mengirimkan data seperti gambar, dokumen, video bahkan animasi. Saat ini ada begitu banyak penyedia E-Mail gratis seperti Gmail, yahoo dan lain sebagainya.

3. Chatting

   Dengan fasilitas ini, internet memungkinkan pengguna untuk melakukan percakapan dengan pengguna lain secara real time. Hampir sama dengan E-Mail, saat ini fasilitas chatting juga memungkinkan penggunanya untuk mengirim gambar. Bahkan apabila perangkat yang digunakan sudah *support* menggunakan

kamera, dapat melakukan Video Chat. Video Chat adalah chatting dengan pengguna lain dengan menampilkan lawan bicara melalui kamera.

4. FTP (File Transfer Protocol)

   FTP atau File Transfer Protocol adalah suatu fasilitas internet yang memungkinkan pengguna untuk mengirimkan file ke pengguna lain melalui suatu server. Contoh nyata dari fasilitas ini adalah layanan Upload ataupun Download, jadi kita dapat mengunggah file kita untuk disimpan di internet ataupun mengambil file yang sudah tersedia di internet

5. Gopher

   Gorpher merupakan fasilitas internet yang menggunakan layer application pada protokol TCP/IP yang dirancang khusus untuk keperluan distribusi, pencarian, maupun pengambilan dokumen melalui jaringan intenet.

6. Mailing List

   Mailing List merupakan sebuah grup diskusi yang tersedia di internet. Untuk menjadi anggota dari Mailing List biasanya kita harus mengirim email kepada admin dan menunggu persetujuan untuk mengikuti diskusi tersebut.

7. Newsgroup

   Sama seperti Mailing List Newsgroup merupakan grup diskusi di internet yang membahas tentang suatu topik. Untuk mengakses Newsgroup kita memerlukan sebuah jaringan khusus yang disebut dengan UseNet.

8. Bulletin Board System

   Sesuai dengan namanya Bulletin Board System adalah suatu fasilitas internet yang menyediakan informasi dalam bidang tertentu seperti pendidikan, ekonomi, politik, bisnis dan lain sebagainya. Selain itu pengguna juga dapat bertukar pikiran dengan pengguna lain tentang suatu topik yang tersedia. Pengguna juga dapat mengupload berita ataupun mendownload berita dari pengguna lain.

2. Serangan hacker ke data perusahaan pelayaran

Ada banyak jenis – jenis serangan di internet, serangan yang paling sering terjadi adalah

1) IP Spoofing

   IP spoofing adalah sejumlah serangan yang menggunakan perubahan sumber IP Address. Protokol TCP/IP tidak memiliki cara untuk memeriksa apakah sumber IP address dalam paket header benar-

benar milik mesin yang mengirimkannya. Kemampuan ini sering dimanfaatkan oleh para hacker untuk melancarkan serangan seperti:

a. SMURF Attack

   Suatu Broadcast ping yang terkirim dan sumber IP dari ping terlihat sama dengan IP address korban. Dalam kasus ini sejmlah besar komputer akan merespon balik dan mengirim suatu Ping reply ke korban. Kejadiannya terus berulang-kali, hingga mesin korban atau link mengalami overload dan dalam kondisi Denial of Service.

b. Prediksi jumlah rangkaian TCP

   Suatu koneksi TCP yang ditandai dengan suatu jumlah rangkaian client dan server. Jika jumlah rangkaian tersebut dapat ditebak, para hacker dapat membuat packet dengan memalsukan IP address dan menebak urutan jumlah untuk melakukan hijack koneksi TCP.

c. Prediksi rangkaian melalui pemalsuan DNS

   Server DNS biasanya mengquery server DNS lain untuk mengetahui nama host yang lain. Seorang hacker akan mengirimkan suatu request ke server DNS target seolah-olah seperti respon ke server yang sama. Dengan cara ini para hacker dapat membuat client yang mengakses, misalnya situs www.hotmail.com ke server milik sang hacker.

2) SNIFFING

SNIFFING adalah penyadapan terhadap lalu lintas data pada suatu jaringan komputer. Contohnya begini, Anda adalah pemakai komputer yang terhubung dengan suatu jaringan dikantor. Saat Anda mengirimkan email ke teman Anda yang berada diluar kota maka email tersebut akan dikirimkan dari komputer Anda trus melewati jaringan komputer kantor Anda (mungkin melewati server atau gateway internet), trus keluar dari kantor melalui jaringan internet, lalu sampe di inbox email teman Anda. Pada saat email tersebut melalui jaringan komputer kantor Anda itulah aktifitas SNIFFING bisa dilakukan oleh administrtor jaringan yang mengendalikan server atau oleh pemakai komputer lain yang terhubung pada jaringan komputer kantor Anda, bisa jadi teman sebelah Anda. Dengan aktifitas SNIFFING ini email Anda bisa di tangkap / dicapture sehingga isinya bisa dibaca oleh orang yang melakukan SNIFFING tadi.

3) Hacker menyerang dengan virus

Virus komputer bisa diartikan sebagai suatu program komputer biasa. Tetapi memiliki perbedaan yang mendasar dengan program-program lainnya,yaitu virus dibuat untuk menulari program-program lainnya, mengubah, memanipulasinya bahkan sampai merusaknya.

3. Cara melindungi data dari serangan hacker

1) IP Spoofing

a. Mencegah web spoofing

- Tidak mengaktifkan Javascript pada browser sehingga penyerang tidak dapat menyembunyikan petunjuk atau bukti dari adanya penyerangan.
- Memastikan bahwa *location line* dari browser selalu tampak.
- Memperhatikan *URL* yang ditampilkan pada *location line* dari browser untuk memastikan *URL* tersebut mengacu pada server dari situs sebenarnya yang dikunjungi.

b. Pencegahan *DNS Spoofing*

DNS spoofing dapat diatasi dengan mendisable recursive query ke name server dengan membuat split DNS yaitu membuat dua name server. Name server utama digunakan untuk menangani domain name dari public domain, sedangkan name server kedua di yang berada di internal network bertugas sebagai cache name server yang bertugas menjawab query dari user yang merequest domain tersebut.

c. Mencegah ARP Spoofing dengan cara

- Melakukan pengecekan MAC Address dengan menggunakan tools Colasoft MAC Scanner.
- Scan network ,jika terdapat 2 buah IP Address yang sama dengan Gateway putus client tersebut dari jaringan kemudian *scan Virus* denggn menggunakan antivirus yang Up-to-date virus databasenya.
- Setelah dilakukan *virus scanning*, dilakukan langkah penutup ini,buka Command prom kemudian ketik : arp –s ip_address_gateway mac_address_gateway lalu tekan tombol Enter.

d. Mencegah Ip Spoofing

- Memasang Filter di Router dengan memanfaatkan "*Ingress* dan *Engress filtering*"

pada router merupakan langkah pertama dalam mempertahankan diri dari spoofing.

- *Enkripsi* dan *Authenfikasi* kita juga dapaat mengatasi IP Spoofing dengan mengiplementasikan authentifikasi dan enkripsi data.

2) SNIFFING

Cara mencegah sniffing hampir tidak ada karena penggunaan antivirus dan penggunaan firewall tidak bisa mencegah sniffing. Hal ini disebabkan sniffing dilakukan pada saat data sudah keluar dari komputer korban dan berada di jaringan komputer, sehingga si sniffer tidak menyerang secara langsung ke komputer korban. Sniffer dapat dicegah dengan cara manual yaitu dengan cara tidak melakukan aktifitas yang sifatnya rahasia pada suatu jaringan komputer yang belum kita kenal. Contoh aktifitas rahasia yaitu email, e-banking, chatting rahasia.

3) Hacker menyerang dengan virus komputer

Ada beberapa langkah agar komputer tidak terserang virus

- Gunakanlah program antivirus yang bagus. Sekarang ini terdapat puluhan program antivirus yang dapat di gunakan. Ada yang dibagikan secara gratis, ada pula yang berbayar. Setiap program antivirus mempunyai kelebihan dan kekurangan masing masing. Untuk mengetahui antivirus mana yang bagus, anda bisa membaca*review* atau tulisan tentang antivirus tersebut di internet atau majalah komputer. Baca pula pengalaman orang orang yang telah menggunakan antivirus tersebut
- Ingatlah selalu untuk menjalankan program antivirus tersebut setiap anda menggunakan komputer. Pastikan antivirus yang anda gunakan memberikan perlindungan secara terus menerus termasuk perlindungan terhadap*email* masuk dan keluar. Hentikan kebiasaan menjalankan antivirus bila diperlukan saja karena anda tidak akan selalu tahu kapan suatu virus akan menyerang
- Pastikan program antivirus yang anda gunakan selalu dalam keadaan ter-*update*. *Update database* virus biasanya diberikan secara cuma cuma oleh pembuat program

antivirus. Bila anda tidak ingin lupa melakukan *update* antivirus, jalankan saja fitur *update* terjadual yang tersedia pada program antivirus. Setiap hari tercipta ratusan virus baru, sehingga melakukan *update* secara rutin sudah menjadi suatu keharusan.

- Pastikan sistem operasi yang anda gunakan selalu dalam keadaan ter-*update*. Semakin hari, semakin sering kita mendengar adanya lubang keamanan dari suatu sistem operasi. Lubang keamanan ini sering dimanfaatkan oleh virus untuk masuk dan merusak sistem komputer anda. Hal itulah yang menyebabkan mengapa sistem operasi harus selalu dalam keadaan ter-*update*. Disamping mengamankan dari serangan virus, melakukan *update* sistem operasi juga akan membuat komputer anda berjalan selalu dalam keadaan stabil. *Update* harus juga dilakukan untuk program lain yang terpasang di komputer anda karena mereka juga bisa menjadi celah bagi masuknya virus.
- Lakukanlah backup data secara rutin. Hal ini untuk mencegah anda kehilangan data penting apabila komputer anda terinfeksi virus.
- Jika anda sering menggunakan disket, *USB Flash Disk, Harddisk external*, pada komputer yang dipakai oleh banyak orang, ingatlah selalu untuk melakukan *scanning* antivirus pada media penyimpanan tersebut sebelum anda menjalankannya pada komputer anda. Selalulah beranggapan bahwa komputer yang digunakan banyak orang adalah komputer yang terinfeksi virus sehingga anda bisa lebih waspada. Selain itu, anda juga bisa menonaktifkan fungsi *autorun* untuk media media penyimpanan tersebut pada komputer anda. Hal ini memudahkan anda melakukan *scanning* manual sebelum komputer menjalankan program yang ada pada media penyimpanan tersebut.
- Waspadalah terhadap lampiran / *attachments email*. Sampai saat ini, lampiran *email* merupakan sarana yang paling disukai oleh pembuat virus untuk menyebarkan virus buatannya. Disamping mudah menipu penerima *email,* penyebaran via lampiran *email* juga berlangsung

sangat cepat. Jangan pernah membuka suatu lampiran *email* sebelum melakukan *scanning* dengan program antivirus walau *email* tersebut datang dari sahabat karib anda. Beberapa virus komputer akan menyebarkan dirinya melalui alamat *email* yang ada pada daftar kontak korbannya. Hal ini tentu tanpa sepengetahuan pemilik komputer.

- Gunakan *email* berbasis teks dalam ber-

  email. Menggunakan *email* berformat html sangat disukai oleh banyak orang karena *email* jenis ini tampak lebih indah dan mudah dikustomisasi tampilannya. Sayangnya, *email* jenis ini juga disukai oleh virus untuk menyebarkan diri. Virus dapat menempel pada kode kode html yang ada pada *body email*, jadi anda bisa terinfeksi hanya dengan membuka *email* tersebut. Sementara itu, pada *email* yang berbasis teks, virus hanya dapat menempel pada lampiran saja.

4. **Aspek - Aspek Keamanan Komputer**

   Tujuan dari keamanan komputer adalah melindungi data dan informasi yang berada di dalam komputer.

Aspek – aspek dari keamanan komputer adalah

1. Privacy, adalah sesuatu yang bersifat rahasia(provate). Intinya adalah pencegahan agar informasi tersebut tidak diakses oleh orang yang tidak berhak. Contohnya adalah email atau file-file lain yang tidak boleh dibaca orang lain meskipun oleh administrator. Pencegahan yang mungkin dilakukan adalah dengan menggunakan teknologi enksripsi, jadi hanya pemilik informasi yang dapat mengetahui informasi yang sesungguhnya.
2. Confidentiality, merupakan data yang diberikan ke pihak lain untuk tujuan khusus tetapi tetap dijaga penyebarannya. Contohnya data yang bersifat pribadi seperti : nama, alamat, no ktp, telpon dan sebagainya. Confidentiality akan terlihat apabila diminta untuk membuktikan kejahatan seseorang, apakah pemegang informasi akan memberikan infomasinya kepada orang yang memintanya atau menjaga klientnya.
3. Integrity, penekanannya adalah sebuah informasi tidak boleh diubah kecuali oleh pemilik informasi. Terkadang data yang telah terenskripsipun tidak terjaga integritasnya karena ada

kemungkinan chpertext dari enkripsi tersebut berubah. Contoh : Penyerangan Integritas ketika sebuah email dikirimkan ditengah jalan disadap dan diganti isinya, sehingga email yang sampai ketujuan sudah berubah.

4. Autentication, ini akan dilakukan sewaktu user login dengan menggunakan nama user dan passwordnya, apakah cocok atau tidak, jika cocok diterima dan tidak akan ditolak. Ini biasanya berhubungan dengan hak akses seseorang, apakah dia pengakses yang sah atau tidak.
5. Availability, aspek ini berkaitan dengan apakah sebuah data tersedia saat dibutuhkan/diperlukan. Apabila sebuah data atau informasi terlalu ketat pengamanannya akan menyulitkan dalam akses data tersebut. Disamping itu akses yang lambat juga menghambat terpenuhnya aspe availability. Serangan yang sering dilakukan pada aspek ini adalah denial of service (DoS), yaitu penggagalan service sewaktu adanya permintaan data sehingga komputer tidak bisa melayaninya. Contoh lain dari denial of service ini adalah mengirimkan request yang berlebihan sehingga menyebabkan komputer tidak bisa lagi menampung beban tersebut dan akhirnya komputer down.

III. PENUTUP

a. Kesimpulan

Kemajuan dibidang teknologi telah membawa perubahan besar bagi perusahaan pelayaran. Teknologi internet yang maju mempunyai kelebihan dalam hal kecepatan dalam arus data, kenyamanan, kemudahan akses, dan sarana komunikasi murah. Dengan adanya kelebihan internet maka perusahan – perusahan pelayaran banyak yang menghubungkan data perusahaannya ke internet.

Teknologi internet yang semakin canggih juga berdampak pada tindak kejahatan yang semakin canggih. Dengan terhubungnya data perusahaan ke internet maka kemungkinan akan diserang hacker (orang yang dapat membobol keamanan data perusahaan lewat internet) akan semakin besar. Jika sebuah perusahaan tidak mempunyai keamanan data yang baik maka akan dengan mudah diserang oleh hacker dan dapat mengalami kerugian yang sangat besar. Hacker biasanya menyerang lewat internet dengan metode IP Spoofing dan Sniffing.

Perusahaan dapat mengatasi serangan hacker yang menggunakan metode IP Spoofing dan Sniffing dengan cara Memasang Filter di Router dengan memanfaatkan "*Ingress* dan *Engress filtering*" pada router merupakan langkah pertama dalam mempertahankan diri dari spoofing *Enkripsi* dan *Authenfikasi*. Sedangkan untuk mengatasi Sniffing dengan cara cara tidak melakukan aktifitas yang sifatnya rahasia pada suatu jaringan komputer yang belum kita kenal. Contoh aktifitas rahasia yaitu email, e-banking, chatting rahasia. Perusahaan jika mempunyai keamanan data yang baik dan mengetahui cara mengatasi serangan hacker, maka tidak perlu khawatir akan data – data mereka yang terhubung ke internet. Sehingga mereka dapat beraktifitas dengan aman dan lancar.

IV. DAFTAR PUSTAKA

- http://www.belajar-komputer-mu.com/
- http://www.gustariart.blogspot.co.id/
- http://www.pintarkomputer.org/2015/08/manfaat-internet-secara umum.html
- http://www.tutorialkomputerlengkap.com/
- The Pearson Education, Inc. Web Hacking : Serangan dan Pertahanannya. 2006. Edisi Cetakan : I, 4th Publish