

# Pemeliharaan Komputer

Disusun oleh : Gun Gun Gunawan

NIM : TK010010

[goen2@dikmenjur.net](mailto:goen2@dikmenjur.net)

<http://putra.galuh.web.id>

## Pengantar :

Tulisan ini diperuntukan untuk melengkapi salah satu tugas kuliah D3 Teknik Informatika Politeknik TEDC Bandung Semester ke-6. Harapan penulis semoga dapat menambah kredit point bagi penulis dan tulisan ini dapat bermanfaat bagi pihak yang berkepentingan. Tulisan ini penulis ambil dari beberapa sumber yang penulis cantumkan di akhir pembahasan. Penulis juga tak lupa ucapakan terima kasih kepada semua pihak yang telah membantu penulis untuk menyelesaikan tugas ini.

Beberapa kajian materi diantaranya menyangkut cara dan tips yang dapat dilakukan dalam melakukan perawatan terhadap Komputer baik dari segi Hardware maupun Software.

Berikut adalah beberapa cara atau tips yang bisa dilakukan :

## 1. Strategi backup data

Walaupun komputer kini sudah dipakai oleh hampir semua orang dan digunakan untuk menyimpan berbagai data-data penting, namun saya lihat masih banyak sekali orang yang lupa memperhitungkan kemungkinan lenyapnya data tsb. Komputer tetap adalah perangkat elektronik yang kompleks walau bagaimana pun Microsoft Windows membuatnya nampak sederhana/tidak rumit; dan peluang untuk terjadi berbagai hal-hal yang tidak terduga atas data Anda sangat besar - virus, kerusakan hard disk, kerusakan file data; yang kesemuanya bisa terjadi dengan berbagai cara.

Untuk itu adalah hal yang penting bagi Anda untuk membuat strategi backup data, untuk mencegah lenyapnya data dari komputer. Saya akan listing berbagai hal yang dapat Anda lakukan berikut dengan berbagai kelebihan dan kekurangannya.

### 1. Disket

Secara umum ini adalah ide yang buruk. Disket adalah media yang sangat tidak reliable, sangat banyak hal yang bisa merusakkannya - tergores sedikit, kena magnet, kena panas, terlipat/terduduki/terinjak, head drive yg tidak akurat lagi - dan bahkan Anda diamkan saja rusak lah data Anda (karena berjamur). SELALU HINDARI MENYIMPAN DATA PENTING ANDA DI DISKET.

### 2. Hard disk lainnya.

Jika Anda memiliki lebih dari satu hard disk, ini adalah cara backup data yang paling feasible; cepat dan murah (tidak perlu membeli tambahan peralatan). Kumpulkan data penting Anda di sebuah direktori di hard disk pertama, dan secara rutin duplikasi direktori tersebut ke hard disk kedua.

Kekurangannya, data Anda masih tetap terkumpul di komputer yang sama, jadi problem spt surge/spike (lonjakan arus listrik) sangat mungkin akan merusakkan kedua hard disk tersebut secara bersamaan.

### 3. CD-R (CD Recordable).

Dengan makin menjamurnya drive CD-R maka walaupun Anda tidak memilikinya namun kemungkinan ada teman Anda yang punya. Manfaatkan untuk membackup data Anda; karena kelebihan-kelebihannya seperti harga yang murah (CD-R blank kalau tidak salah harganya sudah

dibawah Rp 10-ribu sekarang), sangat reliable (data di CD-R bisa bertahan selama puluhan tahun jika disimpan sesuai anjuran dari manufacturer-nya), dan kapasitasnya juga cukup besar kalau hanya untuk sekedar menyimpan file-file Microsoft Word (640 MB). Satu lagi adalah Anda dapat mengakses data2 Anda cukup dengan memasukkan CD tsb ke CD drive di komputer mana saja - sangat mudah untuk mengakses kembali data-data Anda. Kekurangannya adalah kecepatan backup yang agak lambat (640 MB biasanya akan memakan waktu sekitar 1 jam), kapasitas yang terbatas untuk backup data dalam jumlah besar (tidak feasible untuk backup data dalam satuan gigabyte), sangat mudah rusak (jatuhkan ke lantai, atau biarkan anak Anda bermain-main dengan CD tersebut - selamat tinggal data), dan harga drive yang mahal (walaupun sudah jauh lebih murah jika dibandingkan dengan beberapa tahun yang lalu).

4. Zip drive.

Kelebihan: Cukup cepat untuk membackup data, harga drive cukup murah sekarang.  
Kekurangan: 100 MB kadang-kadang tidak cukup lagi untuk menyimpan seluruh data Anda, Zip disk reliabilitasnya tidak bisa dijamin, rasio harga disk/kapasitas terlalu mahal, teknologi yang sudah mulai kuno.

5. Jaz drive.

Kelebihan: Cukup cepat untuk membackup data, kapasitas cukup besar (2 GB).  
Kekurangan: Harga disk-nya masih mahal - rasio harga disk/kapasitas kalah dari hard disk (!), reliabilitas jangka panjang masih dipertanyakan.

6. QIC tape drive.

Kelebihan: Harga drive lebih murah daripada DLT drive, harga cartridge juga lebih murah, bisa backup data via parallel port saja.  
Kekurangan: Kapasitas tidak sebesar DLT (maksimum pada saat artikel ini ditulis adalah 30 GB), kecepatan backup sangat lambat, kadang tidak reliable (!).

7. DLT tape drive.

Kelebihan: Sangat cepat dalam mem-backup data, kapasitas besar, reliable.  
Kekurangan: Harga SANGAT mahal (biasanya sekitar ribuan US dolar).

8. Internet.

Ini alternatif baru yang mungkin bisa cukup feasible, berkat munculnya berbagai website yang menyediakan jasa penyimpanan data secara cuma-cuma di Internet. Beberapa contoh, Briefcase (<http://briefcase.yahoo.com> - 25 MB), Freediskspace (<http://www.freediskspace.com> - max. 300 MB), X-Drive (<http://www.xdrive.com> - sekitar 50 MB), dan lain-lain.

Kelebihan; gratis, dan backup data Anda bisa diakses dari seluruh dunia.  
Kekurangan: tidak efisien untuk data dalam jumlah besar terlebih jika koneksi Internet Anda via modem.

Juga sangat penting untuk tidak HANYA membackup data di Internet, karena ini adalah jasa gratis sehingga kalau tiba-tiba (misalnya) mereka mengalami masalah maka tidak ada yang dapat Anda lakukan. Backup juga data Anda dengan alternatif lainnya.

Satu hal yang penting untuk Anda ingat selalu:

***Tidak ada istilah "terlalu banyak backup" bagi data Anda  
Selalu duplikasi data penting Anda sebanyak-banyaknya***

Pengalaman pribadi, saya membuat beberapa copy dari data2 penting saya. Pertama saya copy-kan ke hard disk saya yang satu lagi. Kedua saya copy-kan ke hard disk di komputer adik saya. Ketiga saya copy-kan ke CD, dan disimpan di rumah. Keempat saya copy-kan ke CD dan saya bawa jika

bepergian jauh, jadi secara teori bahkan sekalipun yang terburuk terjadi (spt rumah terbakar, dll) data2 penting saya tetap akan selamat.

Mungkin Anda akan berpikir "wah repot sekali". Namun apa yang terjadi? Hard disk saya crash, sehingga datanya hilang. Lalu data yang ada di hard disk yang lainnya juga hilang/corrupt. Dan, backup data di CD di rumah saya tidak bisa ditemukan....

Untungnya masih ada backup data di CD yang saya bawa-bawa, dan akhirnya data penting yang dikumpulkan selama bertahun-tahun kembali selamat. Saya tidak bisa membayangkan bagaimana jadinya kalau saya tidak melakukan proses backup data 4 lapis spt ini. Setelah itu saya semakin meng-intensifkan dan mengawasi proses backup data saya secara lebih ketat.

Ini baru untuk data pribadi, untuk data perusahaan harusnya lebih komprehensif lagi prosedurnya. Namun masih juga sering saya dengar bagaimana perusahaan menolak mem-backup data mereka karena "tape drive harganya mahal" dll. Sama saja mencari masalah ini namanya.

### **Beberapa TIPS:**

- Kumpulkan data-data penting Anda di satu direktori saja; misal: C:MyDocument. Disiplin spt ini akan sangat memudahkan Anda dalam melakukan backup atas data-data tsb. (bayangkan misalnya data Anda ada di C:/, D:/MyDocument, C:/ProgramFiles/MicrosoftOffice/Word, dan C:/ProgramFiles/MicrosoftOffice/Excel ? Anda akan keburu segan duluan untuk mem-backup data2 tsb)
- Bagaimana interval backup data yang baik?

Sebenarnya ini tergantung dari seberapa sering Anda meng-update data Anda. Jika data Anda kebanyakan adalah arsip2 file saja yang jarang di-update, maka mungkin satu bulan sekali saja sudah mencukupi. Namun jika setiap hari selalu ada penambahan/update data, maka berdasarkan pengalaman saya maksimal adalah setiap 3 hari sekali. Untuk perusahaan; strategi standar adalah dengan menggunakan sistim backup grandfather-father-son, yaitu 5 buah tape digunakan untuk membackup data (incremental) setiap hari, lalu 4 buah tape untuk membackup data setiap weekend (1 tape tiap minggu, jadi meng-cover data selama satu bulan) full backup, lalu 1 buah tape untuk full backup bulanan.

- Test backup data Anda!

Tidak ada gunanya Anda memiliki puluhan backup data kalau semuanya tidak bisa diakses toh? Namun pada kenyataannya masih banyak orang yang hanya mem-backup datanya tanpa melakukan test apakah bisa datanya tersebut itu diakses kembali. Point ini terutama relevan sekali dengan QIC tape drive, saya pribadi sudah mengalami sendiri bagaimana data perusahaan selama bertahun-tahun yang setiap hari di-backup ternyata ketika dibutuhkan tidak bisa di-restore, betul-betul horor. (walau pada akhirnya bisa juga diakses dengan menggunakan tape drive lainnya, tapi mungkin saya hanya sedang mujur saja).

## **2. Antisipasi Virus Komputer**

***Tahukah Anda bahwa program antivirus yang semestinya dapat melindungi data Anda juga dapat berbahaya jika tidak digunakan dengan benar?. Kenapa ? Apa yang bisa kita lakukan sebagai user?, apa yang seharusnya kita lakukan sebagai programmer antivirus?.***

Sejak pertama ditemukan virus telah mengalami perkembangan teknologi yang cukup besar, demikian juga program Antivirus yang ada. Sayangnya perkembangan Antivirus biasanya hanya mengejar perkembangan virus dan bukan berusaha mendahuluinya. Antivirus yang ketinggalan (teknologinya) justru dapat mengundang bahaya bagi pemakai.

Ketika virus-virus berhasil dideteksi keberadaannya, virus-virus yang baru selalu bermunculan dengan teknologi yang lebih canggih yang membuat antivirus menjadi tak berdaya . Antivirus yang lama misalnya, selalu dapat di-'tipu' dengan teknologi stealth, dengan demikian ketika antivirus ini

berusaha mendeteksi file-file yang lain, virus yang *stealth* tadi justru menyebarkan dirinya ke setiap file yang diperiksa.

Di berbagai majalah tentunya Anda sering melihat adanya program-program antivirus " satuan " (spesifik) yang tujuannya untuk mendeteksi satu jenis virus. Biasanya para pembuat antivirus tidak memberitahukan cara-cara yang benar untuk menggunakan program antivirus ini, padahal antivirus spesifik memiliki risiko yang besar jika tidak digunakan secara benar.

Antivirus spesifik hanya mampu mendeteksi satu jenis virus (dan mungkin beberapa variannya) dan biasanya mampu melumpuhkan virus di memori. Jika Anda menemukan suatu virus dan Anda yakin nama virusnya Anda bisa menggunakan Antivirus semacam ini, namun jika Anda tidak tahu, sebaiknya jangan coba-coba. Jika ternyata virus yang aktif adalah virus lain, yang tentunya tidak terdeteksi oleh antivirus ini, maka antivirus tersebut justru dapat menyebarkan virus yang ada ke seluruh file program yang diperiksanya.

Bahaya yang lebih menakutkan adalah jika antivirus salah mendeteksi suatu virus dan salah membersihkannya sehingga file program yang Anda coba untuk perbaiki justru menjadi rusak. Kejadian ini pernah terjadi misalnya pada kasus virus DenHard, virus ini benar-benar mirip dengan die hard, namun virus ini menggunakan teknik yang berbeda untuk mengembalikan header file yang asli, beberapa antivirus yang berusaha membersihkannya justru merusakkan file program tempat virus itu berada. Selain terjadi pada kasus virus DenHard, kasus inipun pernah (dan mungkin masih akan terus) terjadi pada beberapa virus. Salah satu alasan para pembuat virus membuat virus yang mirip adalah supaya virus tersebut sulit dibersihkan, karena para pembuat antivirus tidak suka jika virusnya dapat dengan mudah dibersihkan oleh user.

#### **SUMBER BAHAYA PROGRAM ANTIVIRUS**

Program Antivirus bisa berbahaya karena sebab-sebab berikut:

- Beberapa program antivirus hanya menggunakan teknik sederhana yang bisa dengan mudah ditipu oleh pembuat virus. Misalnya program antivirus hanya memeriksa beberapa byte di awal virus, pembuat virus bisa saja membuat virus versi lain yang sama di bagian awal tetapi berbeda di bagian-bagian yang penting, misalnya di rutin enkripsi/dekripsi header file asli. Ini akan membuat program antivirus menjadi perusak file bukan penyelamat file. Beberapa antivirus juga dapat ditipu dengan mengubah-ubah file signature antivirus. File signature merupakan file yang berisi ID dari setiap virus yang dikenal oleh antivirus, jika ID tersebut di ubah maka antivirus tidak akan mengenalnya. Antivirus yang baik seharusnya dapat memeriksa jika file signature-nya berubah.
- Program Antivirus tidak membuat backup file yang dibersihkan. Sering program antivirus (terutama yang spesifik) tidak menyediakan sarana untuk membuat backup file yang dibersihkan, padahal ini sangat penting andaikata proses pembersihan gagal.
- Program Antivirus tidak melakukan self check. Self check itu perlu, program antivirus dapat saja diubah oleh orang lain sebelum sampai ke tangan pengguna. Program-program antivirus komersial biasanya melakukan self check untuk memastikan dirinya tidak diubah oleh siapapun, namun ada juga yang tidak dan ini berbahaya. Pada program-program antivirus lokal, yang sering disertakan pada beberapa artikel komputer, biasanya menyertakan source code-nya, sebaiknya Anda mengcompile sendiri source tersebut jika Anda ragu pada keaslian file exe-nya.
- Program Antivirus residen bisa di *matikan* dengan mudah. Antivirus residen yang baik seharusnya tidak bisa dideteksi dan di uninstall dengan mudah. Contoh antivirus residen yang kurang baik adalah VSAFE (ada di paket DOS). VSAFE bisa dideteksi dan dimatikan dengan menggunakan interrupt (coba Anda pelajari/debug program vsafe yang ada di DOS agar Anda mengerti). Pemakai akan mendapatkan rasa aman yang palsu dengan menggunakan antivirus semacam ini. Tidak ada rasa aman justru lebih baik dari rasa aman yang palsu.
- Program antivirus tidak memberi peringatan kadaluarsa. Seiring dengan berjalannya waktu, virus-virus yang bermunculan semakin banyak dan tekniknya semakin canggih. Program antivirus yang baik sebaiknya memberi peringatan jika Antivirus yang digunakan sudah terlalu out of date. Ini penting supaya kejadian antivirus yang menyebarkan virus tidak terulang.

#### **INILAH YANG PERLU ANDA LAKUKAN SEBAGAI PENGGUNA**

Sebagai pengguna program antivirus ada beberapa hal yang bisa Anda lakukan untuk meminimalkan risiko penggunaan antivirus

1. carilah antivirus yang baik, baik di sini artinya program tersebut dapat dipercaya untuk mendeteksi dan membasmi berbagai virus yang ada. Jangan terbuai dengan janji-janji yang ditawarkan para vendor antivirus, dan jangan terbuai juga dengan nama merk yang cukup terkenal. Cobalah cari perbandingan antara berbagai antivirus di berbagai majalah / situs di internet.
2. gunakan selalu Antivirus terbaru, Anda bisa mendapatkannya dari Internet atau dari beberapa majalah. Antivirus yang lama memiliki risiko yang besar jika digunakan (lebih dari 6 bulan sudah sangat berbahaya).
3. buatlah cadangan untuk data dan program Anda yang penting.
4. lakukan proses pembersihan virus dengan benar jika Anda menemukan virus
5. pastikan program Antivirus yang Anda dapat adalah yang asli, ada kemungkinan seseorang telah mengubah antivirus tersebut, atau mungkin menularinya dengan suatu virus.
6. Hubungi ahlinya jika Anda merasa tidak dapat mengatasi virus di komputer atau jaringan Anda.

Langkah proses pembersihan yang baik adalah sebagai berikut :

Jika Anda menjalankan komputer pribadi

1. Boot komputer Anda dengan disket startup yang bersih dari virus (dan di write protect)
2. Jalankan program virus scanner/cleaner pada sebuah file yang terinfeksi
3. Coba jalankan file tersebut, jika file tersebut menjadi rusak, jangan teruskan lagi
4. Jika program dapat berjalan lancar, cobakan sekali lagi pada beberapa file (cari yang ukurannya kecil, yang sedang dan yang besar). File yang ukurannya besar perlu di-check, biasanya file ini mengandung internal overlay yang membuat filenya rusak jika terkena virus.

Jika Anda adalah Admin jaringan, sebaiknya Anda mengambil sampel virus ke disket dan mencoba untuk membersihkannya di komputer lain, ini dilakukan untuk tidak mengganggu pekerjaan yang mungkin sedang dilakukan oleh orang lain. Hal ini juga untuk mengantisipasi, kemungkinan adanya virus baru yang mirip dengan virus lain (bayangkan apa jadinya jika terjadi salah pembersihan sehingga seluruh program di jaringan menjadi tidak bisa dipakai!). Jika gagal dibersihkan Anda perlu memanggil ahlinya untuk menangani, atau mencari informasi lebih lanjut di Internet. Percobaan pada beberapa file tujuannya untuk mencegah salah deteksi dan atau salah perbaikan oleh program antivirus. Jika virus dianggap berbahaya dan aktivitas menggunakan jaringan bisa ditunda sementara, mungkin untuk sementara jaringan dimatikan.

### **SEBAGAI PROGRAMMER INI YANG PERLU ANDA LAKUKAN**

Saat ini untuk menjadi programmer antivirus yang baik tidaklah mudah, Anda perlu tahu teknik-teknik pemrograman virus yang setiap hari semakin bertambah sulit. Program antivirus yang Anda buat sebaiknya juga mengikuti perkembangan teknologi virus. Untuk membuat program antivirus yang baik tidaklah mudah, namun ada beberapa hal yang perlu Anda ingat sebagai pembuat Antivirus jika Anda ingin program Anda dipakai orang lain, dan tidak membahayakan orang tersebut

1. Program Anda sebaiknya bisa mematikan virus di memori, dan dapat memberi peringatan jika ada sesuatu yang aneh di memori komputer pemakai (misalnya besar base mem kurang dari 640 Kb)
2. Dalam membuat ID virus pilihlah beberapa lokasi, lokasi yang baik adalah di awal virus dan di bagian penting virus (misalnya di bagian dekripsi header program asli) ini untuk memastikan tidak ada yang mengubah lokasi dan sistem enkripsi (jika ada) header program asli.
3. Jika data/header di enkrip, verifikasi data yang didapat dari perhitungan, misalnya lihat apakah CS dan IP asli yang di dapat dari perhitungan masih dalam batas besar file, atau apakah instruksi JMP pertama di file COM masuk akal (kurang dari panjang file).
4. Buat cadangan file jika file yang dibersihkan dikhawatirkan rusak
5. Lakukan self check di awal program. Jika tidak seluruh bagian program bisa di self check, bagian ID virus perlu diperiksa apakah berubah atau tidak (misalnya dengan checksum).
6. Buatlah penjelasan yang jelas tentang cara penggunaan antivirus
7. Jika program hanya dapat dijalankan di DOS periksalah selalu ketika program dijalankan apakah program tersebut benar-benar berjalan di DOS
8. Jika ingin membuat program antivirus residen, jangan memakai ID virus yang tidak terenkripsi di memori, antivirus lain yang tidak mengenal antivirus Anda tersebut, justru akan menganggap adanya sebuah (atau beberapa buah) virus aktif di memori. Hal ini bisa terjadi, karena beberapa antivirus memeriksa seluruh memori terhadap adanya ID virus.

9. Untuk antivirus yang non residen teknik no 8 juga perlu digunakan, ini perlu agar program antivirus yang lain tidak mengira program ini terkena virus. Kadang-kadang program juga meninggalkan *bekas* di memori, yang mungkin bisa dicurigai oleh antivirus lain sebagai virus. Jika Anda tidak ingin menerapkan teknik tersebut, Anda bisa menghapus memori variabel ID virus setelah selesai digunakan.
10. Jika mungkin, untuk virus yang polimorfik gunakan metode heuristic (dan atau emulasi) untuk men-scan dan teknik emulasi untuk mendekrip, atau mengembalikan program asli.

Seharusnya 10 hal tersebut cukup, Anda bisa menambahkan sendiri hal tersebut jika perlu. Misalnya masalah kecepatan scanning dan lain-lain.

### **TIPS**

- Update anti-virus Anti-virus HARUS rutin di-update, agar dapat selalu menangkal virus-virus baru yang terus bermunculan setiap hari. Kunjungi secara rutin situs pembuat antivirus yang digunakan.
- Juga dengan berhenti menggunakan Microsoft Outlook, maka Anda akan selamat dari berbagai virus yang ada. Gunakan software lainnya seperti Eudora (<http://www.eudora.com>) atau Pegasus Mail (<http://www.pmail.com>)
- Antivirus yang pada dasarnya relatif sama, yang penting anda melakukan update secara rutin seperti diterangkan di atas. Selain antivirus komersial tersedia juga anti-virus yang gratis dan cukup baik antara lain Grisoft (<http://www.grisoft.com>) dan Avast! 4 Home (<http://www.avast.com>).
- Secara fisik membersihkan komputer baik bagian luar maupun dalam casing dari debu dan benda-benda asing lainnya, yang dapat mempengaruhi kinerja dan fungsi perangkat komputer.
- Memastikan sistem pendingin dan sirkulasi udara dalam casing berjalan dengan baik sehingga temperatur komputer bisa terjaga. Untuk komputer yang beroperasi 24 jam nonstop disarankan diletakkan di ruangan yang menggunakan pendingin (AC)
- Defrag sebaiknya tidak terlalu sering dilakukan. Defrag biasanya hanya dilakukan jika proses baca-tulis ke harddisk terasa lambat, akan menginstal program besar, atau akan mengkopikan file ukuran besar ke harddisk.

Hard disk saat ini sudah sangat kencang, sehingga data yang terfragmentasi biasanya tidak akan banyak memperlambat. Komputer yang lambat seringkali disebabkan karena hal lain; kekurangan memory, ada virus, dan sebagainya. Lagipula full defrag sangat intensif, sehingga jika sering-sering dilakukan maka akan memperpendek umur hard disk.

### **3. Amankah PC Anda???**

***Apakah Anda memiliki banyak data penting yang tersimpan dalam komputer Anda di rumah?, Anda sering kesal dengan orang-orang yang selalu mengganggu hasil pekerjaan, atau Anda sering heran dengan data-data Anda yang sering hilang. Jika jawaban Anda adalah ya, Anda perlu membaca artikel ini.***

Mungkin Anda pernah mengalami data penting Anda yang Anda simpan di komputer Anda di rumah tiba-tiba hilang atau berubah di sana-sini. Kadang Anda tidak tahu siapa pelakunya dan kadang Anda tahu bahwa pelakunya adalah seorang pemula yang *tidak sengaja* merusak data Anda. Meskipun Anda tahu pelakunya dan telah menasihatinya tidak menjamin bahwa hal semacam itu tidak akan terjadi untuk yang kedua kalinya oleh karena itu Anda perlu melindungi komputer Anda. Sebenarnya sudah cukup banyak artikel yang membahas hal pengamanan komputer namun saya akan berusaha membahasnya secara lebih detail disertai dengan kelemahan-kelemahan dari setiap cara yang ada dan bagaimana cara menanggulangnya.

### **Siapa Yang Perlu di Waspadai**

Sebelum melakukan langkah-langkah pengamanan sebelumnya tentu kita harus mengetahui siapa yang menjadi lawan kita dalam mengamankan komputer. Yang menjadi lawan yang paling utama dari keamanan komputer kita adalah kita sendiri, kecerobohan kita lebih sering membuat kerusakan dibanding orang lain. Kealpaan untuk men-scan program baru misalnya, dapat menghancurkan seluruh data yang Anda miliki. Karena diri kita yang menjadi musuh maka tak ada cara lain selain untuk menerapkan disiplin kepada diri sendiri.

Musuh yang kedua adalah orang dekat Anda, telah terbukti melalui riset bahwa pelaku kejahatan komputer adalah orang dekat korban, atau di perusahaan-perusahaan yang menjadi pelaku adalah mereka yang justru dipercaya untuk mengamankan perusahaan tersebut. Mungkin juga orang dekat Anda itu tidak bermaksud merusak data Anda atau melihat data Anda tapi mereka tetap saja bisa melakukannya secara tidak sengaja. Musuh yang lain 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.

### **Pengamanan Fisik**

Inilah tingkat pengamanan pertama dan yang paling aman, taruh PC Anda di tempat yang aman. Kunci pintunya ketika Anda pergi. Mungkin cara inilah yang paling aman, kecuali mungkin ada maling yang *menggondol* komputer Anda. Jika data Anda memang penting dan komputer itu memang hanya akan Anda gunakan sendiri mungkin 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.

### **Password BIOS, pertahanan pertama**

Dari segi komputer inilah pertahanan pertama Anda. Jika Anda menyalakan fasilitas password BIOS Anda, maka begitu komputer dinyalakan Anda akan disodori sebuah tampilan yang menanyakan password Anda. Sebagian orang memakai fasilitas ini dan memandangnya sebagai cara yang *aman*. Namun ada juga yang menolak memakainya, alasannya biasanya karena tampilannya yang kurang *keren*. Biasanya pemakaian password bisa diatur, bisa untuk pengamanan seluruh sistem atau cukup pengamanan setup BIOS. Pertama akan saya bahas kelemahan bila Anda memakai pengamanan untuk seluruh sistem.

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. Mulanya password default ini hanya digunakan oleh para teknisi AWARD jika sedang kepepet namun rupanya hal ini telah dimanfaatkan secara tidak benar oleh banyak orang. Untuk versi 2.xx dan 4.xxg password defaultnya sama untuk setiap komputer (mungkin artikel mengenai ini akan saya letakkan di homepage ini, jika saya sudah punya waktu). Untuk versi 5.xx atau di atasnya password defaultnya berbeda untuk setiap komputer dalam hal dua karakter di belakangnya sehingga total ada 676 password default (karena dua karakter terakhir hanya berkisar antara 'A'..'Z'). Saya sendiri masih belum meneliti apakah dua karakter di belakangnya ini bergantung pada nomor seri BIOS.

BIOS buatan pabrik lain tidak memiliki kelemahan yang dimiliki oleh AWARD, namun Anda jangan terlalu gembira, masih ada cara lain untuk menerobos password BIOS. Perlu Anda ketahui 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. Nah perkecualian yang terakhir itulah yang menjadi masalah, jika ada orang yang membuka casing CPU Anda dan menghubungkan ujung positif dan ujung negatif batere CMOS maka semua data yang ada di CMOS akan hilang termasuk password BIOS. Jika data ini sudah hilang orang bisa dengan bebas masuk.

Pengamanan untuk masalah itu adalah dengan menaruh System Unit Anda di tempat yang sulit dikeluarkan, atau menambahkan kunci agar sulit dibuka. Untuk masalah password default AWARD, Anda bisa mengupdate BIOS Anda atau mengganti password default dengan program dari AWARD. Tapi jangan terlalu kuatir, tidak banyak yang tahu masalah password default ini.

Anda juga bisa membuat pengamanan di 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. Setahu saya 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.

### **Pengamanan tingkat sistem operasi**

Bagi Anda pengguna DOS mungkin mengenal pengamanan dengan membuat password di AUTOEXEC.BAT. Anda perlu tahu bahwa pada DOS versi-versi yang terbaru (kalau tidak salah 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 orang yang mengklaim mampu melindungi Windows 95/98 dengan password namun saya belum pernah mencobanya, karena saya kurang Percy dengan program-program tersebut. Perlu Anda ketahui ada begitu banyak lubang keamanan di Windows 95/98. Anda dapat menekan F8 di awal proses boot yang memungkinkan Anda masuk ke DOS dan memodifikasi semua file sistem Windows, seperti misalnya WIN.INI dan file registry. Perlu Anda ketahui 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). Mungkin Anda mengira registry tidak bisa dimodifikasi dari DOS, Anda salah, program regedit.exe yang ada di disket startup WINDOWS 95/98 bisa mengubah file registry menjadi file teks biasa dan sebaliknya sehingga Anda 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. Seperti sudah saya sebutkan dengan cara inipun orang masih bisa masuk menggunakan startup disknya sendiri. Anda bisa saja mematikan drive A sehingga tidak bisa digunakan untuk boot, namun anda akan kesulitan jika suatu ketika Windows anda 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.

Untuk sistem operasi yang lain tidak saya singgung di sini karena umumnya pemakai PC di Indonesia masih memakai ketiga sistem operasi di atas. Seperti yang Anda bisa lihat pengamanan di tingkat sistem operasi ini sangat mudah diterobos. Solusi yang benar-benar baik saya kira sulit, setiap sistem operasi punya kelemahannya sendiri. Dan sistem operasi apapun tidak akan bisa menahan serangan jika penyerang punya akses fisik ke komputer.

### **Proteksi tingkat aplikasi**

Jika Anda memiliki program-program penting yang ingin Anda lindungi Anda 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. Oh ya, hati-hati dengan program yang memberi password pada file EXE DOS, buat 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.

### Proteksi tingkat dokumen

Inilah level proteksi terakhir, jika ini berhasil dibongkar maka data-data penting Anda mungkin akan terbaca oleh orang lain. Untuk program-program yang menyediakan password ketika menyimpan filenya Anda 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 Anda kelewat penting namun Anda terpaksa menyimpannya di rumah maka enkriplah data Anda itu menggunakan program yang benar-benar aman kalau perlu letakkan di disket dan simpan di tempat yang aman. Tahukah Anda bahwa password PKZIP/WINZIP atau ARJ, yang dikira aman, juga bisa dibongkar? (walaupun tidak mudah). Oleh karena itu Anda perlu menanyakan dulu kepada ahlinya sebelum Anda menggunakan suatu program enkripsi.

### Pengamanan dari ketidaksengajaan

Tidak selamanya Anda berhadapan dengan hacker, mungkin yang Anda takutkan cuma anak Anda tanpa sengaja menghapus dokumen penting Anda atau bermain-main dengan gambar yang Anda miliki, atau Anda punya koleksi gambar-gambar yang akan membuat Anda menjadi malu jika ketahuan orang lain.

Untuk masalah di atas ada beberapa hal yang bisa dilakukan. Pertama buatlah sebuah direktori khusus di mana anda akan meletakkan file-file Anda, pindahkan file-file penting Anda 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 Anda yang menggunakan sistem operasi Windows 95/98, jangan membeli program yang akan menghilangkan semua peringatan ketika Anda menghapus file apa saja, Gunakan shell explorer (Default windows 95/980 kecuali Anda punya shell yang jauh lebih baik. Jalankan explorer (bagi Anda yang memakai explorer sebagai shellnya) kemudian pilih menu **view | options** pada tab **View** pilihlah **hide file of these types** dan klik **OK**. Anda juga bisa mengganti ekstension file Anda dengan daftar yang terpampang pada langkah di atas sehingga file Anda 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. Ubahlah 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. Buatlah cadangan data untuk data yang memang benar-benar penting.
3. Ajarkan kepada pemakai komputer baru langkah-langkah apa yang boleh dan yang tidak boleh diambil dalam mengoperasikan komputer.
4. Install Anti Virus yang up to date, carilah antivirus yang bisa secara otomatis bekerja di background dan bisa memonitor semua jenis virus termasuk virus dokumen.

Secara umum keempat langkah di atas sudah cukup baik untuk mencegah kesalahan karena ketidaksengajaan. Anda bisa menambahkan sendiri langkah-langkah yang dianggap perlu.

### Membuat password yang baik

Password yang baik sangat penting untuk mengamankan komputer Anda oleh karena itu Anda harus mengetahui cara membuat password yang baik. Walaupun program yang Anda gunakan sangat canggih, data Anda bisa saja dibongkar jika seseorang mengetahui password Anda. Beberapa teknik yang diajarkan di sini berlaku juga untuk password non komputer yang Anda miliki (ATM, TeCC, dan lain-lain) Mungkin Anda sudah sering mendengar bagaimana membuat password yang baik, namun biasanya tidak pernah diberi penjelasan mengapa nah sekarang akan saya jelaskan.

1. Jangan pernah memakai kata yang umum yang ada di kamus, apalagi kamus bahasa Inggris. Kenapa ?, para hacker kadang menggunakan kamus untuk menebak password Anda dengan program, cara ini dikenal dengan *dictionary password cracking/dictionary password attack*.

2. Gunakan kombinasi angka dan huruf . Beberapa program menggunakan *brute force cracking/brute force attack* maksudnya program akan mencoba semua kombinasi aa, ab , ac dst sampai passwordnya ketemu, nah untuk melakukan ini diperlukan waktu yang sangat lama, oleh karena itu biasanya beberapa program di set hanya untuk mencari password berupa huruf saja. Sebagai perbandingan coba bandingkan berapa kombinasi yang harus dicari jika menggunakan huruf saja dan kombinasi yang harus dicari bila menggunakan kombinasi huruf dan angka. Rumusnya : banyaknya kombinasi = banyak jenis huruf pangkat panjang password. Untuk password yang memakai huruf saja anggap jenis hurufnya ada 52 (A-Z dan a-z) dan untuk yang memakai huruf dan angka jenis hurufnya ada 62 (A-Z, a-z dan 0..9).
3. Password minimal 5 karakter, kurang dari itu akan mudah sekali ditebak.
4. Gantilah password Anda secara periodik.
5. Jangan gunakan password yang sama untuk berbagai hal. Jika Anda seorang system administrator jangan gunakan password SUPERVISOR anda sebagai password Screen Saver. Mungkin orang akan sulit menebak password supervisor, tapi password screen saver mudah sekali didekripsi.
6. Jangan gunakan tanggal lahir Anda atau keluarga Anda, jangan gunakan nomor telepon Anda atau nomor plat mobil Anda sebagai password (berlaku juga untuk password ATM). Ingat musuh Anda adalah orang dekat Anda yang mungkin tahu itu semua.
7. Jangan bertukarkan password Anda kepada siapapun, termasuk kekasih Anda.
8. Jika ada yang menelepon Anda dan mengatakan bahwa dia perlu password ATM Anda atau password apa saja, JANGAN berikan apapun alasannya (biasanya alasannya kesalahan komputer atau ada pemeriksaan bahwa kartu ATM Anda telah disalahgunakan). Walaupun yang menelpon mengaku dari Bank atau dari Polisi. Hubungi Customer Service Bank itu dan tanyakan kebijakan bank mengenai masalah itu, karena bank tidak pernah menanyakan hal-hal semacam itu. Jika yang menelpon polisi tanyakan nama, pos tempatnya bekerja dan nomor di kartunya. Verifikasikan hal ini ke kantor polisi yang bersangkutan jika Anda ragu.
9. Passwordnya harus mudah diingat, karena kelalaian Anda bisa menimbulkan masalah. Untuk ini Anda bisa menggunakan kombinasi nama dan nomor telepon orang yang Anda sukai yang TIDAK diketahui siapapun. Atau gunakan kombinasi yang hanya Anda sendiri yang tahu.
10. Untuk password email gratis di internet biasanya Anda akan diminta memasukkan hint question ketika Anda mendaftar. Guna hint question ini jika anda lupa password Anda, mereka akan menanyakan pertanyaan di hint question yang sangat mudah dan mereka akan memberi tahu Anda password Anda. Jika Anda yakin akan selalu ingat password Anda, jangan isi pilihan hint question. Jika Anda takut lupa pilihlah pertanyaan yang agak sulit seperti **what is your mother's maiden name?** dan jangan pertanyaan seperti di mana kamu lahir atau yang lainnya yang sederhana. Banyak sekali orang yang ketahuan passwordnya hanya karena hal sepele ini.

### Menghapus File

Jika Anda berniat menghapus file untuk menghapus jejak jangan gunakan perintah del./erase biasa, gunakan program khusus karena sebenarnya perintah del /erase tidak menghapus data Anda. Data tersebut masih bisa dikembalikan dengan program Unerase.

### Sumber Referensi :

---

1. pangsit.com "**Harry Sufehmi, tanggal: 13 September 2000**"
2. langitbiru.hypermart.net "**Amankah PC Anda???**"
3. langitbiru.hypermart.net "**BAHAYA PROGRAM ANTIVIRUS**"