Jurnal Teknovasi
Volume 03, Nomor 1, 2016, 8-15
ISSN : 2355-701X

KEYLOGGER PADA ASPEK KEAMANAN KOMPUTER

Muhammad Siddik Hasibuan
Magister Teknik Informatika, Universitas Sumatera Utara
Jl. Almamater Kampus USU, Medan 20155, Telp. 061-8219005, Fax. 061-8213250
Email : mhdsiddikhasibuan@gmail.com

ABSTRAK

Keamanan data dalam pengaksesan komputer adalah salah satu bentuk yang harus diperhatikan baik secara fisik maupun non fisik. Salah satu bentuk kejahatan pencurian data adalah merekam jejak keyboard komputer dengan bantuan hardware maupun software. Keylogger adalah teknik pencurian data dengan merekan ketikan di keyboard komputer, dengan merekam ketikan komputer tersebut pihak intruder dapat masuk dan mencuri. Tujuan dari penulisan ini adalah untuk memahami bagaimana cara kerja keylogger agar dapat dilakukan cara pencegahan dengan melakukan berbagai macam solusi dan juga untuk mempertahankan sistem keamanan data serta mengetahui software pendukung dan anti keylogger. Metode pencegahan terhadap keylogger dilakukan secara fisik dengan melihat hardware dan non-fisik yaitu software keylogger pada komputer tersebut. perekaman jejak ketikan adalah suatu hal yang dapat terjadi dimana saja tanpa kita sadari, hal yang paling penting untuk mengamankan data selalu mengawasi penggunaan suatu media penyimpan data, network dan selalu menggunakan anti virus yang terupdate.

Keyword : **Keylogger, intruder, Keamanan Data**

PENDAHULUAN

Bidang Keamanan Komputer secara terus menerus mengalami perkembangan luar biasa sebab teknologi informasi memiliki pengaruh yang semakin tinggi terhadap bagaimana kita bekerja, berkomunikasi, berbelanja dan menikmati hiburan. Seiring dengan perkembangan itu maka semakin besar pula ancaman-ancaman terhadap keamanan komputer kita, baik ancaman berupa fisik maupun non fisik seperti *security hole* pada sistem operasi, serangan pada jaringan, virus, dan lain-lain. Dalam membangun sebuah sistem jaringan berbasis internet, masalah keamanan menjadi suatu hal yang mutlak diperlukan. Sistem yang dibangun tanpa adanya sistem keamanan yang baik sama halnya dengan mengajak pencuri untuk masuk ke rumah kita dan membiarkan dia mengambil segala sesuatu yang kita miliki. Seringkali ketika membangun sebuah sistem, kita menemukan berbagai kerawanan dalam sistem kita. Namun hal itu kita anggap sebagai hal kecil karena kita tidak menganggapnya sebagai lubang keamanan (*hole*). Kita tidak sadar bahwa kerawanan-kerawanan kecil seperti inilah yang dimanfaatkan oleh orang-orang yang tidak bertanggungjawab untuk menjalankan aksi kejahatannya.

Menurut Howard (1997) dalam bukunya "*An Analysis of security incidents on the internet*" menyatakan bahwa : "Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab".

Kemajuan sistem informasi memberikan banyak keuntungan bagi kehidupan manusia. Meski begitu, aspek negatifnya juga banyak, seperti kejahatan komputer atau penyerangan yang berupa penyadapan data di jaringan komputer oleh pihak-pihak yang tidak bertanggung jawab. Hal ini terjadi karena kurang pengamanan yang tepat maupun ketidaktahuan masyarakat awam. Bahkan korban penyadapan ini pun tidak sadar bahwa ada seseorang yang sedang menyadapnya. Penyadapan ini dilakukan juga dengan berbagai cara, salah satunya dengan merekam jejak pengetikan pada suatu media. Kerugian akan hal ini sangat berdampak pada keamanan data. Perekaman jejak pengetikan ini menggunakan suatu perangkat pembantu dalam proses penyadapannya. Pada kenyataannya masih

sedikit solusi yang tepat untuk mendeteksi maupun untuk mencegah aktivitas penyadapan ini. Dalam proses penyadapan jejak pengetikan ini, seluruh aktivitas pengetikan akan terekam secara keseluruhan apa saja kegiatan yang dilakukan. Tindakan ini merupakan suatu kejahatan komputer.

Tujuan dari penulisan ini adalah untuk memahami bagaimana cara kerja *keylogger* agar dapat dilakukan cara pencegahan dengan melakukan berbagai macam solusi dan juga untuk mempertahankan sistem keamanan data serta mengetahui software pendukung dan anti *keylogger*.

Menurut Hamzah (2004) dalam bukunya yang berjudul Aspek-aspek Pidana di Bidang Komputer, mengemukakan bahwa pengertian kejahatan komputer adalah segala aktifitas tidak sah yang memanfaatkan komputer untuk tidak pidana . Sekecil apapun dampak atau akibat yang ditimbulkan dari penggunaan komputer secara tidak sah atau ilegal merupakan suatu kejahatan. Dan dalam arti sempit kejahatan komputer adalah suatu perbuatan melawan hukum yang dilakukan dengan teknologi komputer yang canggih. Faktor- faktor Penyebab Kejahatan Komputer Beberapa faktor yang menyebabkan kejahatan komputer makin marak dilakukan antara lain adalah:

1. Akses internet yang tidak terbatas.
2. Kelalaian pengguna komputer. Hal ini merupakan salah satu penyebab utama kejahatan komputer.
3. Mudah dilakukan dengan resiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Walaupun kejahatan komputer mudah untuk dilakukan tetapi akan sangat sulit untuk melacaknya, sehingga ini mendorong para pelaku kejahatan untuk terus melakukan hal ini.
4. Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar, dan fanatik akan teknologi komputer. Pengetahuan pelaku kejahatan computer tentang cara kerja sebuah komputer jauh diatas operator komputer.
5. Sistem keamanan jaringan yang lemah.
6. Kurangnya perhatian masyarakat. Masyarakat dan penegak hukum saat ini masih memberi perhatian yang sangat besar terhadap kejahatan konvesional. Pada kenyataannya para pelaku kejahatan komputer masih terus melakukan aksi kejahatannya.
7. Belum adanya undang-undang atau hukum yang mengatur tentang kejahatan komputer.

Cybercrime dapat didefinisikan sebagai perbuatan melanggar hukum yang dilakukan dengan menggunakan fasilitas internet dengan menggunakan teknologi komputer dan telekomunikasi. Ada beberapa pendapat lain mengenai definisi dari istilah *Cybercrime* seperti dibawah ini : " The U.S Department of justice " memberikan pengertian kejahatan komputer atau *Cybercrime* sebagai berikut :

" *…any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution* ", (riyanarto dan irsyat, 2009).

Macam-macam Bentuk Kejahatan Komputer.

1. Illegal Access / Akses Tanpa Ijin ke Sistem Komputer Dengan sengaja dan tanpa hak melakukan akses secara tidak sah terhadap seluruh atau sebagian sistem komputer, dengan maksud untuk mendapatkan data komputer atau maksud-maksud tidak baik lainnya, atau berkaitan dengan sistem komputer yang dihubungkan dengan sistem komputer lain. Hacking merupakan salah satu dari jenis kejahatan ini yang sangat sering terjadi.
2. Illegal Contents / Konten Tidak Sah Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.
3. Data Forgery / Pemalsuan Data Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi salah ketik yang pada akhirnya akan menguntungkan pelaku.
4. Spionase Cyber / Mata-mata Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*.

Jurnal Teknovasi
Volume 03, Nomor 1, 2016, 8-15
ISSN : 2355-701X

5. Data *Theft* / Mencuri Data Kegiatan memperoleh data komputer secara tidak sah, baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain. Identity theft merupakan salah satu dari jenis kejahatan ini yang sering diikuti dengan kejahatan penipuan (*fraud*). Kejahatan ini juga sering diikuti dengan kejahatan data leakage.
6. *Misuse of devices* / Menyalahgunakan Peralatan Komputer Dengan sengaja dan tanpa hak, memproduksi, menjual, berusaha memperoleh untuk digunakan, diimpor, diedarkan atau cara lain untuk kepentingan itu, peralatan, termasuk program komputer, password komputer, kode akses, atau data semacam itu, sehingga seluruh atau sebagian sistem komputer dapat diakses dengan tujuan digunakan untuk melakukan akses tidak sah, intersepsi tidak sah, mengganggu data atau sistem komputer, atau melakukan perbuatan-perbuatan melawan hukum lain. Contoh kejahatan komputer : Pemalsuan kartu kredit, perjudian melalui komputer, pelanggan terhadap hak cipta, dll.

Keamanan Komputer

Menurut Howard (1997) dalam bukunya "*An Analysis of Security Incidents on The Internet*" menyatakan bahwa keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. Keamanan dalam sistem komputer sangat berpengaruh terhadap beberapa faktor di bawah ini diantaranya adalah :

1. Social engineering
2. Security hole pada sistem operasi dan servis
3. Keamanan fisik
4. Serangan pada jaringan
5. DOS attack
6. Serangan via aplikasi berbasis web
7. Trojan, backdoor, rootkit, *keylogger*
8. Virus, worm
9. Anatomy of A Hack

Menurut wicak dalam bukunya "mengamankan komputer dari *Spywere*:2007" Keamanan dari data dan media serta teknik komunikasi (*Communication security*). Tipe keamanan jenis ini banyak menggunakan kelemahan yang ada pada perangkat lunak, baik perangkat lunak aplikasi ataupun perangkat lunak yang diugunakan dalammengelola sebuah database.

Aspek-aspek Keamanan Komputer. Keamanan komputer meliputi delapan aspek, antara lain:

a. *Authentication*, penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi. Dengan kata lain, informasi itu benar- benar datang dari orang yang dikehendaki.
b. *Integrity*, keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi orang yang tidak berhak.
c. *Non-repudiation*, merupakan hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
d. *Authority*, informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya.
e. *Confidentiality*, merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan ke pihak lain.
f. *Privacy*, lebih ke arah data-data yang bersifat pribadi.
g. *Availability*, aspek availabilitas berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.
h. *Access Control*, aspek ini berhubungan dengan cara pengaturan akses ke informasi. Hal ini biasanya berhubungan dengan masalah otentikasi dan privasi. Kontrol akses seringkali dilakukan dengan menggunakan kombinasi *user id* dan *password* ataupun dengan mekanisme lain.

Jurnal Teknovasi
Volume 03, Nomor 1, 2016, 8-15
ISSN : 2355-701X

Model penyerangan keamanan menurut Stallings (1995), terdiri dari :

a) *Interruption*: Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan *(Availability*) dari sistem. Contoh serangan adalah "*denial of service attack*".
b) *Interception*: Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan *(wiretapping*).
c) *Modification*: Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari *web site* dengan pesan-pesan yang merugikan pemilik *web site*.
d) *Fabrication*: Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti *e-mail* palsu ke dalam jaringan komputer.

Keylogger

Keylogger atau Perekam ketikan merupakan sebuah perangkat baik perangkat keras atau perangkat lunak yang digunakan untuk memantau penekanan tombol papan ketik. Sebuah perekam ketikan biasanya akan menyimpan hasil pemantauan penekanan tombol papan ketik tersebut ke dalam sebuah berkas cecatat (log file). Beberapa perekam ketikan tertentu bahkan dapat mengirimkan hasil rekamannya ke surat elektronik tertentu secara berkala. *Keylogger* dapat digunakan untuk kepentingan yang baik atau bahkan bisa digunakan untuk kepentingan yang jahat. Kepentingan yang baik antara lain untuk memantau produktivitas karyawan, untuk penegakan hukum dan pencarian bukti kejahatan. Kepentingan yang buruk antara lain pencurian data dan password.

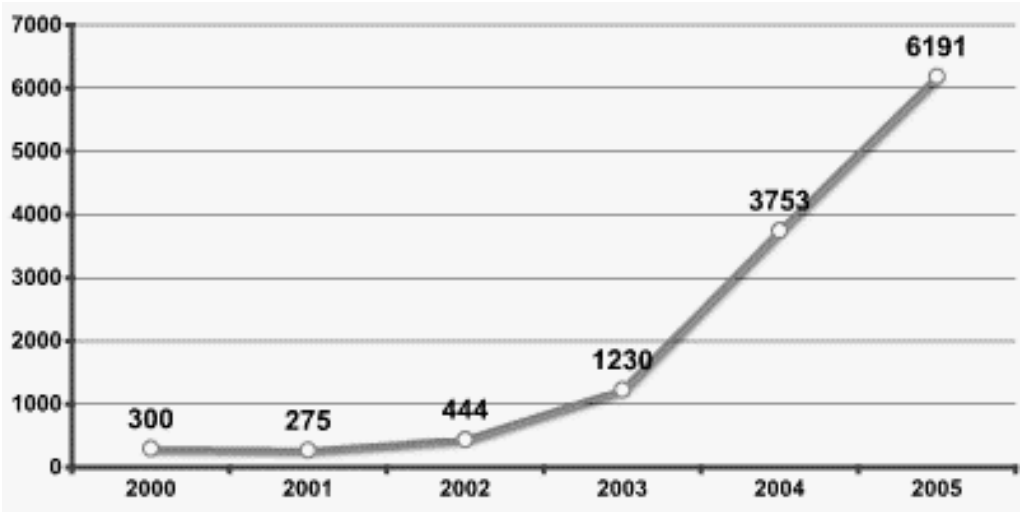
Keylogger yang berupa hardware besarnya seukuran baterai ukuran AA. *Keylogger* jenis ini dipasangkan pada ujung keyboard, sehingga mencegat data yang dialirkan dari keyboard ke CPU. Sementara itu, *keylogger* dalam bentuk perangkat lunak terpasang di dalam komputer dan bekerja secara tersembunyi. Cara sederhana untuk menghindari dampak adanya *keylogger* pada sistem operasi Microsoft Windows adalah dengan menggunakan fitur *on-screen keyboard*.

Fitur utama dan umum pada *Keylogger*

Meskipun *Keylogger* biasanya merupakan aplikasi yang padat, program-program ini menawarkan beragam fitur unik yang menjadikannya sebagai *tool* yang penting dan optimal bagi siapa saja yang ingin melacak kegiatan-kegiatan komputer. Kebanyakan *keylogger* mampu untuk melakukan hal-hal berikut ini:

1. Merekam semua situs yang dikunjungi ke dalam sebuah file pencatat (log file) termasuk URL-URL, potret-potret layar, judul-judul laman web, dan lain-lain.
2. Menyimpan salinan email-email yang dikirim dan diterima sehingga Anda dapat melihatnya secara saksama.
3. Menyimpan salinan obrolan-obrolan Pesan Instan sehingga Anda dapat memantaunya di lain kesempatan sesuai keinginan Anda.
4. Melacak semua penekanan tombol di papan ketik di setiap aplikasi yang dijalankan di komputer yang diberikan (perlu diingat bahwa pencatatan ketikan ini termasuk pengetikan kata-sandi (password), data registrasi dan semacamnya).
5. Memotret layar pada selang waktu yang telah ditetapkan sebelumnya.
6. Mengirimi Anda email atau mengingatkan Anda dengan cara lain seperti ketika komputer menjadi online, atau digunakan untuk suatu kegiatan tertentu. Kebanyakan *keylogger* juga dapat mengirimi Anda file catatan melalui email ke alamat email yang telah ditentukan sebelumnya.
7. Beroperasi tanpa terdeteksi dan tak terhindari. Para pengguna tidak akan bisa mematikan *Keylogger-keylogger* tanpa kata-sandi administrator.

Dampak kerugian akibat *keylogger* dapat dilihat pada gambar di bawah ini.



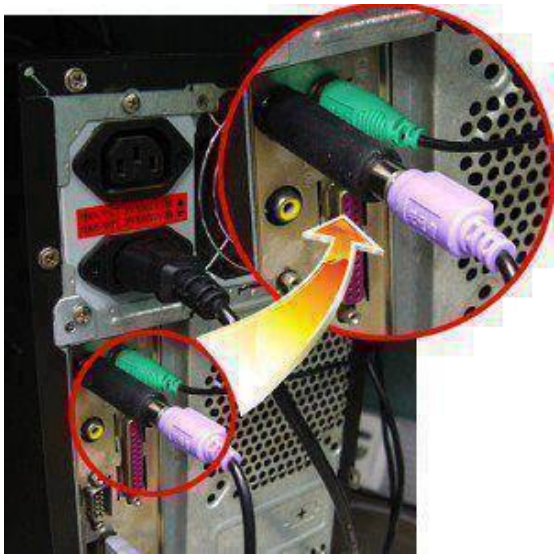
Sumber: iDefense, a VeriSign Company (*www.securelist.com*)

Gambar 1. Grafik Kerugiaan dari kegiatan *keylogger*.

METODE PENELITIAN

Aspek keamanan komputer adalah bentuk pertimbangan yang menyatakan sebuah komputer bisa dinyatakan aman. Begitu pentingnya aspek keamanan dalam teknologi informasi sehingga beberapa perusahaan pengembang software menjadikan keamanan sebagai prioritas bisnisnya. Software yang aman menjadi nilai jual tersendiri bagi perusahaan pengembang dan menjadi pertimbangan utama bagi perusahaan penggguna yang mengutamakan stabilitas sistem dan kerahasiaan datanya. Dalam penelitian ini membahas 2 aspek pengamanan informasi dari serangan keylogger antar lain :

1. Melihat fisik komputer, biasanya komputer yang di pasang semacam alat yang mencurigakan seperti pada gambar 2.



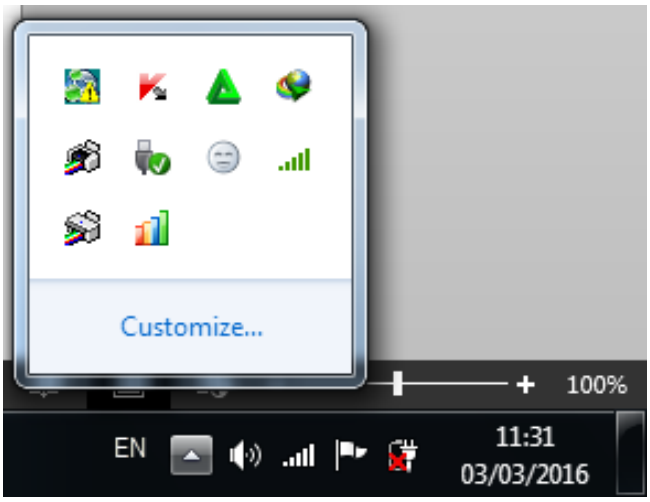
Sumber : Data Diolah

Gambar 2. Perangkat fisik Keylogger Pada Komputer.

Jurnal Teknovasi
Volume 03, Nomor 1, 2016, 8-15
ISSN : 2355-701X

Pada gambar 2 terlihat pada Port Keyboard terpasang suatu alat yang menghubungkan keyboard dengan Port pada Motherboard. Seharusnya pada kondisi normal keyboard secara langsung terhubung dengan port pada motherboard tanpa ada alat tambahan. Pada kondisi ini keylogger dipasang secara fisik, dan dapat terlihat dengan jelas bahwasannya ada yang ingin mengetahui informasi komputer tersebut.

2. Melihat non fisik, melihat di sistem *Tray* atau sistem *startUp*, apakah ada program yang mencurigakan yang telah diinstal ke dalam komputer tersebut. Seperti gambar 3.



Sumber : Data Diolah

Gambar 3. Sistem Tray atau Start Up

User bisa melihat sebelum melakukan pengolahan informasi dengan media keyboard, terlebih dahulu melihat daftar aplikasi yang terinstal di dalam sistem tray tersebut.

HASIL DAN PEMBAHASAN

Aspek Pencegahan

Keylogger memiliki 2 (dua) bentuk yaitu Hardware dan Software dengan karakterisitik yang sangat berbeda membuat teknik mendeteksi dan pencegahannya pun juga berbeda. Dahulu sempat terdengar untuk menghindari Software *keylogger* dapat menggunakan *Virtual Keyboard* yang dapat di akses melalui menu *Accessories>Accessibility>On-Screen Keyboard*. Penggunaan Virtual Keyboard ini tidak berguna untuk menghadapi Software *Keylogger* karena Virtual Keyboard ini tetap mengirimkan text yang akan ditampilkan pada program dan text ini tetap akan direkam oleh Software *Keylogger*, bahkan *Keylogger* juga dapat meng-capture tampilan text tersebut. Untuk mencegah perekaman yang dilakukan *keylogger*, ada beberapa hal yang harus dilakukan antara lain:

1. Virtual keyboard sangat ampuh dan berguna untuk mencegah hardware *keylogger*, karena text yang diketikkan tidak akan melalui keyboard asli dan juga tidak melalui kabel dan port keyboard yang telah dipasangi Hardware *Keylogger*.
2. Menggunakan Program anti-spyware atau antivirus yang tentunya selalu ter-update.
3. Mencari direktori yang disembunyikan, karena biasanya pemasang *Keylogger* membuat directory yang tersembunyi agar tidak diketahui oleh pemakai namun langkah ini juga bisa membantu kita untuk mengetahui keberadaan suatu program yang tidak dikehendaki. Untuk melakukan langkah ini, jalankan perintah "dir /ah /s" pada Command Prompt yang akan menampilkan semua file dan direktori yang disembunyikan

Jurnal Teknovasi
Volume 03, Nomor 1, 2016, 8-15
ISSN : 2355-701X

4. Lakukan pengecekan proses aplikasi yang aktif pada Task Manager, kemudian lihat proses aplikasi yang aktif, bila terdapat *keylogger*, sebaiknya dihapus saja dengan mengklik End Proccess.
5. Cek perangkat komputer Anda. Bila ada benda aneh di ujung kabel keyboard, kemungkinan itu adalah *keylogger* jenis hardware.

Dari banyaknya resiko yang akan dihadapi oleh suatu sistem informasi, semuanya itu merupakan hal yang sangat penting dan tidak dapat dianggap remeh. Salah satunya terhadap *file* data, yang merupakan suatu aset yang banyak digunakan dan selalu ada dalam suatu sistem informasi. Metode untuk mengamankan *file* dapat dilakukan dengan 3 (tiga) cara, yaitu:

1. *Attribut Keying*, yaitu suatu penguncian terhadap attribut sebuah *file* data. Setiap *file* data dalam sistem informasi (komputer) selalu diikuti oleh attribut *file*, yang berfungsi untuk mengamankan *file* agar tidak dapat diserang oleh orang lain. Attribut itu terdiri atas :
   a. R (*read*), yaitu penguncian atrribut sehingga pemakai hanya dapat melakukan pembacaan saja terhadap terhadap isi *file*.
   b. W (*write*), yaitu penguncian attribut sehingga pemakai dapat melakukan penulisan (simpan) terhadap isi *file*.
   c. X atau A (*access*), yaitu penguncian atrribut sehingga pemakai dapat melakukan pengaksesan (eksekusi) *file*.

   Perintah penguncian ini dapat dilakukan dengan menggunkan perintah eksternal dari Sistem Operasi (*Operating System*) seperti :
   a. CLI (*Command Line Interface*) dalam *Disk Operating System* (DOS) dengan menggunkan perintah ATTRIB.
   b. GUI (*Grafics User Interface*) dalam sistem operasi *Windows*.
   c. *Compress Keying*, yaitu suatu penguncian terhadap hasil pemadatan *file* data. Setiap *file* data dapat dirobah kedalam bentuk yang lebih padat dengan menggunakan aplikasi kompres, seperti RAR, ZIP dan lain-lain. Hasil dari kompres dapat di kunci dengan menambahkan Password (kata kunci) pembuka apabila *file* tersebut di decompress atau dikembalikan kedalam bentuk semula (*extract*). Prinsip kerja dari kompres adalah mencari character atau byte yang sering atau banyak berada dalam sebuah *file* data. Karakter tersebut akan dirobah kedalam kumpulan *bit* yang lebih sedikit (kurang dari 8 *bit*).
2. *Encription* (Enkripsi), yaitu merupakan suatu teknik merubah isi *file* data dengan bentuk rahasia yang tidak dimengerti oleh orang lain. Jenis-jenis proteksi data enkripsi terdiri atas :
   a) Teknik Substitusi (*Substitution Technique*), yaitu teknik yang melakukan proteksi data dengan cara menggantikan setiap elemen data atau karakter dengan karakter lain.
   b) Teknik Blok (*Blocking Technique*), yaitu teknik proteksi data dengan cara mengelompokan beberapa karakter ke dalam blok-blok yang berisi beberapa karakter.
   c) Teknik Permutasi (*Permutation Technique*), yaitu teknik proteksi data dengan cara menukarkan letak karakter-karakter yang ada.
   d) Teknik Ekspansi (*Expansion Technique*), yaitu teknik proteksi data dengan cara menambahkan suatu karakter kedalam data.
   e) Teknik Pemadatan (*Compaction Technique*), yaitu teknik proteksi data dengan cara menghilangkan sejumlah karakter dalam data

KESIMPULAN

Inti dari keamanan komputer adalah melindungi komputer dan jaringannya dengan tujuan mengamankan informasi yang berada di dalamnya. Mencegah terjadinya suatu serangan terhadap sistem. Dengan demikian kita perlu memperhatikan hal-hal yang dapat merugikan dalam proses pengamanan data. Proses perekaman jejak ketikan adalah suatu hal yang dapat terjadi dimana saja tanpa kita sadari, hal yang paling penting untuk mengamankan data selalu mengawasi penggunaan suatu media penyimpan data, *network* dan selelu menggunakan anti virus yang terupdate.

Jurnal Teknovasi
Volume 03, Nomor 1, 2016, 8-15
ISSN : 2355-701X

SARAN

Begitu banyak teknik dalam mengamankan data dan informasi yang tersimpan pada sebuah media penyimpanan di komputer. Di antaranya adalah Dengan selulu mengawasi software-software yang terinstal dalam komputer tersebut. Melihat struktur hardware computer tidak ada yang mencurigakan. Teknik tersebut patut diterapkan apabila kita tidak menginginkan terjadinya resiko kehilangan data penting. Namun, pemilihan teknik tersebut perlu dilakukan dengan cermat.

DAFTAR PUSTAKA

Andi, hamzah., 2004, *Aspek-aspek Pidana di Bidang Komputer*, Jakarta : Andi Offset.

Applegate, McFarlan, McKenney, 1999, Corporate Information Systems Management: Text and Cases, 5th Edition, Singapore: Mc Graw Hill.

Ibisa. 2011. *Keamanan Sistem Informasi*. Yogyakarta: CV Andi Offset

John D. Horwart, *An Anlysis of Security Incident On The Internet 1989-1995*, PhD thesis, Engineering and Public Policy, Carnegie Mellon University.

Riyanarto, sarno dan irsyat, iffano, itspress 2009, *The U.S Department of justice, www.usdoj.gov/criminal/Cybercrimes*.

Rahardjo, Budi. 1999. *Keamanan Sistem Informasi Berbasis Internet*. Bandung: PT. Insan Komuikasi.

Wicak, hidayat, 2007,*Mengamankan Komputer Dari Spyware*.(Jakarta : Media Kita).

W. Stallings, 1995,*"Network and Internetwork Security*," Prentice Hall.