PENGANTAR KEAMANAN KOMPUTER

17.1 Munculnya Kejahatan Komputer

- **Penyebab Meningkatnya Kejahatan Komputer**

Maraknya kejahatan komputer hingga saat ini, yang diindikasikan terus mengalami peningkatan, disebabkan seperti berikut :

1. Aplikasi bisnis yang menggunakan teknologi informasi dan jaringan komputer semakin meningkat. Sebagai contoh *online banking, e-commerce, Electronic Data Interchange* (EDI).
2. Server terdesentralisasi dan terdistribusi menyebabkan lebih banyak sistem yang harus ditangani.
3. Meningkatnya kemampuan pemakai di bidang komputer sehingga mulai banyak pemakai yang mencoba-coba bermain atau membongkar sistem yang digunakannya (atau sistem milik orang lain).
4. Mudahnya diperoleh software untuk menyerang komputer dan jaringan komputer. Contohnya seperti SATAN, bahkan hanya membutuhkan sebuah browser Web untuk menjalankannya. Sehingga seseorang yang hanya dapat menggunakan browser Web dapat menjalankan program penyerang (*attack*). Penyerang yang hanya bisa menjalankan program tanpa mengerti apa maksudnya disebut dengan istilah *Script Kiddie*.
5. Kesulitan dari penegak hukum untuk mengejar kemajuan dunia komputer dan telekomunikasi yang sangat cepat. Hukum yang berbasis ruang dan waktu akan mengalami kesulitan untuk mengatasi masalah yang justru terjadi pada sebuah sistem yang tidak memiliki ruang dan waktu.
6. Semakin kompleksnya sistem yang digunakan, seperti semakin besarnya program (*source code*) yang digunakan sehingga semakin besar probabilitas
7. Terjadinya lubang keamanan yang disebabkan kesalahan pemrograman (*bugs*).
8. Semakin banyak perusahaan yang menghubungkan sistem informasinya dengan jaringan komputer yang global seperti Internet.

17.2 Aspek-aspek Keamanan Komputer

- **Aspek keamanan komputer**

  Adalah bentuk pertimbangan yang menyatakan sebuah komputer bisa dinyatakan aman.

  Agar sistem informasi serta data yang kita miliki dapat lebih terjaga keamanannya, setiap perusahaan atau pengguna komputer harus memperhatikan tiga aspek penting, yaitu : teknologi, manusia, dan proses, atau dikenal sebagai segitiga pengaman atau *The Security Triangle*.

Beberapa aspek keamanan komputer meliputi hal-hal seperti berikut ini :

- *Authentication*, yaitu 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.
- *Integrity*, yaitu 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.
- *Nonrepudiation*, yaitu hal-hal yang bersangkutan dengan pengirim, pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
- *Authority*, yaitu informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
- *Confidentiality*, yaitu usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.
- *Privacy*, yaitu lebih ke arah data-data yang sifatnya privat (pribadi).
- *Availability*, yaitu aspek ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan.
- *Access control*, yaitu aspek ini berhubungan dengan cara pengaturan akses kepada informasi. *Access control* sering kali dilakukan dengan menggunakan kombinasi *user ID* dan password pengguna.

17.3 Konsep Keamanan Komputer

- **Tujuan/Syarat Keamanan**

Secara garis besar, persyaratan keamanan sistem komputer dapat dibedakan menjadi tiga, yaitu :

1. Kerahasiaan (*secrecy*)

   Secrecy berhubungan dengan hak akses untuk membaca data atau informasi dari suatu sistem komputer.

2. Integritas (*integrity*)

   Integrity berhubungan dengan hak akses untuk mengubah data atau informasi dari suatu sistem komputer .

3. Ketersediaan (*availability*)

   Availability berhubungan dengan ketersediaan data atau informasi pada saat yang dibutuhkan.

- **Lingkup Pengamanan**

Pada prinsipnya pengamanan sistem komputer mencakup empat hal yang sangat mendasar, yaitu :

1. Pengamanan secara fisik

   Pengamanan secara fisik dapat dilakukan dengan menempatkan sistem komputer pada tempat atau lokasi yang mudah diawasi dan dikendalikan, ruangan yang dapat dikunci, dan sulit dijangkau orang lain, serta kebersihan ruangan.

2. Pengamanan akses

   Ini dilakukan untuk PC yang menggunakan sistem operasi *lagging* (penguncian) dan sistem operasi jaringan. Ini dilakukan untuk mengantisipasi kejadian yang sifatnya disengaja atau tidak disengaja, seperti kelalaian atau keteledoran pengguna yang sering kali meninggalkan komputer dalam keadaan masih menyala, atau jika berada pada jaringan komputer tersebut masih berada dalam *logon user*.

3. Pengamanan data

   Pengamanan data dilakukan dengan menerapkan sistem tingkatan atau hierarki akses di mana seseorang hanya dapat mengakses data tertentu saja yang menjadi haknya.

4. Pengamanan komunikasi jaringan

   Jaringan di sini berkaitan erat dengan pemanfaatan jaringan publik seperti Internet. Pengamanan jaringan dapat dilakukan dengan menggunakan kriptografi di mana data yang sifatnya sensitif dienkripsi atau disandikan terlebih dahulu sebelum ditransmisikan melalui jaringan tersebut.

- **Bentuk-bentuk Ancaman**

Bentuk-bentuk ancaman yang mungkin terjadi pada sistem komputer baik yang berbasis jaringan maupun tidak pada dasarnya dibedakan menjadi empat kategori, yaitu :

1. Interupsi (*Interruption*)

   Interruption merupakan suatu bentuk ancaman terhadap ketersediaan (*availability*), di mana suatu data dirusak sehingga tidak dapat digunakan lagi. Tindakan perusakan yang dilakukan dapat berupa fisik maupun nonfisik. Perusakan fisik umumnya berupa perusakan harddisk dan media penyimpanan lainnya serta pemotongan kabel jaringan, sedangkan perusakan nonfisik berupa penghapusan suatu file-file tertentu dari sistem komputer.

2. Intersepsi (*Interception*)

   Interception merupakan suatu bentuk ancaman terhadap *secrecy*, di mana pihak yang tidak berhak berhasil mendapat hak akses untuk membaca suatu data/informasi dari suatu sistem komputer. Tindakan yang biasa dilakukan biasanya melalui penyadapan data yang ditransmisikan lewat jalur publik/umum.

3. Modifikasi (*Modification*)

   Modification merupakan suatu bentuk ancaman terhadap integritas (*integrity*), di mana pihak yang tidak berhak berhasil mendapatkan hak akses untuk mengubah suatu data atau informasi dari suatu sistem komputer.

4. Pabrikasi (*Fabrication*)

   Fabrication merupakan suatu bentuk ancaman terhadap integritas. Tindakan yang biasa dilakukan adalah dengan meniru dan memasukkan suatu objek ke dalam sistem komputer.

- **Program Perusak/Pengganggu**

1. *Bug*

   Bug merupakan kesalahan-kesalahan yang terdapat pada suatu program aplikasi yang terjadi secara tidak disengaja. Hal ini umumnya dikarenakan kecerobohan dari pihak programer pada waktu menulis program tersebut. *Bug* ini mempunyai dampak yang bermacam-macam seperti komputer menjadi *hang* atau bahkan bisa merusak media penyimpanan pada sistem komputer kita.

2. *Chameleons*

   Chameleons sesuai dengan namanya merupakan program yang diselundupkan atau disisipkan ke dalam suatu sistem komputer dan berfungsi untuk mencuri data dari sistem komputer yang bersangkutan.

3. *Logic Bomb*

   Bomb akan ditempatkan atau dikirimkan secara diam-diam pada suatu sistem komputer yang menjadi target dan akan meledak bila pemicunya diaktifkan. Berdasarkan pemicu yang digunakan, *logic bomb* dapat digolongkan menjadi tiga, yaitu *software bomb*, *logic bomb*, dan *time bomb*. *Software bomb* akan meledak jika dipicu oleh suatu software tertentu, *logic bomb* akan meledak jika memenuhi kondisi tertentu, sedangkan *time bomb* akan meledak pada waktu yang telah ditentukan.

4. *Trojan Horse*

   Prnsip kerja dari trojan horse mirip seperti chameleons, bedanya trojan horse akan melakukan sabotase dan perusakan terhadap sistem komputer yang dijangkitinya.

5. *Virus*

   Pada awalnya *virus* komputer merupakan suatu program yang dibuat hanya untuk menampilkan nama samaran serta beberapa baris kata dari pembuatannya, dan sama sekali tidak membahayakan komputer. Tetapi pada perkembangan selanjutnya pembuat virus komputer mulai menggabungkan beberapa karakteristik dari beberapa program pengganggu dan perusak lainnya dan mulailah bermunculan banyak virus yang dibuat dengan tujuan merusak suatu sistem komputer.

6. *Worm*

   Worm merupakan suatu program pengganggu yang dapat memperbanyak diri dan akan selalu berusaha menyebarkan diri dari satu komputer ke komputer yang lain dalam suatu jaringan. *Worm* menjadikan ukuran suatu file membengkak dan bahkan dapat menguras kapasitas media penyimpanan.

17.4. Ancaman Keamanan Komputer

Serangan pada suatu sistem jaringan komputer sendiri pada dasranya memiliki tiga gelombang tren utama yaitu (Schneier, 2000) :

1. Gelombang pertama adalah serangan fisik.
   Serangan ini ditujukan kepada fasilitas jaringan, perangkat elektronik, dan komputer.
2. Gelombang kedua adalah serangan sintaktik.
   Serangan ini ditujukan terhadap kerentanan (*vulnerability*) pada software, celah yang ada pada algoritma kriptografi atau protokol. Serangan *Denial of Services* (DoS) juga tergolong pada serangan jenis ini.
3. Gelombang ketiga adalah serangan semantik.
   Serangan jenis ini memanfaatkan arti dari isi pesan yang dikirim. Dengan kata lain adalah menyebarkan disinformasi melalui jaringan, atau menyebarkan informasi tertentu yang mengakibatkan timbulnya suatu kejadian.

- **Serangan Lokal**

  Serangan lokal (*Local attack*) atau *console hacking* adalah usaha rekan kita sendiri untuk mengakses data secara tidak sah. Ada beberapa lapis pengamanan terhadap *console hacking,* misalnya mengeset *password* BIOS, mengeset *password screen saver*, mengeset *password* pada folder, dan mengenkripsi dokumen-dokumen penting.

- **Bahaya Internet**

  Infeksi Digital : Virus dan Trojan

- **Serangan Hacker**

  Cracker adalah seseorang yang masuk ke sistem orang lain, biasanya di jaringan komputer, mem-bypass kata sandi atau lisensi program komputer, atau secara sengaja melawan keamanan komputer.

  Hacker menurut *EricRaymond* didefinisikan sebagai programer yang pandai. Sebuah *hack* yang baik adalah solusi yang cantik untuk masalah pemrograman dan “hacking” adalah proses pembuatannya.

17.5 ENKRIPSI

- **Konsep Enkripsi**

Enkripsi adalah proses yang mengubah suatu data menjadi kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi berasal dari bahasa Yunani *kryptos* yang berarti rahasia atau tersembunyi. Sedangkan ilmu yang mempelajari seluk beluk enkripsi dan deskripsi (kebalikan enkrispsi) disebut *Crytography*. Orang yang berusaha memecahkan kode enkripsi tanpa kuncinya disebut *Cryptoanalyst* (*hacker*).

- **Cara Kerja Enkripsi**

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi, data kita disandikan *(encrypted*) dengan menggunakan sebuah kuci (*key*). Untuk membuka (men-*decrypt*) data tersebut, juga digunakan kunci yang dapat sama dengan kunci untuk mengenkripsi (*privat key*) atau dengan kunci yang berbeda (*public key*).

Enkripsi menggunakan semacam algoritma untuk mengubah data atau pesan asli, yang disebut dengan *plain text* untuk menjadi *cipher text*, atau bentuk yang terenkripsi.

Sebaliknya proses untuk mengubah *cipher text* menjadi *plain text* disebut dekripsi. Misalnya kalimat “I Love You” dengan enkripsi Caesar akan menjadi “loryh brx”. Enkripsi Caesar diambil dari nama *Julius Caesar*. Aturan dari enkripsi Caesar adalah menggeser huruf sejumlah bilangan tertentu dengan pesan asli sehingga menjadi huruf lain. Pada contoh di atas, tiap-tiap huruf pada pesan asli digeser 3 huruf ke kanan.

(a b c d e f g h i j k l m n o p q r s t u v w x y z)

Pada prinsipnya model implementasi kriptografi dalam enkripsi data dibedakan menjadi dua, yaitu :

- Kriptografi dengan enkripsi simetris, yaitu penggunaan kunci (*key*) yang sama antara saat pengiriman data dan penerimaan data. Algoritma yang digunakan seperti *Data Encryption Standart* (DES), dan *Blowfish*.
- Kriptografi dengan enkripsi asimetris, yaitu penggunaan kunci (*key*) yang tidak sama (berlainan) saat pengiriman data dan penerimaan data. Sistem ini menggunakan dua buah *key*, yaitu *privat key* dan *public key*.

Model enkripsi yang digunakan secara luas adalah model yang didasarkan pada *Data Encryption Standart* (DES), yang diambil oleh biro Standar Nasional A tahun 1977

17.6 KEAMANAN KOMPUTER

Titik Pengamanan

Titik-titik atau lokasi yang harus diamankan pada komputer yang berbasis jaringan Internet seperti server Web, klien Web (browser Web), *Network Operation System* (NOS) sebagai server, dan transaksi data.

Begitu sebuah komputer terhubung ke Internet, maka peluang bagi pengintip semakin besar untuk menyusup dan mengobrak-abrik file-file kita. Untuk mencegah segala kemungkinan pada komputer atau jaringan, jangan sekali pun memberikan akses kepada orang yang kurang kita percayai.

Untuk menghindari hal tersebut, kita perlu melengkapi komputer atau jaringan dengan beberapa pengaman, di antaranya :

a. *Firewall* untuk meminimalkan kemungkinan hacker masuk secara jarak jauh. Teliti ketika hendak melakukan *file sharing* di jaringan, aturlah dengan tepat siapa saja pengguna yang berhak mengakses komputer kita. Firewall adalah istilah yang bisa digunakan untuk menunjuk pada suatu komponen atau sekumpulan komponen jaringan, yang berfungsi membatasi akses antara dua jaringan.
b. *Zone Alarm* yang selain bisa melindungi PC dari akses ilegal dalam sebuah jaringan, juga berfungsi sebagai firewall. Kita dapat memiliki koneksi Internet software ini pada www.zone-alarm-pro.com atau versi yang gratis di www.zdnet.com. Salah satu fiturnya yang bagus adalah *Trusty IP*. Kita bisa memasukkan nomor alamat IP dari teman yang boleh mengakses PC kita.

Pengamanan E-mail

Akhir-akhir ini virus dan *worm* sering dikirim melalui *attachment* e-mail.

Petunjuk mengirim e-mail secara aman

1. Memiliki kunci publik
2. Kirim e-mail berisi kunci publik ke orang-orang yang kita ingin berkorespondensi dengan mereka menggunakan *secure e-mail*. Saat e-mail itu tiba di *mail client* penerima, kunci publik kita akan secara otomatis ditambahkan ke buku alamat *mail client* penerima.

3. Ketika membalas surat, *e-mail client* miliknya dari buku alamat mengetahui kalau kita mampu bersurat-suratan secara aman. *Mail client* otomatis akan mengode a-mail yang akan terkirim tersebut dengan kunci publik milik kita.
4. Saat menerima e-mail, *mail client* kita secara otomatis membongkar penyandian *mail* terkirim tadi dengan kunci privat, sehingga kita bisa membacanya. E-mail yang aman tidak akan dapat terbaca (dibajak) di tengah jalan.

Tanda Tangan dan Sertifikat Digital

Tanda tangan digital adalah tanda tangan yang dilakukan secara elektronik untuk kepentingan transaksi digital, seperti e-banking dan e-commerce. Teknologi tersebut memanfaatkan teknologi kunci publik. Sepasang kunci publik-privat dibuat untuk keperluan sesorang. Kunci privat disimpan oleh pemiliknya, dan dipergunakan untuk membuat tanda tangan digital.

Sedangkan kunci publik dapat diserahkan kepada siapa saja yang ingin memeriksa tanda tangan digital yang bersangkutan pada suatu dokumen. Proses pembuatan dan pemeriksaan tanda tangan ini melibatkan sejumlah teknik kriptografi seperti *hashing* (membuat 'sidik jari' dokumen) dan enkripsi asimetris. Teknologi kunci publik juga bisa dipergunakan untuk menyandikan/merahasiakan isi dokumen.

Pengamanan Kartu Kredit

Bentuk kejahatan pembobolan kartu kredit adalah bentuk kejahatan yang sering terjadi dalam transaksi perdagangan di Internet.

Selain bentuk pengamanan dengan menggunakan tandatangan digital dan sertifikat digital seperti dijelaskan di atas pada waktu yang hampir bersama dengan tern ini lahir protokol yang disebut *Secure Electronic Transactions* (SET). Protokol yang didesain untuk mengamankan transaksi kartu kredit yang menjadi inti kekuatan untuk menumbuhkan pasar sertifikat digital. Protokol SET, yang akan menjamin transaksi kartu kredit secara online, akan membengkakan perdagangan lewat Internet (e-commerce). Bank akan menjadi pusat kegiatan e-commerce, karena mereka menjadi penerbit sertifikat SET dan melayani pembayaran untuk konsumen maupun pedagang.

Inti dari keamanan dalam protokol SET adalah penggunaan sertifikat digital. Penggunaan sertifikat digital sebagai sarana pengamanan komunikasi memang membuat e-commerce yang menggunakan protokol SET menjadi sistem yang aman.

17.7 PEMELIHARAAN SISTEM

Proses pemeliharaan biasanya dilakukan sebelum perangkat atau data yang digunakan terjadi permasalahan. Artinya bahwa pemeliharaan dilakukan dalam sebagai preventif atau pencegahan dalam sebuah operasi komputer untuk menghadapi sebuah risiko yang mungkin terjadi.

Perawatan terencana dilakukan dengan mendata :

- Jenis dan fungsi komputer
- Komponen-komponen yang dimiliki komputer
- Lama komputer saat digunakan
- Jumlah komputer yang akan dilakukan perawatan

Perawatan terencana dilakukan menjadi tiga jenis perawatan yaitu :

1. **Preventif**, yaitu jenis perawatan yang dilakukan untuk mencegah terjadinya berbagai kemungkinan kerusakan pada sistem komputer. Tindakan preventif tentunya dilakukan sebelum komputer mengalami masalah atau kerusakan.
2. **Prediktif**, yaitu jenis perawatan yang dilakukan karena adanya praduga terhadap sebuah alat atau komponen yang sebenarnya masih berfungsi dengan baik namun diperkirakan tidak lagi tahan sampai dengan pelaksanaan perawatan preventif pada tahap berikutnya.
3. **Korektif**, yaitu tindakan perawatan yang difokuskan terhadap pemeriksaan fungsi dari bagian-bagian utama mesin komputer atau *overload*.

Perawatan yang tidak terencana yaitu perawatan yang dilakukan secara insidental, tidak dapat diduga atau direncanakan sebelumnya, sewaktu-waktu bisa dilakukan.

Menjaga Kinerja Sistem

Untuk menjaga kinerja sistem komputer kita, maka perlu dilakukan langkah-langkah sebagai berikut :

a. **Melakukan update program antivirus secara berkala**

Saat ini banyak jenis variasi virus yang beredar, kebanyakan di antaranya dapat dikelompokkan menjadi enam kategori umum, dimana tiap jenis sedikit berbeda cara kerjanya.

- **Virus boot-sector**. Menggantikan atau memasukkan dirinya ke dalam *boot-sector* sebuah area pada hard drive (atau jenis disk lainnya) yang akan diakses pertama kali saat komputer dinyalakan. Virus ini dapat menghalangi komputer untuk melakukan *booting* dari hard disk.
- **Virus file**. Menginfeksi aplikasi. Virus ini melakukan eksekusi untuk menyebarkan dirinya pada aplikasi dan dokumen yang terkait dengannya saat file yang terinfeksi dibuka atau dijalankan.
- **Virus makro**. Ditulis dengan menggunakan bahasa pemrograman makro yang disederhanakan, dan menginfeksi aplikasi Microsoft Office, seperti Word dan Excel. Sebuah dokumen yang terinfeksi oleh virus makro secara umum akan memodifikasi perintah yang telah ada dan banyak digunakan (seperti perintah "Save") untuk memicu penyebaran dirinya saat perintah tersebut dijalankan.
- **Virus multipartite**. Menginfeksi baik file dan *boot-sector*, penjahat berkedok ganda yang dapat menginfeksikan sistem terus-menerus sebelum ditangkap oleh scanner antivirus.
- **Virus polymorphic**. Akan mengubah kode dirinya saat dilewatkan pada mesin yang berbeda; secara teoritis virus jenis ini lebih susah untuk dapat dideteksi oleh scanner antivirus, tetapi dalam kenyataannya virus jenis ini tidak ditulis dengan baik, sehingga mudah untuk diketahui keberadaannya.
- **Virus stealth**. Menyembunyikan dirinya dengan membuat file yang terinfeksi tampak tidak terinfeksi, tetapi virus jenis ini jarang mampu menghadapi scanner antivirus terbaru.

Indikasi adanya virus pada komputer dapat dilihat pada penjelasan berikut :

- Penambahan ukuran file tanpa alasan yang jelas. Hal ini mengindifikasikan adanya virus.

- Program tidak berjalan secara normal dan diikuti dengan pesan-pesan error. Atau adakalanya disertai dengan animasi-animasi (walaupun menarik).
- Adanya perubahan-perubahan struktur direktori tanpa sebab.
- Penurunan jumlah memori yang tersedia yang disebabkan bukan karena komputer sedang menjalankan program-program komputer.
- Aktivitas sistem keseluruhan berjalan secara lambat. Untuk mengeksekusi program membutuhkan waktu yang lebih lama dari biasanya.

Sedangkan cara mencegah dan menanggulangi virus masuk ke sistem komputer adalah sebagai berikut :

- Mengetahui dengan pasti apakah file atau program yang akan dikirim melalui e-mail tersebut mengandung virus atau tidak.
- Mengetahui dan memastikan *attachment* e-mail tersebut dari siapa, sebelum disimpan atau dijalankan.
- Memastikan bahwa kita telah menanti *attachment* e-mail dari seseorang yang kita kenal dan percayai.
- Menginstalasi software antivirus sekarang pada sistem komputer.
- *Update* secara regular sangat penting.
- Mempunyai komputer *back-up* (cadangan) untuk menyimpan data penting.
- Jika ragu-ragu, hapus beberapa pesan e-mail atau attachment yang mencurigakan dan kirim e-mail kepada pengirim untuk memberitahu bahwa kita mencurigai suatu virus.
- Jangan pernah untuk membuka sebuah lampiran dengan ekstensi file : .EXE, .COM, .VBS, .LNK, .PIF, .SCR, .BAT.

Beberapa langkah dapat kita lakukan untuk menghindarkan sistem dari ancaman virus maupun akibat-akibat buruk yang ditimbulkan. Langkah-langkah tersebut antara lain :

- Pasang antivirus pada sistem kita,
- Update database program antivirus secara teratur.
- Berhati-hati sebelum menjalankan file baru.
- Curigai apabila terjadi keanehan pada sistem kita.
- Back up data kita secara teratur.

b. **Melakukan update sistem operasi**

Untuk melakukan update pada sebuah sistem operasi biasanya dilakukan bila sistem tersebut terjadi masalah (*crash*) pada dukungan sistem aplikasi atau utilitasnya.

c. **Melakukan *ScanDisk* dan *Disk Defragmenter* secara berkala.**

d. **Menghapus *Temporary Files* dan *Internet Files*.**

e. **Mengosongkan *Recycle Bin*.**

f. **Membersihkan *System Tray*.**

Pada taskbar yang terdapat ikon-ikon, itulah yang disebut *System Tray,* dan program dapat meminta Windows untuk menampilkan ikon di situ untuk menampilkan informasi status dak kita dapat mengklik atau klik kanan untuk membukanya.

g. **Setting *Registry*.**

Dalam melakukan menyimpan infomasi berbagai setting dan konfigurasi, Windows menggunakan *registry*. *Registry* merupakan database yang digunakan untuk menyimpan semua setting dan informasi hardware, software.

h. **Tweak UI untuk menambah kecepatan Windows**

Tweak UI, sebuah utilitas yang menawarkan penambahan kecepatan pada Windows, juga memberikan kelebihan yang mengagumkan untuk mengkostumasi dekstop daripada yang biasa.

i. **Kustomasi Menu**

Backup Data

Pemeliharaan komputer yang paling sering dan bahkan rutin dilakukan adalah dengan cara *backup* data (membuat cadangan data) yaitu dengan cara mengcopy atau menggandakan data pada tempat tertentu.

Memelihara Perangkat

Rutinitas perawatan sistem komputer bisa diatur sebagai berikut :

a. Perawatan bulanan

- Hapus semua file yang tidak perlu termasuk yang terdapat pada *Recycle Bin*, selanjutnya lakukan *scan disk* atau *check disk*, dan *defragmentasi*.
- Lakukan backup data pada harddisk secara menyeluruh atau pada file yang baru dan penting.
- Bersihkan debu-debu dan endapan kotoran yang menempel pada keyboard, bola mouse, monitor, dan CPU.

- Lakukan pemeriksaan terhadap kabel-kabel yang ada, mungkin terjepit, lecet, atau bahkan lepas, atur dan rapihkan.

b. Perawatan tengah tahunan atau triwulan

- Bersihkan printer dari debu dan kotoran yang menempel.
- Bersihkan *head* floppy dan CD menggunakan *cleaner* floppy dan CD.
- Jika hard disk banyak yang bad, atau sering terjadi kendala sistem, bisa dilakukan format ulang dan instalasi dengan sistem software yang baru.
- Amati dan lakukan diagnosis pada komponen-komponen penting pada CPU misalnya prosesor dan laju kipasnya, kalau perlu bongkar dan bersihkan tiap bagian dan uji ulang kinerja masing-masing komponen tersebut.