**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

**KDS – Name SME**

**Session 02**

**Attack and Malicious software**

**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:

• Untuk mencegah pencurian atau kerusakan hardware

• Untuk mencegah pencurian atau kerusakan informasi

• 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:

* Kerentanan: adalah kelemahan dari komputer yang memungkinkan penyerang untuk masuk ke sistem jaringann informasi.
* Ancaman: adalah kemungkinan bahaya yang mungkin mengeksploitasi kerentanan untuk melakukan gangguan pada system keamanan dan karena itu dapat menyebabkan kemungkinan bahaya bagi organisasi.
* 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.

Awal mula keamanan computer.

Pada 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, time-sharing, 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.

**Computer Defenses**

Berdasarkan dari fungsi dan kegunaan computer saat ini maka selain fisik atau hardware nya juga harus diperhatikan keamanan jaringan beserta softwarenya. Untuk itu dalam beberapa literature disebutkan bahwa serangan dapat dilakukan melalui beberapa cara yaitu:

1. Melalui perangkat network seperti router, switch, access point dan sebagainya.
2. Melalui operating system seperti Microsoft windows
3. Melalui aplikasi seperti Microsoft office, adobe, database software dan sebagainya.

Namun seiring dengan perkembangan teknologi dan kelemahan manusia maka serangan juga dapat dilakukan melalui orang atau manusia yaitu dengan menggunakan teknik social engineering. Dengan demikian untuk pertahanan terhadap serangan maka harus dilakukan evaluasi dan testing terhadap hal hal tersebut.

Untuk serangan terhadap perangkat keras mulai dari yang sederhana sampai yang rumit. Salah satu contohnya adalah serangan terhadap router mulai dari menggunakan default user name dan password sampai memasukkan code jahat pada firmware router tersebut. Oleh karena untuk router jangan menggunakan user name “admin” dan ganti passwordnya. Kemudian ganti firmware nya atau passtikan sudah menginstall update yang terakhir.

Untuk serangan terhadap operating system seorang hacker akan berusaha mencari jenis operating system yang digunakan oleh target beserta versi nya. Setelah mengetahui inforrmasi jenis operating system dan versi nya, hacker akan mencari tahu vulnerability dari operating system tersebut dengan menggunakan mesin pencari atau lansung ke website Microsoft windows. Setelah itu hacker dapat langsung menyerang computer target dengan tool atau software yang tepat. Oleh karena itu untuk menghadapi serangan terhadap operating system, user harus selalu mengupdate atau menginstall path yang disediakan oleh pembuat operating system.

Serangan terhadap aplikasi adalah serangan yang paling banyak dilakukan karena kerentanan pada aplikasi lebih mungkin terjadi sehingga saat ini lebih mudah menyerang melalui aplikasi.

Saat ini yang paling mudah untuk masuk dalam jaringan adalah melalui aplikasi. Karena kalau melalui operating sistem sudah tidak mudah lagi, hal inipun dapat kita rasakan bahwa pada os windows sudah tidak sering lagi kita mengupdate, ini menunjukkan os sudah relatif cukup aman dibanding os sebelumnya. Demikian juga perangkat perangkat network sudah relatif sulit untuk masuk melalui perangkat network. Yang paling lemah adalah serangan melalui aplikasi, karena sering dijumpai bahwa developer lebih cenderung memperhatikan fuctional sebuah aplikasi sementara masalah security dari aplikasi tersebut di nomor duakan, bahkan mungkin tidak diperhatikan. Padahal ada banyak aplikasi yang baru yang muncul setiap saat didunia ini.

Terakhir adalah serangan dengan menggunakan kelemahan manusia, atau social engineering. Untuk menangkal serangan ini adalah dengan melalui training sumber daya manusia. Training tentang kesadaran keamanan computer sangat perlu dilakukan secara periodic setiap tahun. Isi training dapat juga memberikan contoh contoh serangan yang ada saat ini. Dengan demikian semua staff dapat mengetahui cara atau teknik serangan social engineering.

**Malicious Software (Malware)**

Malicious software adalah istilah untuk perangkat lunak yang terinstal pada komputer Anda yang biasanya tidak diketahui dan perangkat lunak ini melakukan tugas-tugas yang tidak diinginkan, dan untuk kepentingan pihak ketiga atau intruder. Program malware bisa dari yang paling sederhana (iklan pop-up) sampai program yang dapat menyebabkan invasi komputer yang serius dan kerusakan (misalnya, mencuri password dan data atau menginfeksi komputer lain pada jaringan). Selain itu, ada beberapa program malware yang dirancang untuk mengirimkan informasi tentang kebiasaan browsing web dari korban yang gunanya untuk mengirimkan iklan atau kepentingan pihak ketiga lainnya tanpa Anda menyadarinya.

Malware adalah istilah yang luas yang mengacu pada berbagai program jahat. Beberapa jenis malware yang paling umum adalah; adware, bots, bug, rootkit, spyware, trojan horse, virus, dan worm.

Adware

Adware adalah software yang dapat menampilkan iklan yang tidak diinginkan. Ini bisa juga merupakan perangkat lunak atau software yang dapat di download secara gratis yang didalam nya memang ada iklan yang dapat muncul secara pop-up atau muncul pada toolbar di komputer atau browser. Sebagian besar adware sangat menggangu, tapi relative aman. Tetapi beberapa adware dapat digunakan untuk mengumpulkan informasi pribadi Anda, melacak situs yang Anda kunjungi dan atau bahkan merekam keystrokes Anda. Kebanyakan Adware terdapat pada software yang disebarkan secara gratis, adware adware tersebut akan muncul setelah kita menginstall software yang di download secara gratis. Selain itu sebagian adware juga bisa terinstal pada saat kita menginstall browser atau sistem operasi. Atau juga bisa terinstall melalui lubang keamanan dari browser atau system operasi.

Komputer, laptop atau perangkat kita yang lainnya mungkin terinfeksi oleh adware jika. Tanda yang paling mudah terlihat adalah ketika kita mulai melihat iklan bermunculan di aplikasi yang mana kita tidak melihat iklan iklan itu sebelumnya. Bahkan adware juga dapat muncul di perangkat komputer kita ketika kita sedang tidak browsing Internet. Kita dapat menggunakan scanner adware (yang termasuk dalam semua removal tools adware) untuk memeriksa apakah perangkat kita terinfeksi oleh adware atau tidak.

Pada umumnya untuk mencegah agar perangkat kita tidak terinfeksi adware, maka kita dapat melakukan hal hal berikut:

• Pilih dan install antivirus yang dapat mendeteksi adware dan meng-unistall adware tersebut.

• Pastikan bahwa browser, sistem operasi, dan perangkat lunak sudah di-update dengan patch keamanan yang terbaru.

• Mengaktifkan firewall saat menggunakan internet.

Bot

Sebuah "bot" adalah jenis malware yang memungkinkan penyerang untuk mengambil kontrol atas komputer yang menjadi korban. Juga dikenal sebagai "Web robot", bot biasanya bagian dari jaringan mesin yang terinfeksi, yang dikenal sebagai "botnet", yang biasanya terdiri dari computer korban yang membentang di seluruh dunia.

Bot adalah salah satu jenis yang paling canggih dan populer dari cybercrime hari ini. Bot memungkinkan hacker untuk mengambil kendali dari banyak komputer pada satu waktu, dan mengubahnya menjadi komputer "zombie", yang beroperasi sebagai bagian dari "botnet" yang kuat untuk menyebarkan virus, menghasilkan spam, dan melakukan jenis-jenis kejahatan online dan penipuan.

Untuk melindungi computer terhadap bot yang berbahaya, maka dapat dilakukan hal hal sebagai berikut:

• Menginstal perangkat lunak keamanan

• Mengkonfigurasi pengaturan perangkat lunak (software dan operating system) untuk dapat update secara otomatis.

• Meningkatkan pengaturan keamanan pada browser.

• Membatasi hak-hak pengguna pada komputer ketika online.

• Jangan pernah mengklik lampiran kecuali jika kita dapat memverifikasi sumber.

• Pastikan bahwa sistem kita sudah di patch dengan Microsoft Windows Update yang terbaru.

• Mengatur pengaturan keamanan computer (antivirus) kita untuk update secara otomatis, untuk memastikan kita selalu memiliki patch sistem terbaru

Rootkit

Rootkit adalah program komputer yang dirancang untuk memberikan akses ke komputer yang sedang aktif dengan secara diam diam atau tanpa diketahui administrator atau menyembunyikan kehadirannya. Rootkit adalah tool atau aplikasi yang memungkinkan seorang administrator mengakses komputer atau jaringan yang menjadi tanggung jawabnya dengan tujuan untuk mempermudah pekerjaan mereka. Tetapi, sekarang rootkit umumnya dapat digunakan oleh attacker atau orang jahat menjadi sebuah malware - seperti Trojan, worm, virus. Rootkit memungkinkan seseorang yang tidak berhak untuk mengontrol komputer tanpa diketahui oleh pemilik computer.

Rootkit ini menjadi sangat berbahaya karena tidak ada produk komersial (antivirus ataupun software security) yang ada yang 100% dapat menemukan dan menghapus semua rootkit yang dikenal dan tidak dikenal. Metode deteksi yang sering digunakan untuk mendetek rootkit biasanya metode berbasis perilaku (misalnya, mencari perilaku aneh pada sistem komputer), tanda tangan pemindaian dan analisis dump memori.

Seringkali, satu-satunya pilihan untuk menghapus rootkit adalah untuk benar-benar menghapus atau uninstall software atau yang paling pasti adalah dengan format kembali hard disk dan membangun kembali operating sistem.

Kebanyakan rootkit dapat masuk ke sistem komputer dengan membonceng free software yang berguna. Kita dapat menjaga sistem computer dari rootkit dengan memastikan bahwa kita sudah mengupdate atau mendownload path dari kerentanan/vulnerability yang sudah diketahui. Ini termasuk patch dari OS, aplikasi dan up-to-date definisi virus. Kemudian juga, jangan pernah menerima dan membuka file atau berkas dari lampiran pada email dari sumber yang tidak diketahui. Hati-hati saat menginstal perangkat lunak dan hati-hati membaca perjanjian lisensi dan term and condition.

Spyware

Spyware adalah istilah umum yang digunakan untuk menjelaskan perangkat lunak yang melakukan perilaku tertentu, umumnya tanpa diketahui oleh anda atau korban terlebih dahulu. Tujuan spyware adalah untuk:

• Mendapatkan informasi dengan tujuan iklan

• Mengumpulkan informasi pribadi

• Mengubah konfigurasi komputer Anda

Spyware sering dikaitkan dengan perangkat lunak yang menampilkan iklan (disebut adware) atau perangkat lunak yang melacak informasi pribadi atau sensitif. Spyware dapat mengubah halaman web atau penelusuran halaman web browser, atau menambahkan komponen tambahan ke browser yang kita tidak perlu atau inginkan. Biasanya, spyware diinstal ketika pengguna menginstal software gratis yang mereka inginkan. Untuk itu kita harus membaca syarat dan ketentuan sebelum menginstal free software di computer serta membaca ulasan tentang perangkat lunak sebelum menginstal di komputer kita.

Trojan Horse

Sebuah Trojan horse atau Trojan adalah jenis malware yang sering menyamar sebagai perangkat lunak yang sah. Trojan dapat digunakan oleh cyber attacker dan hacker untuk mendapatkan akses ke sistem pengguna. Pengguna biasanya ditipu oleh beberapa bentuk social engineering untuk download dan menginstall Trojan pada sistem mereka. Setelah Trojan diaktifkan, hacker dapat memata-matai Anda, mencuri data sensitif Anda, dan mendapatkan akses backdoor ke sistem anda. Sebuah Trojan kemungkinan besar akan digunakan untuk memata-matai dan mencuri informasi pribadi dan sensitif (spionase industri). Berikut adalah data yang sering dicuri oleh attacker:

• informasi kartu kredit (sering digunakan untuk pendaftaran domain atau belanja)

• data pribadi (password email, password dial-up, layanan Web password, dll)

• dokumen rahasia

• alamat email (misalnya, rincian kontak pelanggan)

• desain rahasia atau gambar pribadi

• informasi kalender tentang keberadaan pengguna

• menggunakan komputer untuk tujuan ilegal, seperti untuk hack, scan, ddos atau menyusup komputer lain pada jaringan atau Internet.

Protect from Malware and Trojans

• Lindungi komputer Anda dengan software keamanan yang kuat dan pastikan untuk tetap up to date.

• Aktifkan update Windows otomatis atau men-download update Microsoft secara teratur untuk menjaga sistem operasi Anda terhadap kerentanan yang sudah dikenal.

• Hati-hati saat membuka lampiran. Mengkonfigurasi perangkat lunak anti-virus Anda untuk secara otomatis menscan semua email dan pesan termasuk dilampiran.

• Hati-hati saat terlibat dalam peer-to-peer (P2P) file-sharing. Trojan dalam program file sharing menunggu untuk di-download.

• Download versi terbaru dari browser Anda untuk memastikan bahwa browser sudah diupdate dan menggunakan teknologi terbaru untuk mengidentifikasi dan menyaring situs phishing yang dapat menginstal Trojan.

• Pastikan situs web bebas dari malware sebelum Anda mengunjungi web tersebut. Menggunakan perangkat lunak yang secara otomatis memeriksa ini.

• Back up file Anda secara teratur dan menyimpan backup di suatu tempat. Jika Anda menjadi korban serangan Trojan, Anda dapat memulihkan foto, musik, film, dan informasi pribadi seperti pajak dan laporan bank.

**SIMPULAN**

1. Saat ini kejahatan di bidang internet lebih cenderung memanfaatkan kelemahan dari sifat manusia, seperti teknik social engineering.
2. Untuk dapat berinternet dengan aman sebaiknya user mengenal beberapa jenis malware atau malicious software.

**DAFTAR PUSTAKA**

1. Stallings, William. (2006). Cryptography and Network Security. 4th edition. Pearson Education.Whitman, M.E., Mattoro, H.J. (2013).
2. Scambray, Joel; Liu, Vincent; Sima, Caleb. (2011). Hacking Exposed Web Applications: Web Application Security Secrets and Solutions. 3rd Edition. McGraw-Hill. ISBN: 9780071740647.