MATA KULIAH SISTEM OPERASI
KODE MATA KULIAH CCS210

DISUSUN OLEH
NIZIRWAN ANWAR

FAKULTAS ILMU KOMPUTER
UNIVERSITAS ESA UNGGUL
JAKARTA
2018

MATERI

"COMPUTER SECURITY"

(KEAMANAN KOMPUTER)

10.1 Pendahuluan

Keamanan komputer (bahasa Inggris: computer security) atau dikenal juga dengan sebutan cybersecurity atau IT security adalah keamanan informasi yang diaplikasikan kepada komputer dan jaringannya. Computer security atau keamanan komputer bertujuan membantu user agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi. Informasinya sendiri memiliki arti non fisik.

Keamanan komputer adalah suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada komputer. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian atau korupsi, atau pemeliharaan ketersediaan, seperti dijabarkan dalam kebijakan keamanan.

Sistem keamanan komputer merupakan sebuah upaya yang dilakukan untuk mengamankan kinerja dan proses komputer. Penerapan computer security dalam kehidupan sehari-hari berguna sebagai penjaga sumber daya sistem agar tidak digunakan, modifikasi, interupsi, dan diganggu oleh orang yang tidak berwenang. Keamanan bisa diindentifikasikan dalam masalah teknis, manajerial, legalitas, dan politis. computer security akan membahas 2 hal penting yaitu Ancaman/Threats dan Kelemahan sistem/vulnerabillity.

Keamanan komputer memberikan persyaratan terhadap komputer yang berbeda dari kebanyakan persyaratan sistem karena sering kali berbentuk pembatasan terhadap apa yang tidak boleh dilakukan komputer. Ini membuat keamanan komputer menjadi lebih menantang karena sudah cukup sulit untuk membuat program komputer melakukan segala apa yang sudah dirancang untuk dilakukan dengan benar. Persyaratan negatif juga sukar untuk dipenuhi dan membutuhkan pengujian mendalam untuk verifikasinya, yang tidak praktis bagi kebanyakan program komputer. Keamanan komputer memberikan strategi teknis untuk mengubah persyaratan negatif menjadi aturan positif yang dapat ditegakkan.

Pendekatan yang umum dilakukan untuk meningkatkan keamanan komputer antara lain adalah dengan membatasi akses fisik terhadap komputer, menerapkan mekanisme pada perangkat keras dan sistem operasi untuk keamanan komputer, serta membuat strategi pemrograman untuk menghasilkan program komputer yang dapat diandalkan.

10.1.1 Sejarah Keamanan Komputer

Arti dari keamanan komputer telah berubah dalam beberapa tahun terakhir. Sebelum masalah keamanan data/informasi menjadi popular, kebanyakan orang berpikir bahwa keamanan computer difokuskan pada alat alat computer secara fisik. Secara tradisional, fasilitas komputer secara fisik dilindungi karena tiga alasan:

(a) Untuk mencegah pencurian atau kerusakan hardware

(b) Untuk mencegah pencurian atau kerusakan informasi

(c) Untuk mencegah gangguan layanan

Prosedur yang sangat ketat untuk akses ke ruang server diaplikasikan oleh sebagian besar organisasi, dan prosedur ini sering digunakan untuk mengukur level keamanan computer. Dengan adanya akses jarak jauh atau remote terminal, jaringan yang sudah banyak serta teknologi internet yang berkembang pesat maka perlindungan secara fisik sudah jarang atau tidak dapat lagi digunakan untuk mengukur level keamanan. Meskipun demikian, masih ada beberapa perusahaan yang masih melindungi fasilitas fisik server mereka dengan peralatan cangih tetapi kurang memperhatikan perlindungan terhadap data atau informasi itu sendiri yang disimpan dalam server. Walupun nilai data atau informasi tersebut beberapa kali lebih besar dari nilai hardware.

Oleh karena itu konsep atau definisi computer security atau keamanan computer saat ini manjadi lebih luas atau bisa juga didefinisikan sebagai berikut: keamanan komputer dirancang untuk melindungi komputer dan segala sesuatu yang berkaitan dengan itu, bangunannya, workstation dan printer, kabel, dan disk dan media penyimpanan lainnya. Yang paling penting, keamanan komputer melindungi informasi yang disimpan dalam sistem anda. Keamanan komputer tidak hanya dirancang untuk melindungi terhadap penyusup dari luar yang masuk ke sistem, tetapi juga bahaya yang timbul dari dalam seperti berbagi password dengan teman, gagal atau tidak dilakukan untuk backup data, menumpahkan kopi pada keyboard dan sebagainya.

Didalam information security sering juga dikenal CIA Triad atau segitiga confidentiality (kerahasiaan), integrity (integritas), dan availability (ketersediaan). Kerahasiaan, integritas dan ketersediaan, yang dikenal sebagai segitiga CIA ini adalah model yang dirancang untuk memandu kebijakan untuk keamanan informasi dalam sebuah organisasi. Model ini juga kadang-kadang disebut sebagai triad AIC (ketersediaan, integritas dan kerahasiaan) untuk menghindari kebingungan dengan Central Intelligence Agency. Unsur-unsur dari tiga serangkai tersebut dianggap tiga komponen yang paling penting dari system keamanan.

Bila bicara kerahasiaan sama dengan bicara privasi. Langkah-langkah yang dilakukan untuk menjamin kerahasiaan dirancang untuk mencegah informasi rahasia dan sensitif di ambil oleh orang yang tidak berhak. Oleh karena itu access harus dibatasi hanya untuk mereka yang berwenang saja yang dapat melihat data yang sensitive atau rahasia tersebut. Sebuah sistem komputer yang aman harus menjaga agar informasi selalu tersedia untuk pengguna. Ketersediaan berarti bahwa perangkat keras dan perangkat lunak sistem komputer terus bekerja secara efisien dan bahwa sistem ini mampu pulih dengan cepat dan benar jika ada bencana.

Integritas melibatkan beberapa unsur yaitu: menjaga konsistensi, akurasi, dan kepercayaan dari data melalui seluruh siklus hidupnya. Data tidak boleh diubah pada saat ditransmisikan. Dalam hal ini harus diambil langkah langkah untuk memastikan bahwa data tidak dapat diubah oleh orang yang tidak berhak dan tidak kurang suatu apapun serta benar adanya. Dalam keamanan komputer ada tiga komponen yang selalu menjadi diskusi:

(a) Kerentanan: adalah kelemahan dari komputer yang memungkinkan penyerang untuk masuk ke sistem jaringann informasi.

(b) Ancaman: adalah kemungkinan bahaya yang mungkin mengeksploitasi kerentanan untuk melakukan gangguan pada system keamanan dan karena itu dapat menyebabkan kemungkinan bahaya bagi organisasi.

(c) Penanggulangan: adalah suatu tindakan, perangkat, prosedur, atau teknik yang mengurangi ancaman, kerentanan, atau serangan dengan menghilangkan atau mencegah, dengan meminimalkan kerugian itu dapat menyebabkan, atau dengan menemukan dan melaporkan masalah system keamanan sehingga tindakan korektif dapat diambil.

ada saat computer diperkenalkan pertama kali, ukuran komputer sangat besar, langka, dan sangat mahal. Oleh karena itu organisasi atau perusahaan yang cukup beruntung memiliki komputer akan mencoba dengan cara terbaik untuk melindungi computer tersebut. Keamanan komputer hanya salah satu aspek dari keamanan secara keseluruhan dari asset organisasi. Keamanan difokuskan pada fisik pembobolan, pencurian peralatan komputer, dan pencurian atau perusakan kemasan disk, gulungan pita, dan media lainnya. Hanya sedikit orang yang tahu bagaimana menggunakan komputer, dan dengan demikian pengguna harus dengan hati-hati dipilih. Pada saat itu computer tidak terhubung dengan jaringan internet sehingga memang masalah keamanan hanya berfokus pada fisik dan lingkungannya saja.

Pada 1970-an, teknologi komunikasi berubah, dan dengan itu cara-cara berkomunikasi juga berubah, pengguna yang berhubungan dengan komputer dan data dapat bertukar informasi dengan menggunakan jaringan telepon. Selain itu multi-programaming, timesharing, dan jaringan mengubah semua aturan dalam berkomunikasi. Dengan terkoneksinya computer pada jaringan telepon maka pengguna berkemampuan untuk mengakses komputer dari lokasi terpencil. Dengan kemampuan itu mengubah penggunaan komputer. Komputer merambah ke bidang bisnis dengan mulai menyimpan informasi secara online dan terkoneksi dengan jaringan secara bersama-sama dan dengan mainframe yang berisi database.

Dengan di mulainya computer dan jaringan untuk keperluan bisnis maka mulai muncul masalah keamanan computer terutama menyangkut pencurian data dan informasi. Sehingga masalah keamanan computer tidak lagi terfokus pada masalah fisik dan lokasi, tetapi di tambah dengan masalah kemanan data dan informasi **(Binus, 2017).**

10.1.2 Definisi

Keamanan komputer (Computer Security) merupakan suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada komputer. Pengertian tentang keamanan komputer ini beragam-ragam, sebagai contoh dapat kita lihat beberapa defenisi keamanan komputer menurut para ahlinya, antara lain :

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 system komputer

10.1.3 Tujuan

Menurut Garfinkel dan Spafford, ahli dalam computer security, komputer dikatakan aman jika bisa diandalkan dan perangkat lunaknya bekerja sesuai dengan yang diharapkan. Keamanan komputer memiliki 5 tujuan, yaitu:

(a) Availability
(b) Integrity
(c) Control
(d) Audit
(e) Confidentiality

Tujuan Keamanan Komputer dalam CASIFO:

(a) Perusahaan

Berusaha melindungi data dan informasi dari orang yang tidak berada dalam ruang lingkupnya.

(b) Ketersediaan

Tujuan SIFO adalah menyediakan data dan informasi bagi mereka yang berwenang untuk menggunakannya.

(c) Integritas

Semua subsistem SIFO harus menyediakan gambaran akurat dari sistem fisik yang di wakilinya

10.1.4 Metode Keamanan

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

(a) 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.

(b) 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.

(c) Keamanan **Level 2**, yaitu keamanan dari segi keamanan jaringan. Keamanan ini sebagai tindak lanjut dari keamanan level 1.

(d) 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.

(e) 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.

Berdasarkan sistem, metode pengamanan komputer terbagi dalam beberapa bagian antara lain :

(a) Network Topology

Sebuah jaringan komputer dapat dibagi atas kelompok jaringan eksternal (Internet atau pihak luar) kelompok jaringan internal dan kelompok jaringan eksternal diantaranya disebut DeMilitarized Zone (DMZ). - Pihak luar : Hanya dapat berhubungan dengan host-host yang berada pada jaringan DMZ, sesuai dengan kebutuhan yang ada. - Host-host pada jaringan DMZ : Secara default dapat melakukan hubungan dengan host-host pada jaringan internal. Koneksi secara terbatas dapat dilakukan sesuai kebutuhan. - Host-host pada jaringan Internal : Host-host pada jaringan internal tidak dapat melakukan koneksi ke jaringan luar, melainkan melalui perantara host pada jaringan DMZ, sehingga pihak luar tidak mengetahui keberadaan host-host pada jaringan komputer internal.

(b) Security Information Management

Salah satu alat bantu yang dapat digunakan oleh pengelola jaringan komputer adalah Security Information Management (SIM). SIM berfungsi untuk menyediakan seluruh informasi yang terkait dengan pengamanan jaringan komputer secara terpusat. Pada perkembangannya SIM tidak hanya berfungsi untuk mengumpulkan data dari semua peralatan keamanan jaringan komputer tetapi juga memiliki kemampuan untuk analisis data melalui teknik korelasi dan query data terbatas sehingga menghasilkan peringatan dan laporan yang lebih lengkap dari masing-masing serangan. Dengan menggunakan SIM, pengelola jaringan komputer dapat mengetahui secara efektif jika terjadi serangan dan dapat melakukan penanganan yang lebih terarah, sehingga organisasi keamanan jaringan komputer tersebut lebih terjamin.

(c) IDS / IPS

Intrusion detection system (IDS) dan Intrusion Prevention system (IPS) adalah sistem yang digunakan untuk mendeteksi dan melindungi sebuah sistem keamanan dari serangan pihak luar atau dalam. Pada IDS berbasiskan jaringan komputer , IDS akan menerima kopi paket yang ditujukan pada sebuah host untuk selanjutnya memeriksa paket-paket tersebut. Jika ditemukan paket yang berbahaya, maka IDS akan memberikan peringatan pada pengelola sistem. Karena paket yang diperiksa adalah salinan dari paket yang asli, maka jika ditemukan paket yang berbahaya maka paket tersebut akan tetap mancapai host yang ditujunya.Sebuah IPS bersifat lebih aktif daripada IDS. Bekerja sama dengan firewall, sebuah IPS dapat memberikan keputusan apakah sebuah paket dapat diterima atau tidak oleh sistem. Apabila IPS menemukan paket yang dikirimkan adalah paket berbahaya, maka IPS akan memberitahu firewall sistem untuk menolak paket data itu. Dalam membuat keputusan apakah sebuah paket data berbahaya atau tidak, IDS dan IPS dapat memnggunakan metode

(1) Signature based Intrusion Detection System : Telah tersedia daftar signature yang dapat digunakan untuk menilai apakah paket yang dikirimkan berbahaya atau tidak.
(2) Anomaly based Intrusion Detection System : Harus melakukan konfigurasi terhadap IDS dan IPS agar dapat mengetahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Paket anomaly adalah paket yang tidak sesuai dengan kebiasaan jaringan komputer tersebut.

(d) Port Scanning

Metode Port Scanning biasanya digunakan oleh penyerang untuk mengetahui port apa saja yang terbuka dalam sebuah sistem jaringan komputer. Cara kerjanya dengan cara mengirimkan paket inisiasi koneksi ke setiap port yang sudah ditentukan sebelumnya. Jika port scanner menerima jawaban dari sebuah port, maka ada aplikasi yang sedang bekerja dan siap menerima koneksi pada port tersebut.

(e) Packet Fingerprinting

Dengan melakukan packet fingerprinting, kita dapat mengetahui peralatan apa saja yang ada dalam sebuah jaringan komputer. Hal ini sangat berguna terutama dalam sebuah organisasi besar di mana terdapat berbagai jenis peralatan jaringan komputer serta sistem operasi yang digunakan.

10.1.5 Jenis Ancaman jaringan

(a) Probe

Probe atau yang biasa disebut probing adalah usaha untuk mengakses sistem dan mendapatkan informasi tentang sistem

(b) Scan

Scan adalah probing dalam jumlah besar menggunakan suatu tool

(c) Account compromise

Meliputi User compromize dan root compromize

(d) Packet Snifer

Adalah sebuah program yang menangkap data dari paket yang lewat di jaringan. (username, password, dan informasi penting lainnya)

(e) Hacking

Hacking adalah tindakan memperoleh akses ke komputer atau jaringan komputer untuk mendapatkan atau mengubah informasi tanpa otorisasi yang sah

(f) Denial-of-Service

Serangan Denial-of-service (DoS) mencegah pengguna yang sah dari penggunaan layanan ketika pelaku mendapatkan akses tanpa izin ke mesin atau data. Ini terjadi karena pelaku membanjiri jaringan dengan volume data yang besar atau sengaja menghabiskan sumber daya yang langka atau terbatas, seperti process control blocks atau koneksi jaringan yang tertunda. Atau mereka mengganggu komponen fisik jaringan atau memanipulasi data yang sedang dikirimkan, termasuk data terenkripsi.

(g) Malicious code (Kode Berbahaya)

Malicious code adalah program yang menyebabkan kerusakan sistem ketika dijalankan. Virus, worm dan Trojan horse merupakan jenis-jenis malicious code. - Virus komputer adalah sebuah program komputer atau kode program yang merusak sistem komputer dan data dengan mereplikasi dirinya sendiri melalui peng-copy-an ke program lain, boot sector komputer atau dokumen. - Worm adalah virus yang mereplikasi dirinya sendiri yang tidak mengubah file, tetapi ada di memory aktif, menggunakan bagian dari sistem operasi yang otomatis dan biasanya tidak terlihat bagi pengguna. Replikasi mereka yang tidak terkontrol memakan sumber daya sistem, melambatkan atau menghentikan proses lain. Biasanya hanya jika ini terjadi keberadaan worm diketahui. - Trojan horse adalah program yang sepertinya bermanfaat dan/atau tidak berbahaya tetapi sesungguhnya memiliki fungsi merusak seperti unloading hidden program atau command scripts yang membuat sistem rentan gangguan.

(h) Social Engineering / Exploitation of Trust

Sekumpulan teknik untuk memanipulasi orang sehingga orang tersebut membocorkan informasi rahasia. Meskipun hal ini mirip dengan permainan kepercayaan atau penipuan sederhana, istilah ini mengacu kepada penipuan untuk mendapatkan informasi atau akses sistem komputer. Beberapa jebakan yang dapat dilakukan diantaranya dengan : - Memanfaatkan kepercayaan orang dalam bersosialisasi dengan komputer - Memanfaatkan kesalahan orang secara manusiawi misal : kesalahan ketik dll - Bisa dengan cara membuat tampilan Login yang mirip (teknik fake login)

(i) Phishing

Tindakan pemalsuan terhadap data atau identitas resmi.

10.1.6 Aspek dan Lamgkah Keamanan Komputer

Inti dari keamanan komputer ialah melindungi komputer dan jaringannya dengan tujuan mengamankan informasi yang berada di dalamnya. Keamanan komputer ini sendiri meliputi beberapa aspek , antaranya ialah :

(a) *Privacy*, ialah sesuatu yang bersifat rahasia(provate). Intinya ialah pencegahan agar informasi tersebut tidak diakses oleh orang yang tidak berhak.

(b) *Confidentiality*, adalah data yang diberikan kepada pihak lain untuk tujuan khusus tetapi tetap dijaga penyebarannya.

(c) *Integrity*, penekanannya merupakan sebuah informasi tidak boleh diubah kecuali oleh pemilik informasi

(d) *Autentication*, ialah ini akan dilakukan sewaktu user login dengan menggunakan nama user dan passwordnya, apakah cocok atau tidak, apabila cocok diterima dan tidak akan ditolak.

(e) *Availability*, aspek ini ialah berkaitan dengan apakah sebuah data tersedia saat dibutuhkan/diperlukan.

Langkah-langkah Keamanan Komputer

(a) Aset : ialah “Perlindungan aset merupakan hal yg penting dan juga merupakan langkah awal dari berbagai implementasi keamanan komputer.”

(b) Analisa Resiko : ialah “Identifikasi akan resiko yg mungkin terjadi, sebuah even yg potensial yg bisa mengakibatkan suatu system dapat dirugikan.”

(c) Perlindungan : ialah “Pada era jaringan, perlu dikwatirkan tentang keamanan dari sistem komp, baik PC maupun yg terkoneksi dgn jaringan.

(d) Alat : ialah “Tool yang digunakan pd PC memiliki peran penting dlm hal keamanan krn tool yg digunakan harus benar2 aman.”

(e) Prioritas : ialah “perlindungan PC secara menyeluruh.”

10.2 Implementasi Keamanan

Ada 3 (tiga) macam Computer security yang berkaitan dengan kehidupan sehari-hari antara lain :

(1) Keamanan eksternal / external security, berkaitan dengan pengamanan fasilitas komputer dari penyusup dan bencana seperti kebakaran /kebanjiran.
(2) Keamanan interface pemakai / user interface security, berkaitan dengan indentifikasi pemakai sebelum pemakai diijinkan mengakses program dan data yang disimpan
(3) Keamanan internal / internal security, berkaitan dengan pengamanan beragam kendali yang dibangun pada perangkat keras dan sistem operasi yang menjamin operasi yang handal dan tak terkorupsi untuk menjaga integritas program dan data.

Dari berbagai macam jenis implementasi computer security ada hal yang perlu untuk diperhatikan dalam menjaga keamanan komputer. Di bawah ini adalah dua masalah penting di kehidupan sehari-hari yang harus diperhatikan dalam keamanan computer;

(a) Kehilangan data / data loss

Masalah data loss dapat disebabkan oleh :

1. Bencana
2. Kesalahan perangkat lunak dan perangkat keras
3. Kesalahan manusia / human error

(b) Penyusup / intruder, penyusup bisa dikategorikan kedalam dua jenis :

1. Penyusup **pasif** yaitu membaca data yang tidak terotorisasi (tidak berhak mengakses)
2. Penyusup **aktif** yaitu mengubah susunan sistem data yang tidak terotorisasi.

Selain itu ancaman lain terhadap sistem keamanan komputer bisa dikategorikan dalam empat macam :

(c) Interupsi / interruption, sumber daya sistem komputer dihancurkan sehingga tidak berfungsi. Contohnya penghancuran harddisk atau pemotongan kabel. Ini merupakan ancaman terhadap ketersediaan.

(d) Intersepsi / interception, orang yang tak diotorisasi dapat masuk / mengakses ke sumber daya sistem. Contohnya menyalin file yang terotorisasi. Ini merupakan ancaman terhadap kerahasiaan.

(e) Modifikasi / modification, orang yang tak diotorisasi tidak hanya dapat mengakses tetapi juga mengubah,merusak sumber daya. Contohnya mengubah isi pesan, atau mengacak program. Ini merupakan ancaman terhadap integritas

(f) Fabrikasi / fabrication, orang yang tak diotorisasi menyisipkan objek palsu ke dalam sistem. Contohnya memasukkan pesan palsu, menambah data palsu. Dari kategori yang ada diatas dan jika dikaitkan dalam kehidupan sehari-hari pasti kita akan menemukan masalah dalam komputer.

10.3 Ancaman Keamanan terhadap Komputer

Dibawah ini merupakan nama-nama ancaman yang sering dilihat dalam sistem keamanan komputer.

(a) Adware
(b) Backdoor Trojan
(c) Bluejacking
(d) Bluesnarfing
(e) Boot Sector Viruses
(f) Browser Hijackers
(g) Chain Letters
(h) Cookies
(i) Denial of Service Attack
(j) Dialers
(k) Document Viruses
(l) Email Viruses
(m) Internet Worms
(n) Mobile Phone Viruses

10.4 Jenis Ancaman Keamanan terhadap Komputer

Berikut ini adalah contoh ancaman-ancaman yang sering dilihat :

(a) Virus
(b) Email Virus
(c) Internet Worms
(d) Spam
(e) Trojan Horse
(f) Spyware
(g) Serangan Brute-force

10.5 Manfaat Keamanan terhadap Komputer

Guna manfaat sistem keamanan computer yaitu menjaga suatu sistem komputer dari pengaksesan seseorang yang tidak memiliki hak untuk mengakses sistem komputer tersebut. Sistem keamanan komputer semakin dibutuhkan saat ini seiring dengan meningkatnya penggunaan komputer di seluruh penjuru dunia. Selain itu makin meningkatnya para pengguna yang menghubungkan jaringan LANnya ke internet, namun tidak di imbangi dengan SDM yang dapat menjaga keamanan data dan infomasi yang dimiliki. Sehingga keamanan data yang ada menjadi terancam untuk diakses dari orang-orang yang tidak berhak. Keamanan komputer menjadi penting karena ini terkait dengan Privacy, Integrity, Autentication, Confidentiality dan Availability. Beberapa ancaman keamanan komputer adalah virus, worm, trojan, spam dan lain-lain. Masing-masingnya memiliki cara untuk mencuri data bahkan merusak sistem komputer. Ancaman bagi keamanan sistem komputer ini tidak dapat dihilangkan begitu saja, namun kita dapat meminimalkan hal ini dengan menggunakan perangkat lunak (software) keamanan sistem diantaranya antivirus, antispam dan sebagainya..

10.5.1 Faktor

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

(a) Meningkatnya penggunaan komputer dan internet.

(b) Banyaknya software yang pada awalnya digunakan untuk melakukan audit sebuah system dengan cara mencari kelemahan dan celah yang mungkin disalahgunakan untuk melakukan scanning system orang lain.

(c) Banyaknya software untuk melakukan penyusupan yang tersedia di Internet dan bisa di download secara gratis.

(d) Meningkatnya kemampuan pengguna komputer dan internet.

(e) Kurangnya hukum yang mengatur kejahatan komputer.

(f) Semakin banyaknya perusahaan yang menghubungkan jaringan LAN mereka ke Internet.

(g) Meningkatnya aplikasi bisnis yang menggunakan internet.

(h) Banyaknya software yang mempunyai kelemahan (bugs).

Ada beberapa macam penyusup yang bisa menyerang system yang dimiliki, antara lain :

(a) **Ingin Tahu**, jenis penyusup ini pada dasarnya tertarik menemukan jenis system yang digunakan.

(b) **Perusak**, jenis penyusup ini ingin merusak system yang digunakan atau mengubah tampilan layar yang dibuat.

(c) **Menyusup untuk popularitas**, penyusup ini menggunakan system untuk mencapai popularitas dia sendiri, semakin tinggi system keamanan yang kita buat, semakin membuatnya penasaran. Jika dia berhasil masuk ke sistem kita maka ini menjadi sarana baginya untuk mempromosikan diri.

(d) **Pesaing**, penyusup ini lebih tertarik pada data yang ada dalam system yang kita miliki, karena dia menganggap kita memiliki sesuatu yang dapat menguntungkannya secara finansial atau malah merugikannya (penyusup).

10.5.2 Dampak

Dampak negatif yang ditimbulkan dari penggunaan sistem keamanan komputer yaitu.;

(a) Menurunnya nilai transaksi melalui internet terhadap E-Commerse

(b) Menurunnya tingkat kepercayaan dalam melakukan komunikasi dan transaksi melalui media online

(c) Merugikan secara moral dan materi bagi korban yang data-data pribadinya dimanipulasi

Seperti juga masalah yang ada di Indonesia yang menurut saya bisa dijadikan salah satu contoh dampak negative dari penggunaan sistem keamanan komputer yaitu;

(a) Pencurian dan penggunaan account Internet milik orang lain. Salah satu kesulitan dari sebuah ISP (Internet Service Provider) adalah adanya account pelanggan mereka yang “dicuri” dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, pencurian account cukup menangkap user id dan password saja. Hanya informasi yang dicuri. Sementara itu orang yang kecurian tidak merasakan hilangnya benda yang dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak berhak. Akibat dari pencurian ini, pengguna dibebani biaya penggunaan account tersebut. Kasus ini banyak terjadi di ISP. Membajak situs web. Salah satu kegiatan yang sering dilakukan oleh cracker adalah mengubah halaman web, yang dikenal dengan istilah deface. Pembajakan dapat dilakukan dengan meng[eksploitasi lubang keamanan.

(b) Probing dan port scanning. Salah satu langkah yang dilakukan cracker sebelum masuk ke server yang ditargetkan adalah melakukan

pengintaian. Cara yang dilakukan adalah dengan melakukan port scanning atau probing untuk melihat servis-servis apa saja yang tersedia di server target. Sebagai contoh, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mai server Sendmail, dan seterusnya. Analogi hal ini dengan dunia nyata adalah dengan melihat-lihat apakah pintu rumah anda terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci menggunakan (firewall atau tidak) dan seterusnya. Yang bersangkutan memang belum melakukan kegiatan pencurian atau penyerangan, akan tetapi kegiatan yang dilakukan sudah mencurigakan.

Berbagai program yang digunakan untuk melakukan probing atau portscanning ini dapat diperoleh secara gratis di Internet. Salah satu program yang paling populer adalah nmap (untuk sistem yang berbasis UNIX, Linux) dan Superscan (untuk sistem yang berbasis Microsoft Windows). Selain mengidentifikasi port, nmap juga bahkan dapat mengidentifikasi jenis operating system yang digunakan.

(a) Virus. Seperti halnya di tempat lain, virus komputer pun menyebar di Indonesia. Penyebaran umumnya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terkena virus tidak sadar akan hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

(b) Denial of Service (DoS) dan Distributed DoS (DDos) attack. DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet.

10.6. Cara Mudah Tingkatkan Keamanan Komputer

Selain menggunakan smartphone (https://www.liputan6.com/tekno/read/3227324/ini-7-cara-mudah-tingkatkan-keamanan-komputer), komputer dan laptop merupakan perangkat teknologi yang sering digunakan dalam keseharian. Namun, komputer yang terhubung ke jaringan internet bisa mengancam data dan privasi para penggunanya.

Internet memang memudahkan berbagai aktivitas, tapi pengguna tetap harus waspada karena ada berbagai ancaman siber yang mengancam data-data mereka. Oleh karena itu, pengguna komputer atau laptop harus selalu berhati-hati agar data

mereka tetap terjaga. Berikut 7 (tujuh) cara untuk meningkatkan keamanan komputer agar terbebas dari berbagai hal yang tidak diinginkan, termasuk malware:

10.6.1. Gunakan selalu Incognito mode saat berada di luar

Saat berpergian, kalian terkadang memerlukan komputer atau laptop seperti untuk mengakses email dan media sosial. Untuk melakukan aktivitas tersebut, maka dibutuhkan jaringan internet.

Fitur Incognito mode sangat berguna ketika mengakses data penting saat berselancar internet, terutama di tempat publik. Saat masuk dalam mode ini, kalian tidak perlu terlalu mengkhawatirkan data yang tersimpan, bahkan saat lupa menekan tombol logout. Incognito mode adalah fitur privasi pada situs web untuk menonaktifkan history dan cache browsing.

10.6.2. Pakai Antivirus

Saat membeli komputer baru, banyak orang khawatir mengenai fitur keamanannya. Kekhawatiran tersebut membuat mereka memasang beberapa aplikasi keamanan sekaligus seperti antivirus dan antispyware. Padahal, hal ini akan membebani kinerja komputer yang berimbas pada performa.

Untuk mengatasi permasalahan semacam itu, saat ini OS seperti Windows 10 sudah menyediakan antivirus bawaan. Namun jika masih terasa kurang, kalian cukup memasang satu antivirus lagi sesuai dengan yang diinginkan.

10.6.3. Selalu update OS dan aplikasi

Ada sejumlah orang yang tidak peduli terhadap versi terbaru OS atau aplikasi yang digunakan pada komputer. Berbagai alasan dituturkan seperti proses update lama hingga kinerja komputer akan menurun.

Menggunakan versi terbaru OS dan aplikasi merupakan salah satu cara untuk membuat komputer tetap aman. Selain terkait dengan keamanan, proses update terutama OS justru akan meningkatkan performa komputer.

10.6.4. Ganti password secara berkala

Mengganti password secara berkala setiap enam bulan hingga satu tahun sekali sangat dianjurkan. Selain itu, sebaiknya gunakan password kuat dengan berbagai kombinasi di dalamnya seperti huruf, angka dan simbol.

Kalian bisa menggunakan aplikasi kalender untuk memberikan pemberitahuan jika sudah saatnya mengganti password. Kalian juga bisa menggunakan sejumlah aplikasi password manager untuk mengelola password pada berbagai akun online.

10.6.5. Backup data dan dokumen penting

Jika kalian sering bekerja secara offline, pasti akan menyimpan data dan dokumen pada drive penyimpanan yang tersedia. Untuk mencegah kehilangan data yang disebabkan berbagai hal, kalian dapat melakukan proses backup.

Saat ini ada banyak layanan cloud seperti OneDrive atau Dropbox untuk menyimpan data dan dokumen secara online. Bagi yang jarang terhubung ke internet, bisa menyimpan data-data tersebut pada flashdisk atau hard disk eksternal.

Salah satu aktivitas yang sering dilakukan menggunakan komputer adalah belanja online. Selain menghemat waktu dan tenaga, barang yang dijual di situs belanja online juga jauh lebih murah. Namun, kalian harus berhati-hati dan jangan sembarang melakukan pembayaran secara online.

Gunakan platform e-Commerce terpercaya dalam melakukan sistem pembayaran. Untuk mencegah penipuan, hindari memberikan data pribadi dan nomor rekening pada saat berbelanja secara pribadi.

10.6.6. Jangan sembarangan melakukan pembayaran online

Salah satu aktivitas yang sering dilakukan menggunakan komputer adalah belanja online. Selain menghemat waktu dan tenaga, barang yang dijual di situs belanja online juga jauh lebih murah. Namun, kalian harus berhati-hati dan jangan sembarang melakukan pembayaran secara online.

Gunakan platform e-Commerce terpercaya dalam melakukan sistem pembayaran. Untuk mencegah penipuan, hindari memberikan data pribadi dan nomor rekening pada saat berbelanja secara pribadi.

10.6.7. Abaikan pesan spam

Pengguna komputer sering kali menerina pesan berantai berisi promosi atau iklan menarik di berbagai media sosial. Hal ini sangat berbahaya, terutama jika ternyata

itu adalah pesan spam. Oleh karena itu, jangan pernah membuka link di dalam pesan spam tersebut.

Hal pertama yang perlu dilakukan adalah memastikan link tersebut asli dan bukan jebakan dari penjahat siber. Gunakan Google untuk memeriksa situs web resmi dari pesan yang diterima. Segera hapus jika ternyata pesan tersebut mencurigakan.

Tujuh tips di atas sebenarnya tidak hanya berlaku untuk pengguna komputer, tapi juga para pengguna gadget lain seperti smartphone dan laptop.

Daftar Pustaka

Andrew S Tanembaun 2015. Modern Operating System 4th EditIion

William Stallings 6th EditI/On 2008. Operating System, Internals and design Principles.

Anonymous. Sejarah Keamanan Komputer. 2017. https://mti.binus.ac.id/2017/04/05/sejarah-keamanan-komputer/ diakses novermber 2018

Anonymous. Pengertian dan Aspek-Aspek Keamanan Komputer. 2018. https://www.ayoksinau.com/pengertian-dan-aspek-aspek-keamanan-komputer-lengkap/ diakses novermber 2018

Anonymous. 3 Keamanan Jaringan (Tujuan, Resiko dan Ancaman Pada Jaringan Komputer). 2017. http://edukasiteki.blogspot.com/2017/08/3-keamanan-jaringan-tujuan-resiko-dan.html diakses novermber 2018