EDISI JANUARI 2003, Volume VIII, No. 1 ISSN : 0854-9524

ASPEK-ASPEK SEKURITAS PADA SISTEM KOMPUTER

Oleh :
Aji Supriyanto, ST

ABSTRAK

Resiko yang dihadapi oleh kebanyakan pengguna atau pemakai komputer sering kurang mendapatkan perhatian yang utama dalam perlakuan antisipasi yang mungkin akan terjadi pada komputernya. Padahal perlakuan preventif atau pencegahan ini sangat penting sekali. Para pemakai komputer baru sadar dan baru melakukan perlakuan pengamanan secara represif setelah resiko terjadi dan menimbulkan akibatkan yang sangat merugikan baik pada dirinya secara langsung maupun secara tidak langsung. Para pengguna kurang begitu menyadari dan bahkan kurang peduli terhadap perlakuan system sekuritas terhadap komputernya, hal ini diakibatkan karena pengetahuan yang terbatas dari kebanyakan pemakai komputer. Untuk itu dalam penelitian ini perlu mengambil topik tentang aspek-aspek sekuritas pada system komputer.

Hasil penelitian ini dapat melakukan identifikasi masalah sekuritas komputer, yaitu menentukan bagaimana komputer dapat rusak ditinjau dari sisi perangkat keras (hardware), perangkat lunak (software), dan pengaruhnya terhadap pemakai (user), dan bagaimana langkah pencegahan sebelum terjadinya kerusakan, dan menentukan langkah penanggulangannya setelah terjadi kerusakan. Bentuk pengamanan tersebut dapat dilakukan dengan menentukan model tingkat pengamanan seperti melakukan kewaspadaan terhadap pemakai, pengamanan fisik baik fisik komputer maupun lingkungan yang terlibat,. Setelah melakukan tindakan pengamanan fisik maka selanjutnya melakukan tindakaan pengamanan fungsi komputer. Ancaman yang sering dirasakan oleh pengguna komputer yang berhubungan langsung dengan keamanan data, aplikasi, dan system operasi adalah Virus komputer. Saat ini untuk proteksi data dari bentuk manipulasi data yang sedang berkembang adalah dengan cara metode enkripsi. Metode ini akan melakukan enkrip atau membuat kode sandi tertentu dengan cara menyamarkan data.

Kata kunci :
Sekuritas, user, virus, enkripsi

PENDAHULUAN

1. Latar Belakang

Kebanyakan user dalam menggunakan komputer karena alasan fasilitas yang ada pada komputer itu sendiri, yang memberikan banyak kemudahan dalam membantu menyelesaikan masalah yang dihadapi manusia. Namun tidak banyak yang mengetahui

tentang resiko yang bisa diakibatkan atau ditimbulkan dari penggunaan atau pemakaian komputer itu sendiri baik penggunaan komputer secara stand alone maupun secara jaringan.

Resiko yang dihadapi oleh kebanyakan pengguna atau pemakai komputer sering kurang mendapatkan perhatian yang utama dalam perlakuan antisipasi yang mungkin akan terjadi pada komputernya. Padahal perlakuan preventif atau pencegahan ini sangat penting sekali. Para pemakai komputer baru sadar dan baru melakukan perlakuan pengamanan secara represif setelah resiko terjadi dan menimbulkan akibatkan yang sangat merugikan. Hal ini diibaratkan seperti sescorang baru sadar setelah dirinya sakit, bahkan sampai di rumah sakit, karena kesalahan dari perilaku yang tidak antisipasif saat sebelum sakit.

Keluhan-keluhan pengguna komputer yang sering terjadi misalnya privatisasi data yang kurang terjamin karena pemakaian oleh banyak user, komputer yang sering ngadat, terjadinya perubahan data secara tidak terduga, bahkan tiba-tiba terjadi kehilangan data, data teriveksi virus, tempat yang kurang nyaman, dan banyak lagi keluhan-keluhan yang terjadi. Bahkan dengan adanya teknologi internet yang memberikan berbagai macam fasilitas ternyata juga bisa menjadi kekawatiran bagi sebagian browser untuk melakukan akses data di internet, hal ini bisa dicontohkan misalnya software-software yang bisa diambil (download) ternyata terinfeksi virus, kemudaian adanya fasilitas pengaksesan kartu kredit yang tidak sesua dengan nominalnya, dan sebagainya.

Dengan begitu banyaknya permasalahan yang timbul maka diperlukan tindakan pencegahan, penanggulangan, dan penanganan keamanan di segala aspek system komputer. Untuk mewujudkan atau melakukan tindakan tersebut diperlukan Langkah-langkah tertentu yang sekiranya dapat mengatasi masalah yang ada dan yang dimungkinkan akan timbul, yaitu dengan melakukan analisis berupa tinjauan dari berbagai aspek yang berhubungan dengan system sekuritas komputer.

2. Perumusan Masalah

Secara garis besar resiko yang bisa diakibatkan atau ditimbulkan dari sebuah kesalahan-kesalahan atau masalah-masalah yang ada baik secara sengaja, maupun tidak sengaja dapat merugikan bagi berbagai pihak yang berkompeten baik secara langsung

maupun tidak langsung. Permasalaha-permasalahan yang timbul pada sebuah system komputer bisa disebabkan oleh berbagai hal, untuk itu pemakaian komputer bisa ditinjau dari sistem yang telibat dari pemakaian komputer itu sendiri, yaitu dari sisi pengguna komputer (*brainware*), sisi perangkat keras komputer (*hardware*), dan sisi perangkat lunak komputer (*software*). Selain itu bisa juga diakibatkan dari lingkungan baik secara langsung maupun tidak langsung yang terlibat sehingga menimbulkan berbagai masalah pada system komputer.

Untuk itu perlu dilakukan proses pengendalian dari berbagai aspek yang memungkinkan agar system komputer berjalan sebagai mana mestinya, terutama gangguan dari keamanan, baik keamanan dari pengguna, perangkat keras, perangkat lunak maupun lingkungannya. Untuk mengetahui permasalahan yang timbul maka perlu dilakukan analisis dengan melakukan tinjauan dari berbagai aspek yang akan mengakibatkan system sekuritas komputer terjamin.

3. Tujuan dan Manfaat

Tujuan Penelitian ini adalah :

- Menguraikan tentang siklus sebuah system komputer
- Meninjau dan menganalisis tentang berbagai aspek yang dapat menimbulkan masalah pada system komputer
- Menentukan metoda yang dapat mengatasi suatu masalah yang timbul pada system komputer.
- Menentukan teknik yang dapat digunakan untuk melakukan antisipasi terhadap kemungkinan yang akan terjadi masalah pada system komputer serta melakukan pemeliharaan.
- Menentukan aspek-aspek yang berkaitan dengan system sekuritas pada komputer.

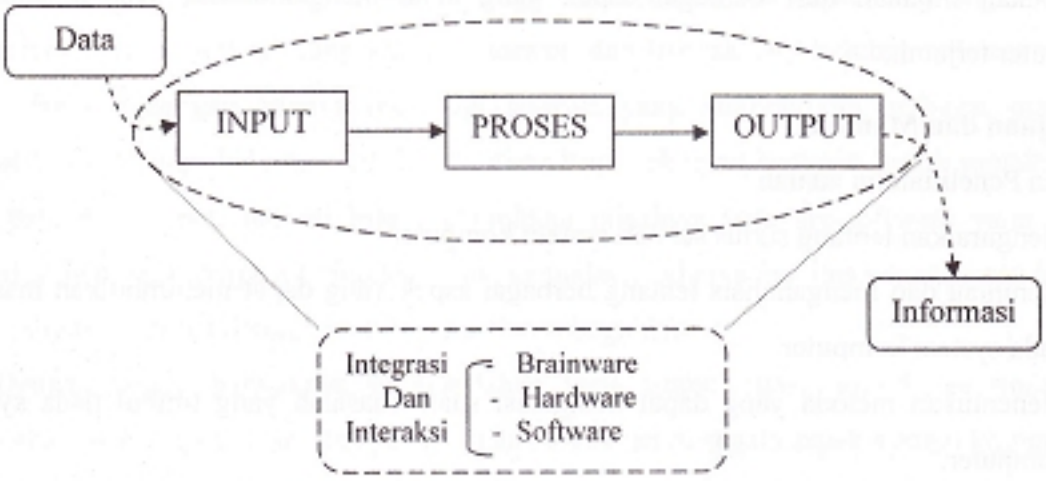
Manfaat dari penelitian ini adalah :

- Dapat mengetahui fungsi-fungsi perangkat sebuah system komputer.
- Dapat menemukan masalah-masalah yang dapat timbul pada sebuah system komputer.

- Dapat melakukan penanganan dan antisipasi terjadinya masalah-masalah pada komputer (problem solving).
- Melakukan prosedur pemeliharaan system komputer dengan secara efektif.
- Terjaminya sebuah system komputer yang dapat diandalkan.

TINJAUAN PUSTAKA

Sebelum melakukan penerapan system sekuritas pada komputer, sangat penting sekali perlu diketahui tentang bagaimana system komputer melakukan aktifitas kerjanya sesuai dengan prinsip kerja yang berlaku. Untuk mengetahui hal tersebut maka perlu dilakukan tinjauan tentang system kerja komputer. Untuk menjelaskan tentang prinsip kerja komputer dapat dilihat dalam gambar 1. berikut ini :



***Gambar 1.** Sistem Kerja Komputer*

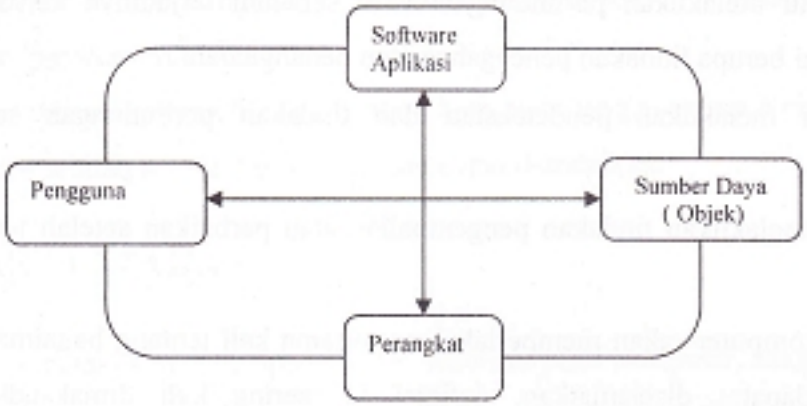
Sistem sekuritas komputer diterapkan karena dalam melakukan aktifitasnya bisa mengalami kendala-kendala yang ditimbulkan baik sengaja maupun tidak sengaja, dimana kendala-kendala itu bisa merugikan bagi pengguna komputer itu sendiri baik yang terlibat langsung maupun secara tidak langsung. Sekuritas merupakan perlindungan terhadap asset yang dimiliki. Secara garis besar klasifikasi perlindungan komputer dapat dilakukan antara lain :

- **Preventif**, yaitu melakukan perlindungan asset sebelum terjadinya kerusakan atau musibah, hal ini berupa tindakan pencegahan atau penangkalan.
- **Deteksi**, yaitu melakukan pendeteksian dan tindakan perlindungan saat terjadi kerusakan.
- **Reaksi**, yaitu melakukan tindakan pengembalian atau perbaikan setelah terjadi suatu kerusakan.

Sekuritas komputer akan memperlakukan pertama kali tentang bagaimana sebuah asset informasi dapat diselamatkan, definisi ini sering kali dimaksudkan untuk memberlakukan aspek-aspek, yaitu :

- **Kepercayaan (Confidentiality)**, bahwa informasi yang dihasilkan harus dapat dipercaya bagi yang berkepentingan dan terlindungi dari yang tidak berhak.
- **Integritas (Integrity)**, yaitu melakukan perlindungan atau pencegahan terhadap terjadinya perubahan informasi dari yang tidak berhak.
- **Ketersediaan (Availability)**, yaitu melakukan perlindungan atau pencegahan terhadap yang tidak berhak dengan tidak memberi informasi atau sumberdaya.

Prinsip-prinsip sekuritas komputer bisa dilihat dari beberapa rancangan parameter dasar. Yang mana rancangan ini memberikan kerangka kerja untuk melakukan tinjauan baik secara horizontal maupun vertical. Gambar dibawah ini memperlihatkan tentang dimensi utama dalam lingkup perancangan sekuritas komputer. Gambaran secara horizontal memperlihatkan pada kebijakan keamanan. (Gambar 2), sedangkan gambaran secara Vertikal memeperlihatkan tentang tingkatan system komputer dimana mekanisme perlindungan dapat diterapkan (Gambar 3).



Gambar 2. Dimensi-dimensi Sekuritas

Pada gambar 2. diatas dapat dijelaskan bahwa prinsip penerapan sekuritas komputer dapat dilakukan dari beberapa sisi, hal ini berakibat pula bahwa kendala-kendala sekuritas komputer juga dapat diakibatkan pada sisi yang sama, bentuk yang demikian terjadi suatu proses sebab akibat pada sebuah system komputer. Komponen-komponen seperti pada gambar 2. yang terdiri dari Pengguna (user) sebagai subjek, Perangkat keras (hardware) sebagai perangkat fisik berupa input device, process device, dan output device , Perangkat lunak (software) berupa system operasi dan program atau paket aplikasi yang digunakan untuk mengolah data, serta sumber daya lain yang digunakan untuk membantu proses pengolahan data, seperti perangkat utilitas dan lain sebagainya.

Kendala-kendala yang terjadi seperti gambar 2. diatas merupakan kendala yang disebabkan oleh faktor internal system komputer. Selain itu kendala-kendala sistem komputer dapat disebabkan oleh faktor eksternal, misalnya bencana alam, pencurian, dan lain sebagainya. Dari faktor-faktor tersebut diatas yang paling dominan dalam prinsip sekuritas komputer adalah pada skala mesin dan manusia. Biasanya mekanisme sekuritas pada skala manusia-mesin terbatas pada hubungan kompleksitasnya. Secara umum terjadinya permasalahan atau system keamanan yang kurang baik karena system proteksi yang kurang memadai. Untuk mencapai tingkat jaminan yang tinggi, system sekuritas harus dilakukan pengujian

secara mendetail dan selengkap mungkin, namun perlakuan seperti itu tidak mudah dilakukan.

Gambar 3. Model pada mekanisme proteksi komputer

Dalam system pengendalian sekuritas komputer dapat dilakukan menjadi dua system pengendalian yaitu pengendalian secara sentralisasi dan pengendalian secara desentralisasi. Dalam mengambil kebijakan tentang system kendali mana yang dipilih hal ini tentunya harus dilakukan beberapa pertimbangan. Jika dilakukan system pengendalian secara sentralisasi akan memudahkan dalam mencapai keseragaman pengamanan, tetapi system sentralisasi ini dapat menjadikan kinerja pad tiap level bagian menjadi tidak produktif. Begitu sebaliknya, bahwa solusi terdistribusi bisa menjadi lebih efisien, tetapi kita harus bisa melakukan perawatan untuk menjamin bahwa komponen-komponen yang berbeda bisa diandalkan sesuai kebijakan yang konsiten. Begitu lama, untuk menunjuk secara cepat tentang jaminan keamanan, tetapi memunculkan pilihan penetapan prediksi awal memberikan gambaran tindakan yang lebih patut tentang suatu kebijakan pengamanan. Pada saat ini untuk memikirkan tentang percobaan penyerangan harus dilakukan jalan pintas tentang mekanisme perlindungan. Setiap mekanisme perlindungan didefinisikan sebagai lingkaran pengamanan (security perimeter) atau batasan (boundary).

Bentuk sekuritas yang tidak kalah pentingnya adalah pengendalian terhadap virus komputer. Virus Komputer adalah program komputer biasa yang biasa di buat oleh manusia. Perbedaan dengan program lain adalah virus komputer dibuat dengan tujuan

pembuatannya.Virus Kompoter dibuat untuk menulari program (file) yang lain, memanipulasikan atau bahkan merusak sistem komputer seprti menghapus file, partisi *disk*, atau mengacaukan program.

METODOLOGI PENELITIAN

Metodologi yang digunakan untuk melakukan penelitian ini adalah :

1. Melakukan identifikasi terhadap suatu system komputer
2. Melakukan analisa terhadap system kerja sebuah komputer, dan menentukan kapan, apa, dan bagaimana permasalahan bisa timbul dalam sebuah system komputer.
3. Menemukan metode-metode yang dapat digunakan secara tepat pada system keamanan komputer ditinjau dari segala aspek.

HASIL DAN PEMBAHASAN

1. Identifikasi Masalah Sekuritas

Pada keamanan terdapat dua masalah penting, yaitu Kehilangan data *(data loss)*,dan Penyusup *(intruder)*.

Kehilangan data dapat disebabkan antara lain:

a. Bencana

Merupakan masalah yang timbul karena bukan faktor kesengajaan, dan merupakan diluar system komputer. Bentuk bencana ini seperti : kebakaran, Kebaanjiran, gempa bumi, Peperangan, kerusuhan, Grogotan tikus pada pita rekaman data atau *floppy disk*, dan lain sebagainya

b. Kesalahan perangkat keras dan perangkat lunak

Merupakan masalah yang ditimbulkan karena faktor internal system, hal ini dapat timbul baik sengaja maupun tidak disengaja. Bentuk kesalahan ini bias berupa : Ketidak berfungsian pemroses, disk atau tape yang tak terbaca, kesalahan telekomunikasi, kesalahan program *(bugs)*.

c. **Kesalahan atau kelalaian manusia**

Merupakan masalah yang ditimbulkan oleh manusia baik pengguna komputer yang berhak maupun yang tidak berhak. Kesalahan-kesalahan ini beruapa : kesalahan pemasukan data, memasang *tape* atau *disk* yang salah, eksekusi program yang salah, kehilangan *disk* atau *tape.*

Kehilangan data dapat diatasi dengan mengelola beberapa *backup* dan *backup* ditempatkan jauh dari data yang *online.*

Penyusup, terdiri dari :

a. Penyusup pasif, yaitu yang membaca data yang tak diotorisasi.
b. Penyusup aktif, yaitu mengubah data yang tak diotorisasi.

Kategori penyusupan :

1. Terlihat oleh pemakai *non*-teknis. Pada sistem time-sharing, kerja pemakai dapat diamati orang sekelilingnya. Bila dengan lirikan itu dapat mengetahui apa yang diketik saat pengisian *password*, maka pemakai *non*-teknis dapat mengakses fasilitas yang bukan haknya.
2. Penyadapan oleh orang dalam.
3. Usaha *hacker* dalam mencari uang.
4. Spionase militer atau bisnis.

Tipe-tipe ancaman terhadap keamanan sistem komputer dapat dimodelkan dengan memandang fungsi sistem komputer sebagai penyedia informasi. Berdasarkan fungsi ini, ancaman terhadap sistem komputer dikategorikan mebnjadi empat ancaman, yaitu:

a. Interupsi (Interuption)

Sumber daya sistem komputer dihancurkan atau menjadi tak tersedia atau tak berguna. Interupsi merupakan ancaman terhadap ketersediaan. Contoh penghancuran bagian perangkat keras; seperti harddisk, pemotongan kabel komunikasi.

b. Intersepsi (Interception)

Pihak tak diotorisasi dapat mengakses sumber daya. Intersepsi merupakan ancaman terhadap kerahasiaan. Pihak tak diotorisasi dapat berupa orang atau program komputer. Contoh penyadapan untuk mengambil data rahasia, mengkopi file tanpa diotorisasi.

c. Modifikasi (Modification)

Pihak tak diotorisasi tidak hanya mengakses tapi juga merusak sumber daya. Modifikasi merupakan ancaman terhadap integritas. Contoh mengubah nilai-nilai file data, mengubah program sehingga bertindak secara berbeda, memodifikasi pesan-pesan yang ditransmisikan pada jaringan.

d. Fabrikasi (Fabrication)

Pihak tak diotorisasi menyisipkan/memasukan objek-objek palsu ke sistem. Fabrikasi merupakan ancaman terhadap integitas. Contoh memasukan pesan-pesan palsu ke jaringan, penambahan record ke file.

2. Kesalahan Utama dalam sekuritas Komputer

Sistem Keamanan Komputer telah banyak negara yang sudah mulai menaruh perhatian pada keamanan komputer (computer security) atau Internet security dengan adanya hukum cyber atau hukum mengenai kejahatan komputer. Dengan adanya hukum yang mengatur keamanan di bidang komputer ini bukan berarti dapat menghilangkan pelanggaran atau kejahatan dalam bidang ini tetapi setidaknya ada langkah yang akan diambil seandainya terjadi pelanggaran. Tapi sebenarnya masalah utama yaitu terletak pada pengguna/user yang menggunakan komputer.

Berikut ini terdapat 5 kesalahan utama dalam security komputer, yaitu :

1. Menuliskan Password di kertas atau tempat-tempat yang bisa dijangkau orang lain, sehingga mudah untuk dibaca orang lain. Berdasarkan survei yang pernah dilakukan oleh lembaga security di US menemukan bahwa sekitar 15 - 20 % user di suatu perusahaan melakukan hal ini. Andaikan user di perusahaan A mencapai 100 orang maka ada sekitar 15 sampai 20 orang yang melakukan keteledoran ini. Suatu jumlah yang besar yang dapat mengakibatkan kebocoran data perusahaan.

2. Membuat password yang kurang unik. Ada kecenderungan orang dalam memilih password mereka adalah dengan menggunakan nama orang dekat mereka seperti nama suami atau istri, nama pacar, nama orang-tua, nama binatang kesayangan atau tulisan di sekitar mereka yang gampang ditebak oleh orang lain. Atau bahkan menggunakan tanggal lahir mereka sendiri. Penggunaan password seperti ini akan dengan gampang di-"crack" apalagi kalau password yang digunakan sama dengan user-name maka kurang dari semenit password tersebut akan dapat di-crack. Jika menggunakan password dengan kombinasi abjad, nomor dan huruf besar-kecil, maka dibutuhkan waktu yang cukup lama untuk meng-crack dan juga tergantung seberapa panjang password yang digunakan juga.
3. Meninggalkan komputer yang sedang digunakan, tanpa melakukan "lock". Ada banyak orang yang meninggalkan komputer mereka tanpa proteksi apapun. Berbagai sistem operasi sudah memberikan fasilitas seperti screen saver yang bisa diaktifkan passwordnya setelah misalnya 5 menit atau berapa sesuai dengan yang diset atau bisa di "lock" begitu kita mau meninggalkan kkomputer kita.
4. Membuka lampiran (attachment) e mail tanpa melakukan pengecekan terlebih dahulu. Seiring dengan maraknya penggunaan email, virus banyak menyebar melalui email. Salah satu kesalahan utama yang banyak dilakukan oleh orang adalah membuka attachment email tanpa melakukan konfirmasi atau pengecekan terlebih dahulu terutama kalau mendapat kiriman dari orang yang tidak dikenal. Efek yang ditimbulkan selanjutnya jika attachmen itu berupa virus maka akan berakibat pada kehilangan data.
5. Tidak adanya kebijakan security komputer di perusahaan. Bukan hal yang aneh jika perusahaan di Indonesia tidak memiliki hal ini karena perusahaan di Indonesia masih tidak begitu cukup peduli dengan security kecuali perusahaan multinasional, itupun karena keharusan dari headquarter yang mengharuskan menerapkan kebijakan di perusahaan mereka di Indonesia. Kebijakan sekuritas ini yang mengatur segala hal yang berkaitan dengan keamanan komputer seperti penerapan password setiap orang (mis : 6

karakter panjangnya dan kombinasi numerik dan karakter), juga berisi sanksi yang akan diterima jika terjadi pelanggaran.

3. Model Tingkat Pengamanan

Model-model tingkat pengamanan yang bisa dilakukan oleh user antara lain :

1. Melakukan Kewaspadaan Pemakaian Komputer

Kewaspadaan dapat dilakukan dengan cara mengetahui "lawan", dari system pengamanan. Pertama kita sendiri, yaitu berupa kecerobohan kita lebih sering membuat kerusakan dibanding orang lain, sehingga kedisiplinan dalam pemakaian komputer harus tetap dijaga. Kedua adalah orang yang dekat dengan kita, sebenarnya orang-orang disekitar kita tidak bermaksud merusak data kita atau melihat data kita tapi mereka tetap saja bisa melakukannya secara tidak sengaja. Ketiga adalah orang tak dikenal, mereka inilah para pembuat virus, trojan horse, time bomb dan lain-lain yang gunanya memang hanya untuk menghancurkan orang lain tanpa tujuan yang jelas.

2. Pengamanan Fisik

Bentuk pengamanan ini merupakan tingkat pengamanan pertama dan yang paling aman, taruh PC di tempat yang aman. Jika data yang ada memang penting dan komputer itu memang hanya akan digunakan sendiri, inilah cara yang paling sederhana dan paling aman. Namun perlu diakui tidak semua orang punya komputer yang benar-benar untuk dipakai pribadi atau memiliki kamar pribadi untuk meletakkannya, apalagi bila dikantor.

3. Pengamanan dengan Password BIOS

Dari sisi pemakaian komputer, hal ini merupakan pertahanan pertama saat komputer dihidupkan. Jika fasilitas password BIOS diaktifkan , maka begitu komputer dinyalakan akan disodori sebuah tampilan yang menanyakan password yang harus diinputkan. Sebagian orang memakai fasilitas ini dan memandangnya sebagai cara yang *aman*. Biasanya pemakaian password bisa diatur , bisa untuk pengamanan seluruh sistem atau cukup pengamanan setup BIOS. Sebenarnya password BIOS memiliki kelemahan yang cukup besar. Pada BIOS keluaran AWARD versi 2.xx, versi 4.xxg dan versi 5.xx atau di

atasnya memiliki password yang disebut password default. Dengan password default ini setiap orang bisa menjebol masuk tanpa perlu password asli. Untuk versi 5.xx atau di atasnya password defaultnya berbeda untuk setiap komputer dalam hal dua karakter di belakangnya sehingga total ada 676 password. BIOS buatan pabrik lain tidak memiliki kelemahan yang dimiliki oleh AWARD, masih ada cara lain untuk menerobos password BIOS. Perlu diketahui bahwa password BIOS tersimpan dalam sebuah chip CMOS bersama-sama dengan data setup BIOS, chip ini mendapat tenaga dari batere CMOS sehingga data yang tersimpan di dalamnya tetap aman meskipun komputer dimatikan. Perkecualian terjadi jika batere CMOS mulai habis atau terjadi hubungan pendek. Pengamanan untuk masalah itu adalah dengan menaruh System Unit di tempat yang sulit dikeluarkan, atau menambahkan kunci agar sulit dibuka. Untuk masalah password default AWARD, bisa di-update BIOS nya atau mengganti password default dengan program dari AWARD. Hal ini tidak perlu terlalu dikuatirkan, tidak banyak yang tahu masalah password default ini. Pengamanan juga bisa dibuat pada tingkat setup saja, ini berguna untuk menghindari orang-orang yang belum berpengalaman mengubah-ubah isi setup. Kelemahan teknik ini adalah password bisa dihapus dari sistem operasi, tidak ada cara untuk mencegah sebuah program menghapus password ini dari sistem operasi. Banyak program yang bisa digunakan untuk menghapus password ini, bahkan dengan BASIC atau DEBUG pun bisa. Program yang banyak dimanfaatkan untuk menghapus password biasanya adalah program pencatat isi CMOS (misalnya dari Norton Utilities) , dengan memasukkan data CMOS dari sistem yang tidak berpassword, maka password akan terhapus.

4. Pengamanan tingkat sistem operasi

Bagi pengguna DOS pengamanan bisa dilakukan dengan membuat password di AUTOEXEC.BAT. Yang perlu diketahui bahwa DOS versi-versi yang terbaru (mulai versi 5) AUTOEXEC.BAT bisa dihambat perjalanannya dengan menekan F5 atau F8 (pada MS-DOS), tujuan pemberian fasilitas ini adalah untuk melacak jalannya file-file startup tapi ternyata hal ini telah memberi masalah baru. Cara lain adalah dengan meletakkan program

password di boot record atau partisi harddisk. Kedua cara ini sangat tidak aman, karena semua orang bisa saja memboot komputer dari disket DOS yang dibawanya.

Untuk sistem operasi Windows 3.1 atau 3.11, keduanya memiliki kelemahan yang sangat besar. Karena keduanya berdiri di atas DOS, maka segala operasinya bisa diatur dari DOS, misalnya kita membuat password dengan meletakkan nama programnya di baris RUN di file WIN.INI, maka file ini bisa dimodifikasi dari DOS. Tidak banyak yang bisa kita lakukan dengan kelemahan ini.

Sistem operasi Windows 95 dan Windows 98 juga memiliki kelemahan yang sama, walaupun ada beberapa kelebihan yang mampu melindungi Windows 95/98 dengan password. Perlu diketahui ada begitu banyak lubang keamanan di Windows 95/98, yaitu dapat menekan F8 di awal proses boot untuk masuk ke DOS dan memodifikasi semua file sistem Windows, seperti misalnya WIN.INI dan file registry. Perlu diketahui juga bahwa di Windows 95/98 program-program bisa dijalankan dengan menuliskan namanya di baris RUN di file WIN.INI, dengan meletakkannya di grup STARTUP atau bisa juga dengan meletakkannya di key RUN, RUNONCE, RUNSERVICES atau di RUNSERVICES ONCE di branch *HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion* di registry dengan cara inilah program-program yang selalu muncul di startup di jalankan (Selain menggunakan kedua cara di atas). Program regedit.exe yang ada di disket startup WINDOWS 95/98 bisa mengubah file registry menjadi file teks biasa dan sebaliknya sehingga bisa mengubahnya termasuk menghilangkan baris yang menjalankan program password. Penekanan F8 (Dan tombol-tombol lain) di Windows 95/98 bisa dimatikan dengan meletakkan baris BOOTKEYS=0 di file MSDOS.SYS. Dengan cara inipun orang masih bisa masuk menggunakan startup disknya sendiri. Ini bisa dilakukan dengan mematikan drive A sehingga tidak bisa digunakan untuk boot, namun akan kesulitan jika suatu ketika Windows mengalami masalah.

Linux merupakan sistem operasi yang saat ini cukup banyak dipakai dan cukup aman, namun bagi orang awam sistem operasi ini masih cukup sulit dipakai. Jika tidak di setting

dengan benar sistem operasi ini memiliki beberapa feature default yang memudahkan orang untuk menerobos masuk.

Seperti penjelasan diatas bahwa pengamanan di tingkat sistem operasi ini sangat mudah diterobos. Solusi yang benar-benar baik sangat sulit diterapkan, setiap sistem operasi punya kelemahannya sendiri. Dan sistem operasi apapun tidak akan bisa menahan serangan jika penyerang punya akses fisik ke komputer.

5. Proteksi tingkat aplikasi

Jika didalam komputer memiliki program-program penting yang ingin terlindungi maka bisa memberinya password. Beberapa program yang berbahaya atau bersifat rahasia telah menerapkan sistem password ini sebagai bagian darinya, misalnya NU, PCTOOLS dan lain-lain. Ada banyak program DOS yang bisa memberi password ke file-file EXE ataupun COM. Sayangnya tidak banyak yang bisa memberikan hal yang sama untuk file EXE Windows. Perlu hati-hati dengan program yang memberi password pada file EXE DOS, harus dibuat dulu cadangan filenya karena file beberapa file EXE bisa rusak jika diberi password. Bagi para programmer assembly, membongkar password semacam ini tidak sulit, karena jalannya program bisa dilacak dengan menggunakan debugger.

6. Proteksi tingkat dokumen

Ini adalah level proteksi terakhir, jika ini berhasil dibongkar maka data-data penting akan terbaca oleh orang lain. Untuk program-program yang menyediakan password ketika menyimpan filenya bisa memanfaatkan fasilitas ini. Tapi hati-hati banyak sekali program yang bisa membongkarnya. Password pada MS WORD, Lotus Organizer dan lain-lain ternyata tidak sulit untuk dibongkar, oleh karena itu Anda perlu berhati-hati. Jika data-data kelewat penting namun terpaksa menyimpannya di rumah atau dikantor maka enkriplah data itu menggunakan program yang benar-benar aman kalau perlu letakkan di disket dan simpan di tempat yang aman. Password PKZIP/WINZIP atau ARJ , yang dikira aman, juga bisa dibongkar (walaupun tidak mudah). Oleh karena itu perlu menanyakan dulu kepada ahlinya sebelum menggunakan suatu program enkripsi.

7. Pengamanan dari ketidaksengajaan

Tidak selamanya bahwa pengguna berhadapan dengan hacker saja ,tetapi bisa dari keluarga atau teman terdekat, yang ditakutkan tanpa sengaja menghapus dokumen penting atau bermain-main dengan gambar yang ada, atau terdapat koleksi gambar-gambar yang akan membuat malu jika ketahuan orang lain. Untuk masalah itu ada beberapa hal yang bisa dilakukan. Pertama buatlah sebuah direktori khusus di mana akan meletakkan file-file, pindahkan file-file penting ke direktori itu. Kedua buatlah attribut direktori itu menjadi hidden, system dan read only, untuk semua file di dalamnya lakukan hal yang sama, gunakan program ATTRIB atau semacamnya. Yang ketiga hanya bagi yang menggunakan sistem operasi Windows 95/98, jangan membeli program yang akan menghilangkan semua peringatan ketika menghapus file apa saja, Gunakan shell explorer (Default windows 95/980 kecuali punya shell yang jauh lebih baik. Jalankan explorer (bagi yang memakai explorer sebagai shellnya) kemudian pilih menu **view | options** pada tab **View** pilihlah **hide file of these types** dan klik **OK.** Juga bisa mengganti ekstension file dengan daftar yang terpampang pada langkah di atas sehingga file tidak akan ditampilkan.

Cara ini memang cukup aman, orang tidak akan bisa dengan *tidak sengaja* menghapus file-file tersebut. Namun file-file tersebut bisa dengan *sengaja* di ubah atau dihapus. Jadi pengamanan di tingkat ini hanya untuk menghindari ketidaksengajaan. Hal-hal lain yang perlu diperhatikan antara lain :

1. Merubah nama file program yang berbahaya supaya tidak bisa dijalankan misalnya file FORMAT.EXE dan FDISK.EXE. Beberapa pemula suka mencoba-coba program-program, termasuk program yang berbahaya ini.
2. Membuat cadangan data untuk data yang memang benar-benar penting.
3. Mengajarkan kepada pemakai komputer baru langkah-langkah apa yang boleh dan yang tidak boleh diambil dalam mengoperasikan komputer.
4. Melakukan Install Anti Virus yang up to date, mencari antivirus yang bisa secara otomatis bekerja di background dan bisa memonitor semua jenis virus termasuk virus dokumen.

KESIMPULAN DAN SARAN

1. Kesimpulan

Keamanan sistem komputer adalah untuk menjamin sumber daya tidak digunakan atau dimodifikasi orang yang tak otorisasi. Pengamanan termasuk masalah teknis, manajerial, legalitas dan politis. Sistem sekuritas komputer diterapkan karena dalam melakukan aktifitasnya bisa mengalami kendala-kendala atau ancaman-acaman yang ditimbulkan baik sengaja maupun tidak sengaja, dimana kendala-kendala itu bisa merugikan bagi pengguna komputer itu sendiri baik yang terlibat langsung maupun secara tidak langsung. Sekuritas merupakan perlindungan terhadap asset yang dimiliki. Secara garis besar klasifikasi perlindungan komputer dapat dilakukan secara preventif, deteksi, dan reaksi .

Sekuritas komputer akan memperlakukan pertama kali tentang bagaimana sebuah asset informasi dapat diselamatkan, definisi ini sering kali dimaksudkan untuk memberlakukan aspek-aspek, yaitu Kepercayaan (Confidentiality), Integritas (Integrity), dan Ketersediaan (Availability).

Model-model tingkat pengamanan yang bisa dilakukan oleh user antara lain :

1. *Melakukan Kewaspadaan Pemakaian Komputer*
2. Pengamanan Fisik
3. Pengamanan dengan Password BIOS
4. Pengamanan tingkat sistem operasi
5. Proteksi tingkat aplikasi

SARAN

a. Para pemakai komputer agar dapat menerapkan model sekuritas pada komputernya, supaya tidak terjadi hal-hal yang tidak diinginkan terutama keamanan data yang ada pada komputer yang digunakannya.

b. Pembahasan penelitian ini banyak mengungkapkan konsep-konsep sekuritas, dan hanya memberikan beberapa contoh aplikasinya. Untuk itu pembaca dapat mengaplikasikan pada komputer dengan melekaukan percobaan sendiri.

b. Perkembangan Teknologi Komputer begitu pesatnya dan banyak kasus yang bisa terjadi, sehingga banyak contoh-contoh aplikasi yang belum disebutkan, begitu juga aspek ancaman yang ada juga semakin beragam, bila ada aspek yang belum dibahas dalam tulisan ini untuk itu pembaca bisa mencari referensi lain untuk melengkapi isi penelitian ini.

DAFTAR PUSTAKA

1. Arief Hamdani Gunawan, "Utility Network Password Windows 95", Internet.
2. Bambang Hariyanto,1999, "Sistem Operasi", Informatika Bandung.
3. Budi Sukmawan, "Keamanan data dan Metoda Enkripsi", Internet
4. Dieter Gollmann, 1999, "Computer Security", John Wiley & Sons.
5. Harry Lim , "Security is a process not just technology", Internet.
6. Hartoyo Salim, "Virus Komputer, Teknik Pembuatan dan Langkah-langkah Penanggulangannya", 1995, Andi Offset.
7. Joko Yuliantoro dan Onno W. Purbo, " Meningkatkan Sekuritas Jaringan Komputer", Internet
8. Onno W. Purbo dan Tony W.,2000," Keamanan Jaringan Internet", elex Media Komputindo
9. Rizal Akbar, "Mekanisme Keamanan Standar ISO", Internet.
10. Wisnu Arya Wardhana, Supriyono dan Djiwo Harsono "Aspek Keselamatan Kerja pada Pemakaian Komputer", Internet.
11. Yohanes Nugroho "Bahaya Program AntiVirus", Internet.