Pengantar Teknologi Informasi

Keamanan Komputer

Rahma Djati Kusuma, S.SI., M.T.
Suci Sri Utami S., S.T., M.Kom.

Keamanan

- Kata “AMAN” dapat didefinisikan sebagaimana dari serangan atau kegagalan.
- Membentuk kata ’Keamanan’ dapat diartikan sebagai keadaan aman dan ketentraman
- Kata Security mengandung berbagai arti, yaitu: Sesuatu yang bernilai, berharga, jaminan dan kepastian.
- Keamanan menjadi sebuah kebutuhan pokok.
- Baru menjadi perhatian besar ketika ancaman keamanan dirasakan oleh pemilik/orang yang bersangkutan.
- Akibatnya, perencanaan kebutuhan keamanan menjadi sesuatu yang khusus

Definisi, Fungsi dan Ancaman

Keamanan Komputer merupakan kebutuhan mendesak bagi organisasi atau perusahaan yang menyelenggarakan pengolahan data elektronik (PDE) secara sistematis dan profesional.

Definisi

Menurut **John D. Howard** 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.

Menurut **Gollmann** pada tahun 1999 dalam bukunya "Computer Security" menyatakan bahwa :

Keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer.

Menurut **Watne, Donald A and Turney, Peter BB**. *Auditing EDP*, System Security yang artinya :

Perlindungan terhadap fasilitas komputer, kesalahan program dan data dari kerusakan oleh resiko lingkungan, kesalahan perangkat lunak, kesalahan manusia atau penyalahgunaan komputer.

Fungsi

- Lingkup kerja keamanan komputer mencakup aspek yang sangat luas, seluas studi komputer yang mencakup semua aspek kerja dalam sebuah organisasi / perusahaan.

- Keamanan Komputer mencakup atas Keamanan Fisik, Keamanan H/w, Keamanan S/w, Keamanan Jaringan, Keamanan Personel, Hukum dan Etika.

Beberapa Fungsi Penting

- Mendukung misi organisasi atau perusahaan secara keseluruhan.
- Keamanan komputer adalah bagian integral perhatian manajemen terhadap keseluruhan sistem keamanan.
- Keamanan komputer harus efektif dari segi biaya.
- Pertanggungjawaban dan kelayakan keamanan komputer harus dibuat dengan tegas dan pemilik sistem memiliki tanggung jawab terhadap keamanan komputer dari organisasi yang dimilikinya.
- Keamanan komputer membutuhkan pendekatan komprehensif dan terpadu.
- Keamanan komputer harus ditinjau secara periodik.
- Keamanan komputer dibatasi oleh faktor masyarakat/sosial.

Aspek keamanan komputer

Privacy / Confidentiality

- Definisi : menjaga informasi dari orang yang tidak berhak mengakses.
- Privacy : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai *(user*) tidak boleh dibaca oleh administrator.
- Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.
- Contoh : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.
- Bentuk Serangan : usaha penyadapan (dengan program *sniffe*r).
- Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

Aspek keamanan komputer

Integrity

- Definisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.
- Contoh : e-mail di *intercep*t di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
- Bentuk serangan : Adanya virus, *trojan hors*e, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

Aspek keamanan komputer

Authentication

- Definisi : metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
- Dukungan :
  - Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking (untuk menjaga*"intellectual propert*y", yaitu dengan menandai dokumen atau hasil karya dengan "tanda tangan" pembuat) dan digital signature.
  - Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

Aspek keamanan komputer

Availability

- Definisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.
- Contoh hambatan :
  - *"denial of service attac*k" (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *dow*n, *han*g, *cras*h.
  - *mailbom*b, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

Aspek keamanan komputer

Access Control

- Definisi : cara pengaturan akses kepada informasi. berhubungan dengan masalah
- authentication dan juga privacy
- Metode : menggunakan kombinasi user id/password atau dengan
- menggunakan mekanisme lain.

Non - repudiation

- Definisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

Mengapa keamanan komputer dibutuhkan

"information-based society", menyebabkan nilai informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi.

Infrastruktur Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan (*Security Hole)*

Kejahatan komputer meningkat karena

- Aplikasi bisnis berbasis TI dan jaringan komputer meningkat .
- Desentralisasi server.
- Transisi dari single vendor ke multi vendor.
- Meningkatnya kemampuan pemakai (user).
- Kesulitan penegak hukum dan belum adanya ketentuan yang pasti.
- Semakin kompleksnya system yang digunakan, semakin besarnya source code program yang digunakan.
- Berhubungan dengan internet.

Klasifikasi Kejahatan Komputer

- Keamanan yang bersifat fisik
  - Wiretapping, atau hal-hal yang berhubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.
  - *Denial of servic*e, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan).
  - *Syn Flood Attac*k, dimana sistem *(hos*t) yang dituju dibanjiri oleh permintaan sehingga dia menjadi terlalu sibuk dan bahkan dapat berakibat macetnya sistem *(han*g).
- Keamanan yang berhubungan dengan orang (personel)
  - Identifikasi user
  - Profil resiko dari orang yang mempunyai akses
- Keamanan dari data dan media serta teknik komunikasi
- Keamanan dalam operasi : Adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan *(post attack recover*y).

Karakteristik Penyusup

- ***The Curious*** (Si Ingin Tahu) - tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang anda miliki.
- ***The Malicious*** (Si Perusak) - tipe penyusup ini berusaha untuk merusak sistem anda, atau merubah web page anda, atau sebaliknya membuat waktu dan uang anda kembali pulih.
- ***The High-Profile Intruder*** (Si Profil Tinggi) - tipe penyusup ini berusaha menggunakan sistem anda untuk memperoleh popularitas dan ketenaran. Dia mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya.
- ***The Competition*** (Si Pesaing) - tipe penyusup ini tertarik pada data yang anda miliki dalam sistem anda. Ia mungkin seseorang yang beranggapan bahwa anda memiliki sesuatu yang dapat menguntungkannya secara keuangan atau sebaliknya.

Istilah bagi penyusup

- ***Mundane*** ; tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
- ***lamer (script kiddies)*** ; mencoba script2 yang pernah dibuat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
- ***wannabe*** ; paham sedikit metode hacking, dan sudah mulai berhasil menerobos sehingga berfalsafah ; HACK IS MY RELIGION.
- ***larva (newbie)*** ; hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.
- ***hacker*** ; aktivitas hacking sebagai profesi.
- ***wizard*** ; hacker yang membuat komunitas pembelajaran di antara mereka.
- ***guru ; master of the master hacker***, lebih mengarah ke penciptaan tools-tools yang powerfull yang salah satunya dapat menunjang aktivitas hacking, namun lebih jadi tools pemrograman system yang umum.

Model Serangan Keamanan

- ***Interruption*:** Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan *(availability*) dari sistem. Contoh serangan adalah "denial of service attack".
- ***Interception*:** Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan*(wiretapping*).
- ***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 website dengan pesan-pesan yang merugikan pemilik website.
- ***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.

Perbedaan Hacker dan Cracker

Secara Definisi :

- Hacker merupakan orang yang melakukan proses hacking atau peretasan terhadap suatu sistem, sehingga orang atau kelompok hacker ini bisa masuk ke dalam sebuah sistem. Ketika seseorang atau kelompok sudah masuk ke dalam sistem, baik melalui wormhole ataupun metode lainya, maka proses hacking sudah terlaksana. Proses yang dilakukan oleh hacker biasanya hanya sampai pada masuk ke dalam jaringan atau sistem tertentu saja. Pada dasarnya hacker bertujuan untuk menyusup dan masuk ke dalam suatu sistem.
- Sedangkan cracker, memiliki proses yang kurang lebih sama seperti hacker. Cracker pada awalnya akan masuk dan menyusup ke dalam suatu sistem ataupun jaringan. Ketika cracker sudah berhasil masuk dan menyusup ke dalam suatu sistem atau jaringan, maka kemudian cracker tersebut akan mengutak atik jaringan tersebut secara illegal tentunya, seperti melakukan penghapusan data, mengcopy data, mengubah konten, dan sebagainya, dengan intensi untuk merugikan pihak – pihak tertentu, dan mengambil keuntungan bagi diri atau kelompoknya sendiri.

Perbedaan Hacker dan Cracker

- Hacker merupakan seseorang yang melakukan penyusupan dan peretasan ke dalam suatu sistem saja, sedangkan cracker masuk dan menyusup ke dalam sistem atau jaringan untuk tujuan yang destruktif.
- Hacker banyak memberikan masukan kepada developer mengenai kelemahan dari sistem yang dikembangkan, sedangkan cracker tidak.
- Hacker pada dasarnya merupakan pekerjaan yang “baik” karena membantu mencari kelemahan sistem, sedangkan cracker lebih sering dikonotasikan dengan hacker yang jahat.
- Hacker melakukan tugasnya untuk membantu developer dalam mengembangkan sistem, terutama dari segi keamanan sistem, sedangkan cracker bekerja untuk motif – motif tertentu, seperti pembalasan dendam, pembajakan, serta pengambilan keuntungan pribadi dari hasil penyusupan ke dalam sistem.

Pada dasarnya, hacker dan juga cracker memiliki teknik, serta kemampuan yang tidak jauh berbeda, karena sama – sama mampu untuk menyusup dan masuk ke dalam jaringan atau sistem tanpa dideteksi. Yang membedakan hanyalah motif yang dilakukan dalam proses penyusupan.

Baik hacker dan juga cracker bisa saling bekerja sama, terutama untuk kepentingan khusus, seperti kepentingan penyidikan dalam misi forensic, mencari buronan dan daftar pencarian orang.

Memahami Hacker Bekerja

- Hacker akan masuk ke dalam suatu sistem atau jaringan tertentu, kemudian hacker akan mencari titik kelemahan dari sistem, jaringan ataupun aplikasi yang akan disusupi. Ketika sudah menemukan celah atau wormhole tersebut, maka hacker kemudian beraksi, dan mulai masuk dan menyusup ke dalam sistem atau program tersebut.

Cont ... Memahami Hacker Bekerja

- Melalui cara tersebut, maka seorang hacker bisa memantau, melihat, dan mengidentifikasi situasi yang ada di dalam sistem atau jaringan, atau program tertentu, untuk kepentingan tertentu pula. Biasanya, hacker bekerja untuk tujuan yang sudah dipersiapkan sebelumnya, seperti :
  - Melakukan pengembangan terhadap sistem, jaringan ataupun program komputer
  - Memberikan masukan bagi developer untuk memperbaiki sistem yang dibuat
  - Mencegah kejahatan cracking yang dilakukan oleh cracker
  - Mencegah agar data dan informasi di dalam sistem atau jaringan komputer tidak mudah dicuri
- Itulah beberapa tujuan dari proses peretasan atau hacking yang dilakukan oleh hacker secara umum. Akan tetapi, saat ini hacker sudah digeneralisasikan sama seperti cracker, yang sebenarnya berbeda

Cont ... Memahami Hacker Bekerja

Proses dari cara kerja cracker pada dasarnya mirip seperti pada proses hacking. Akan tetapi, perbedaannya terletak pada proses selanjutnya. Apabila pada proses hacking, tidak melakukan proses serta kegiatan yang merusak, maka cracker akan melakukan kegiatan dan proses yang merusak suatu sistem.

Beberapa tujuan yang ingin dicapai oleh para cracker dalam melakukan proses cracking terhadap suatu sistem, yaitu :

- Menunjukkan eksistensi mereka sebagai penghancur dan perusak suatu sistem dan jaringan
- Membalas dendam terhadap instansi tertentu (cyber crime)
- Mengambil keuntungan dari informasi dan data rahasia dari sebuah sistem
- Membajak dan mengcopy secara ilegal konten – konten yang memiliki lisensi serta hak atas kekayaan intelektual, terutama lisensi yang berbayar, sehingga dapat diedarkan secara ilegal dengan gratis tanpa harus membayar
- Menghapus data – data dan informasi penting pada suatu sistem, misalnya data Daftar Pencarian Orang, Daftar blacklist, dan daftar lainnya, yang mungkin dapat merugikan pihak tertentu apabila terdaftar
  Menyebarkan keresahan pada masyarakat, terutama pengguna sistem

Cont ... Memahami Hacker Bekerja

Salah satu kegiatan cracker yang paling banyak meresahkan banyak orang adalah kegiatan cracking pada situs perbankan. Banyak cracker yang berhasil menyusup masuk ke dalam sistem perbankan, ataupun sistem yang berafiliasi dengan perbankan, sehingga tiap kali ada user yang melakukan transaksi menggunakan sistem tersebut, cracker akan dengan mudah memperoleh data, seperti nomor kartu kredit, nama, alamat, dan informasi lainnya yang sifatnya personal dan rahasia.

Meskipun kebanyakan proses cracking memiliki banyak tujuan yang mengarah pada hal negative, namun demikian pada dasarnya kegiatan cracking merupakan salah satu kegiatan yang secara forensic sangat bermanfaat. Polisi dan penegak hukum lainnya, seperti inteligen sangat membutuhkan kemampuan cracking ini untuk membantu mereka dalam menuntaskan misi – misi tertentu, seperti mengejar buronan dan menangkap penjahat.

Tujuan Keamanan Komputer

Untuk menyakinkan

Ketersediaan (*Availability*)
Keutuhan (*Integrity*)
Kerahasiaan (*Confidentiality)*
Akuntabilitas (*Accountability*)
Jaminan/Kepastian (*Assurance*)

Ketersediaan (Availability)

- Ketersediaan adalah persyaratan untuk menjamin sistem bekerja dengan cepat dan pelayanan tidak ditolak bagi pemakai yang berhak.
- Tujuan ini melindungi ancaman dari:
  - Yang bermaksud / Kecelakaan melakukan penghapusan data / melakukan hal lain yang mengakibatkan penolakan pelayanan atau data
  - Berusaha memakai sistem atau data untuk tujuan yang tidak diotorisasi.

Keutuhan (Integrity)

- Keutuhan data (data tidak berubah karena akses tidak sah ketika penyimpanan, proses atau ketika pengangkutan/pemindahan)
- Keutuhan sistem (kualitas sistem ketika melakukan fungsi yang yang diinginkan dalam keadaan tidak terhalang dan bebas dari manipulasi yang tidak sah).
- Keutuhan merupakan yang penting dalam tujuan keamanan setelah ketersediaan.

Kerahasiaan (Confidentiality)

Kerahasiaan adalah persyaratan yang menunjukkan bahwa informasi tidak dibuka oleh orang yang tidak berhak / tidak diotorisasikan

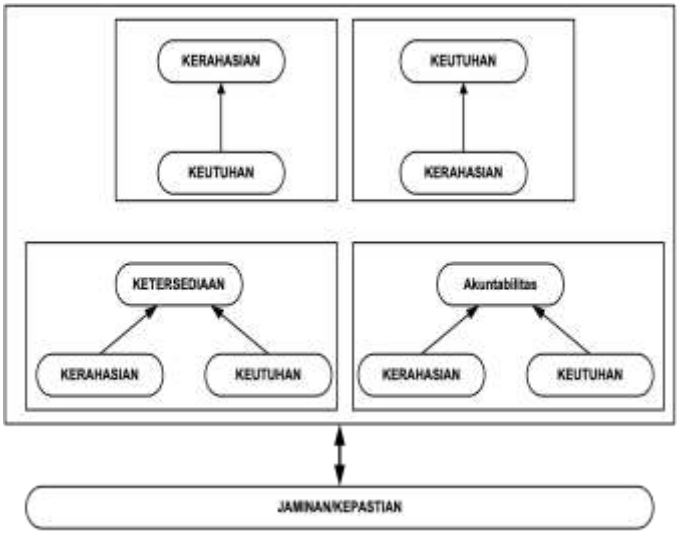
Akuntabilitas (Accountability)

- Ditujukan untuk level perorangan.
- Akuntabilitas adalah persyaratan aksi entitas yang bisa dilacak secara unik terhadap entitas itu.
- Menjadi persyaratan kebijakan organisasi dan secara langsung mendukung pencegahan penolakan, isolasi kesalahan, pendeteksian penyusupan, recovery dan tindakan hukum.

Jaminan/Kepastian (Assurance)

- Untuk memantapkan empat tujuan yang dicapai.
- Merupakan dasar untuk meyakinkan bahwa ukuran keamanan secara teknik dan operasional bekerja dengan baik dalam melindungi sistem dan pemrosesan informasi.
- Jaminan merupakan sesuatu yang penting karena tanpa hal ini tujuan tidak akan dicapai.

Keterkaitan Tujuan Keamanan Komputer



Manajemen Keamanan Komputer

1. Keamanan komputer yang baik serta ancaman yang bisa diperkirakan menuntut pengelolaan sistem keamanan dengan cara-cara yang tepat dan efektif.
2. Manajemen keamanan mengelola tiga elemen penting.
   a. Sumber Daya Manusia
   b. Teknologi
   c. Operasi

Sumber Daya Manusia

Personil dalam organisasi harus memahami ancaman yang diikuti dengan;

- Pemahaman tentang kebijakan jaminan dan prosedur.
- Penetapan tugas dan tanggungjawab,
- Pelatihan untuk user
- Akuntabilitas individual
- Dll.

Teknologi

- Memberikan jaminan keamanan dan mendeteksi penyusupan.
- Meyakinkan teknologi didapatkan dan diterapkan dengan tepat, organisasi harus menerapkan kebijakan dan proses akuisisi teknologi

Operasi

- Pemeliharaan kebijakan sistem keamanan agar tetap layak dan terbaharui.
- Sertifikasi dan akreditasi perubahan teknologi informasi.
- Mengelola postur jaminan keamanan teknologi informasi.
- Memberikan pelayanan manajemen kunci dan melindungi infrastruktur yang menguntukan.
  Melakukan penilaian sistem keamanan untuk menilai kontinuitas “Kesiagaan Keamanan”.
  Memonitor dan menghadapi ancaman saat ini.
  “Merasakan” Serangan, memberikan peringatan dan merespon dengan benar