PENGANTAR

A. Pendahuluan

Dalam dunia komunikasi data global dan perkembangan teknologi informasi yang senantiasa berubah serta cepatnya perkembangan software, keamanan merupakan suatu isu yang sangat penting, baik itu keamanan fisik, keamanan data maupun keamanan aplikasi.

Perlu kita sadari bahwa untuk mencapai suatu keamanan itu adalah suatu hal yang sangat mustahil, seperti yang ada dalam dunia nyata sekarang ini. Tidak ada satu daerah pun yang betul-betul aman kondisinya, walau penjaga keamanan telah ditempatkan di daerah tersebut, begitu juga dengan keamanan sistem komputer. Namun yang bisa kita lakukan adalah untuk mengurangi gangguan keamanan tersebut.

Tidak ada sistem yang benar-benar aman, tapi kita bisa mengurangi gangguan keamanan tersebut. Dalam keamanan sistem komputer yang perlu kita lakukan adalah untuk mempersulit orang lain untuk mengganggu sistem yang kita pakai, baik itu kita menggunakan komputer yang sifatnya stand alone, jaringan lokal maupun jaringan global. Kita harus memastikan sistem bisa berjalan dengan baik dan kondusif, selain itu program aplikasinya masih bisa dipakai tanpa ada masalah.

B. Definisi Keamanan Komputer

1. Menurut **John D. Howard** dalam bukunya "An Analysis of security incidents on the internet" menyatakan bahwa: Keamanan computer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab.
2. 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 system komputer. Dengan semakin berkembangnya eCommerce dan internet, maka masalah keamanan tidak lagi masalah keamanan data belaka

C. PENGAMANAN SISTEM KOMPUTER

Secara garis besar, pengamanan sistem computer mencakup 4 hal berikut:

Berdasarkan level, metode pengamanan komputer dibedakan berdasarkan level keamanan, dan disusun seperti piramida, yaitu:

1. Keamanan Level 0, merupakan keamanan fisik (Physical Security) atau keamanan tingkat awal. Apabila keamanan fisik sudah terjaga maka keamanan di dalam computer juga akan terjaga.
2. Keamanan Level 1, terdiri dari database security, data security, dan device security. Pertama dari pembuatan database dilihat apakah menggunakan aplikasi yang sudah diakui keamanannya. Selanjutnya adalah memperhatikan data security yaitu pendesainan database, karena pendesain database harus memikirkan kemungkinan keamanan dari database. Terakhir adalah device security yaitu adalah yang dipakai untuk keamanan dari database tersebut.
3. Keamanan Level 2, yaitu keamanan dari segi keamanan jaringan.

Keamanan ini sebagai tindak lanjut dari keamanan level 1.

4. Keamanan Level 3, merupakan information security. Informasi – informasi seperti kata sandi yang dikirimkan kepada teman atau file – file yang penting, karena takut ada orang yang tidak sah mengetahui informasi tersebut.
5. Keamanan Level 4, keamanan ini adalah keseluruhan dari keamanan level 1 sampai level 3. Apabila ada satu dari keamanan itu tidak terpenuhi maka keamanan level 4 juga tidak terpenuhi.

Beberapa hal yang menjadikan kejahatan komputer terus terjadi dan cenderung meningkat adalah sebagai berikut:

1. Meningkatnya pengguna komputer dan internet
2. Banyaknya software yang pada awalnya digunakan untuk melakukan audit sebuah system dengan cara mencari kelemahan dan celah yang mungkin ada disalahgunakan untuk melakukan scanning system orang lain.
3. Banyaknya software-software untuk melakukan probe dan penyusupan yang tersedia di Internet dan bisa di download secara gratis.
4. Meningkatnya kemampuan pengguna komputer dan internet
5. Kurangnya huku yang mengatur kejahatan komputer.
6. Semakin banyaknya perusahaan yang menghubungkan jaringan LAN mereka ke Internet.
7. Meningkatnya aplikasi bisnis yang menggunakan internet.
8. Banyaknya software yang mempunyai kelemahan (bugs).

Ada beberapa hal yang bisa menjawab pertanyaan mengapa kita perlu mengamankan sistem komputer, antara lain:

1. Menghindari resiko penyusupan,

   Kita harus memastikan bahwa system tidak kemasukaan penyusup yang bisa membaca, menulis dan menjalankan program- program yang bisa mengganggu atau menghancurkan system kita.

2. Mengurangi resiko ancaman,

   Hal ini biasa berlaku di institusi dan perusahaan swasta. Ada beberapa macam penyusup yang bisa menyerang system yang kita miliki, antara lain:

   a. Si Ingin Tahu, jenis penyusup ini pada dasarnya tertarik menemukan jenis system yang kita gunakan.
   b. Si Perusak, jenis penyusup ini ingin merusak system yang kita gunakan atau mengubah tampilan layar yang kita buat.
   c. Menyusup untuk popularitas, penyusup ini menggunakan system kita untuk mencapai popularitas dia sendiri, semakin tinggi system keamanan yang kita buat, semakin membuat dia penasaran. Jika dia berhasil masuk kesistem kita maka merupakan sarana bagi dia untuk mempromosikan diri.
   d. Si Pesaing, penyusup ini lebih tertarik pada data yang ada dalam system yang kita miliki, karena dia menganggap kita memiliki sesuatu yang dapat mengguntungkan dia secara finansial atau malah merugikan dia (penyusup).

3. Melindungi system dari kerentanan

   Keretanan akan menjadikan system kita berpotensi untuk memberikan akses yang tidak diizinkan bagi orang lain yang tidak berhak.

4. Melindungi system dari gangguan alam seperti petir dan lain-lainnya.

E. Aspek Keamanan Komputer

Inti dari keamanan komputer adalah melindungi komputer dan jaringannya dengan tujuan mengamankan informasi yang berada di dalamnya. Keamanan komputer sendiri meliputi beberapa aspek, antara lain:

1. ***Privacy*****,**

   Yaitu sesuatu yang bersifat rahasia (provate). Intinya adalah pencegahan agar informasi tersebut tidak diakses oleh orang yang tidak berhak. Contohnya adalah email atau file-file lain yang tidak boleh dibaca orang lain meskipun oleh administrator. Pencegahan yang mungkin dilakukan adalah dengan menggunakan teknologi enksripsi, jadi hanya pemilik informasi yang dapat mengetahui informasi yang sesungguhnya.

2. ***Confidentiality***

   Merupakan data yang diberikan ke pihak lain untuk tujuan khusus tetapi tetap dijaga penyebarannya. Contohnya data yang bersifat pribadi seperti: nama, alamat, no ktp, telpon dan sebagainya. Confidentiality akan terlihat apabila diminta untuk membuktikan kejahatan seseorang, apakah pemegang informasi akan memberikan infomasinya kepada orang yang memintanya atau menjaga

clientnya.

3. ***Integrity***,

   Penekanannya adalah sebuah informasi tidak boleh diubah kecuali oleh pemilik informasi. Terkadang data yang telah terenskripsipun tidak terjaga integritasnya karena ada kemungkinan chpertext dari enkripsi tersebut berubah. Contoh: Penyerangan Integritas ketika sebuah email dikirimkan ditengah jalan disadap dan diganti isinya, sehingga email yang sampai ketujuan sudah berubah.

4. ***Autentication***

   Merupakan validasi terhadap pemilik data. Ini akan dilakukan sewaktu user login dengan menggunakan nama user dan passwordnya, apakah cocok atau tidak, jika cocok diterima dan tidak akan ditolak. Ini biasanya berhubungan dengan hak akses seseorang, apakah dia pengakses yang sah atau tidak.

5. ***Availability***

   Aspek ini berkaitan dengan apakah sebuah data tersedia saat dibutuhkan/diperlukan. Apabila sebuah data atau informasi terlalu ketat pengamanannya akan menyulitkan dalam akses data tersebut. Disamping itu akses yang lambat juga menghambat terpenuhnya aspe availability. Serangan yang sering dilakukan pada aspek ini adalah denial of service (DoS), yaitu penggagalan service sewaktu adanya permintaan data sehingga komputer tidak

bisa melayaninya. Contoh lain dari denial of service ini adalah mengirimkan request yang berlebihan sehingga menyebabkan komputer tidak bisa lagi menampung beban tersebut dan akhirnya komputer down.

Keamanan computer terbagi dalam beberapa level, yaitu sebagai berikut:

1. **Keamanan Level 0,**

   Merupakan keamanan fisik (Physical Security) atau keamanan tingkat awal. Apabila keamanan fisik sudah terjaga maka keamanan di dalam computer juga akan terjaga.

2. **Keamanan Level 1,**

   Terdiri dari database security, data security, dan device security. Pertama dari pembuatan database dilihat apakah menggunakan aplikasi yang sudah diakui keamanannya. Selanjutnya adalah memperhatikan data security yaitu pendesainan database, karena pendesain database harus memikirkan kemungkinan keamanan dari database. Terakhir adalah device security yaitu adalah yang dipakai untuk keamanan dari database tersebut.

3. **Keamanan Level 2,**

   Yaitu keamanan dari segi keamanan jaringan. Keamanan ini sebagai tindak lanjut dari keamanan level 1.

4. **Keamanan Level 3,**

   Merupakan information security. Informasi – informasi seperti kata sandi yang dikirimkan kepada teman atau file – file yang penting, karena takut ada orang yang tidak sah mengetahui informasi tersebut.

5. **Keamanan Level 4,**

   Keamanan ini adalah keseluruhan dari keamanan level 1 sampai level 3. Apabila ada satu dari keamanan itu tidak terpenuhi maka keamanan level 4 juga tidak terpenuhi.

F. ANCAMAN KEAMANAN

Tipe-tipe ancaman yaitu:

1. ***Interruption***

   Merupakan suatu ancaman terhadap *availability.* Informasi atau data yang ada dalam sistem komputer dirusak dan dihapus sehingga jika dibutuhkan maka sudah tidak ada lagi

2. ***Interception***

   Merupakan suatu ancaman terhadap kerahasiaan (*secrecy*). Informasi yang ada di dalam sistem disadap oleh orang yang tidak berhak.

3. ***Modification***

   Merupakan suatu ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu-lintas informasi yang sedang dikirim lalu mengubahnya sesuai keinginan orang itu.

4. ***Fabrication***

   Merupakan suatu ancaman terhadap integritas. Orang yang tidak berhak, berhasil meniru atau memalsukan suatu informasi sehingga orang yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi tersebut.

G. Etika Pengunaan Komputer

Berikut 10 etika dalam menggunakan komputer dari cyber world ethics ("Ten Commandment of Computer Ethics"):

1. Jangan menggunakan komputer untuk menyakiti, berbohong dan merugikan orang lain

   Dalam menggunakan komputer kita tidak boleh merugikan orang lain, misalnya menggunakan komputer untuk membobol sebuah bank, menggunakan komputer untuk membuat virus, menggunakan komputer untuk merusak sistem keamanan seseorang. Selain itu, penggunaan komputer juga bukan untuk menyakiti orang lain, misalnya di fiture facebook maupun twitter `tidak untuk menyakiti atau menghina-hina orang lain

2. Jangan melanggar atau mengganggu hak atau karya komputer orang lain

   Bagi pengguna komputer,diharapkan jangan mengganggu dan menggunakan komputer untuk mengganggu hak-hak orang lain,seperti melakukan pembajakan terhadap karya orang lain,meginstal sebuah program yang tidak legal. Kegiatan ini biasa dilakukan oleh para Cracker dan Hacker yang tidak bertanggung jawab.

3. Jangan memata-matai file-file yang bukan haknya

   Memata-matai,mengintai dan mengambil data milik orang lain yang bukan haknya,sebaiknya hal tersebut tidak dilakukan oleh penggun komputer karna

sangat merugikan orang lain dan kegiatan ini biasa dilakukan oleh para Cracker dan Hacker yang tidak bertanggung jawab.

4. Jangan menggunakan komputer untuk mencuri

   Ini biasa digunakan oleh perampok-perampok dan pencuri yang biasa menggunakan komputer untuk membobol sistem keamanan sebuah bank,dan digunakan oleh para teroris untuk mencari dana dengan membobol identitas pribadi targetnya.

5. Jangan menggunakan komputer untuk memberikan kesaksian palsu

   Menggunakan komputer untuk menyebarkan berita-berita palsu dan berkebalikan dengan fakta,serta mengumbar informasi tentang seseorang yang semuanya berupa kebohongan,dan cenderung kepada pelanggaran hukum yaitu merusak nama baik seseorang.

6. Jangan menduplikasi atau menggunakan software tanpa membayar

   Ini yang biasa dilakukan masyarakat awam yang biasanya dengan tampang tidak berdosa menduplikasi software atau data seseorang tanpa mencantumkan sumber yang dia ambil

7. Jangan menggunakan sumberdaya komputer orang lain tanpa sepengetahuan yang bersangkutan

Apabila kita ingin membuka computer orang lain,kita diharapkan meminta izin dari empunya terlebih dahulu.

8. Jangan mencuri kekayaan intelektual orang lain

   Ini seperti menduplikatkan sebuah software lalu memperbanyaknya dan kemudian di komersialkan

9. Pertimbangkan konsekuensi dari program yang dibuat atau sistem komputer yang dirancang

   Dalam membuat sebuah program hendaknya kita menilai sisi positif dan negatifnya,apabila program yang kita buat lebih banyak dampak buruknya lebih baik kita menghentikan membuat program itu.

10. Selalu mempertimbangkan dan menaruh respek terhadap sesama saat menggunakan computer

    Dalam menggunakan komputer kita harus mempertimbangkan setiap sisi baik buruknya,jangan sampai kita merugikan pihak lain.

Prinsip disain sistem sekuriti yang telah dipublikasikan oleh Jerome Saltzer dan MD. Schroeder, antara lain adalah:

1. Least Privilege

Prinsip ini menyatakan bahwa setiap proses dan user/ pengguna suatu sistem komputer harus beroperasi pada level/ tingkatan terendah yang diperlukan untuk menyelesaikan tugasnya. Dengan kata lain setiap proses dan user hanya memiliki hak akses yang memang benar-benar dibutuhkan. Hak akses harus secara eksplisit diminta, ketimbang secara default diberikan. Tindakan seperti ini dilakukan untuk mengantisipasi kerusakan yang dapat ditimbulkan oleh suatu penyerangan.

2. Economy of Mechanisms

Prinsip ini menyatakan bahwa mekanisme sekuriti dari suatu sistem harus sederhana sehingga dapat diverifikasi dan diimplementasi dengan benar. Mekanisme tersebut harus merupakan bagian yang tak terpisahkan dari desain sistem secara keseluruhan.

3. Complete Mediation

Prinsip ini menyatakan bahwa setiap akses ke sistem komputer harus dicek ke dalam informasi kontrol akses untuk otorisasi yang tepat. Hal ini juga berlaku untuk kondisi-kondisi khusus seperti pada saat recovery/ pemeliharaan.

4. Open Design

Prinsip ini menyatakan bahwa mekanisme sekuriti dari suatu sistem harus dapat diinformasikan dengan baik sehingga memungkinkan adanya umpan balik yang dapat diman faatkan untuk perbaikan sistem sekuriti/ keamanan. Selain itu desain sistem harus bersifat terbuka, artinya jika memiliki source code/ kode sumber maka kode tersebut harus dibuka, dengan maksud untuk meminimalkan kemungkinan adanya hole/ celah keamanan dalam sistem.

5. Separation of Priviledge

Prinsip ini menyatakan bahwa untuk mengakses suatu informasi tertentu seorang user harus memenuhi beberapa persyaratan tertentu. Hal ini dapat implementasikan dengan menerapkan sistem akses bertingkat, di mana user dibagi dalam beberapa tingkatan dan mempunyai hak akses yang berbeda.

6. Least Common Mechanism

Prinsip ini menyatakan bahwa antar user harus terpisah dalam sistem. Hal ini juga dapat diimplementasikan dengan sistem akses bertingkat.

7. Psychological Acceptability

Prinsip ini menyatakan bahwa mekanisme pengendalian sistem sekuriti harus mudah digunakan oleh user. Hal ini dapat dilakukan dengan mengadakan survei mengenai perilaku user yang akan menggunakan sistem.