MERANCANG PENGAMAN (*SECURITY*) JARINGAN KOMPUTER

Oleh : Dwi Heri Sudaryanto *)

ABSTRAK

Pengaman (security) atau yang sering disebut dengan Firewall merupakan suatu perangkat keamanan jaringan computer yang memperkenankan berbagai bagian ruas jaringan untuk melaksanakan komunikasi antara satu dengan yang lainnya sesuai dengan definisi kebijakan keamanan (security policy) yang telah ditetapkan sebelumnya.

Firewalls peka terhadap kesalahan konfigurasi dan kegagalan untuk menerapkan kebijakan yang ditetapkan, sehingga diperlukan tambahan atau peningkatan keamanan lain. Oleh karena itu, konfigurasi dan administrasi firewall harus dilakukan secara hati-hati, sehingga jaringan seharusnya dapat bertahan dengan mengurangi kelemahan dan gangguan baru. Firewall merupakan garis pertahanan yang terdepan dari suatu jaringan komputer, sehingga dalam merancang pengaman jaringan seharusnya menerapkan strategi keamanan jaringan dengan sungguh-sungguh, terkait dengan di lapisan-lapisan mana saja firewall dan sistem keamanan lainnya digunakan diseluruh jaringan. Yang paling penting, administrasi jaringan perlu bekerja keras untuk memelihara semua sistem dan untuk menghentikan ancaman keamanan tidak semata-mata mengandalkan hanya pada firewall. OLeh karena itu sistem keamanan jaringan memerlukan perencanaan backup untuk mengatasi kasus kegagalan firewall sehingga sistem tidak terganggu dengan adanya penyusup (hacker) yang akan merusaknya.

Kata Kunci : Strategi, Pengaman, Jaringan Komputer.

I. LATAR BELAKANG

Dalam dunia Internet yang berkembang sedemikian pesatnya, jumlah para *hacker*, *cracker*, dan sebagainya juga semakin meningkat. Kita tidak bisa terus-menerus terlena akan keadaan dan kondisi dimana kita dalam keadaan aman. Apakah kita akan menunggu hingga jaringan kita dirusak oleh mereka? Tentu tidak! Setelah sebuah jaringan komputer kita berfungsi dan terhubung ke jaringan Internet, saat itulah kita harus mulai bersiaga dan memikirkan strategi beserta cara-cara untuk meningkatkan sekuriti jaringan komputer yang kita miliki. Strategi dalam sekuriti jaringan komputer bertujuan untuk memaksimalkan sumber daya yang ada untuk mengamankan sistem jaringan komputer pada titik-titik yang tepat sehingga lebih efisien. Bila tanpa strategi yang tepat, hasil implementasi strategi tersebut tidak akan menghasilkan tingkat sekuriti yang tinggi disamping mengakibatkan terbuangnya sumber daya yang ada akibat tidak tepatnya penempatan dalam jaringan komputer.

II. RUMUSAN MASALAH

Tujuan sekuriti jaringan adalah memaksimalkan sumber daya yang ada untuk mengamankan sistem jaringan komputer pada titik-titik yang tepat sehingga lebih efisien. Tetapi disisi lain kita tidak bisa mengikuti hal-hal yang setiap saat dapat merusak jaringan komputer kita. Dari latar belakang di atas dapat dikemukakan rumusan masalah sebagai berikut :

1. Bagaimana kita merancang dan menerapkan sistem keamanan jaringan komputer ?
2. Apa saja yang harus dipenuhi di dalam merancang keamanan jaringan komputer ?
3. Langkah-langkah apa saja dilakukan terhadap jaringan tanpa kabel ?

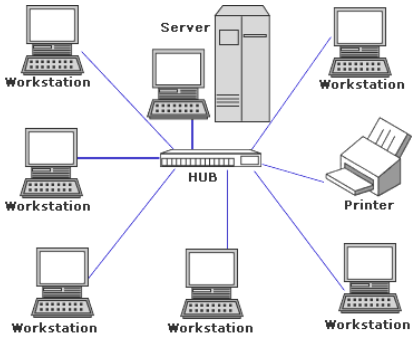
III. JARINGAN KOMPUTER

Jaringan komputer adalah hubungan antara 2 (dua) komputer atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). Dua unit komputer dikatakan terkoneksi apabila keduanya bisa saling bertukar data/informasi, berbagi sumber (*resource*) yang dimiliki, seperti: file, printer, media penyimpanan (hardisk, floppy disk, cd-rom, flash disk, dll). Data yang berupa teks, audio maupun video, bergerak melalui media kabel atau *wireless* sehingga memungkinkan pengguna komputer dalam jaringan komputer dapat saling bertukar file/data, mencetak pada printer yang sama dan menggunakan perangkat keras/lunak (*hardware/software*) yang terhubung dalam jaringan secara bersama-sama.

Secara umum jenis-jenis jaringan dibagi menjadi 4 (empat) : local area network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN), dan Internet – Intranet.

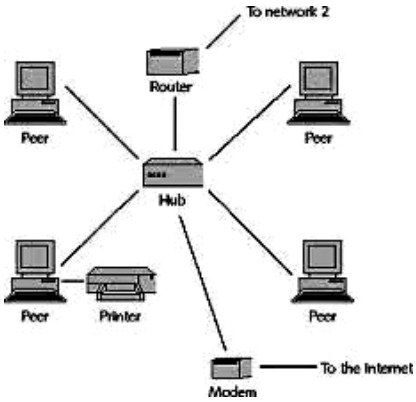
A. *Local Area Network* (LAN)

Local Area Network (LAN) dapat didefinisikan sebagai kumpulan komputer yang saling dihubungkan bersama didalam satu areal tertentu, seperti di dalam satu kantor atau gedung. LAN dapat juga didefinisikan berdasarkan pada penggunaan alamat IP komputer pada jaringan. Suatu komputer atau host dapat dikatakan satu LAN bila memiliki alamat IP yang masih dalam satu alamat jaringan, sehingga tidak memerlukan router untuk berkomunikasi.



Gambar Local Area Network (LAN)

Jaringan LAN dapat juga dibagi menjadi dua tipe, yaitu jaringan peer to peer dan jaringan client-server. Pada jaringan peer to peer, setiap komputer yang terhubung dapat bertindak baik sebagai workstation maupun server, sedangkan pada jaringan client-server, hanya satu komputer yang bertindak sebagai server dan komputer lain sebagai client/workstation.

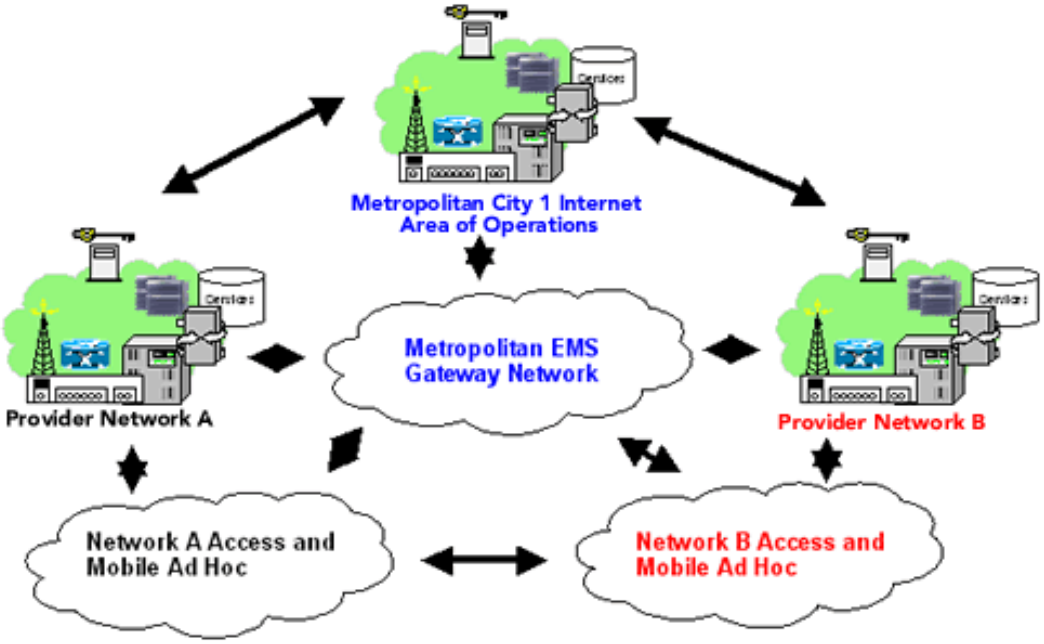


Gambar Jaringan Peer to Peer

Gambar Jaringan Client-Server

B. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN) merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.



Gambar Jaringan Metropolitan Area Network (MAN)

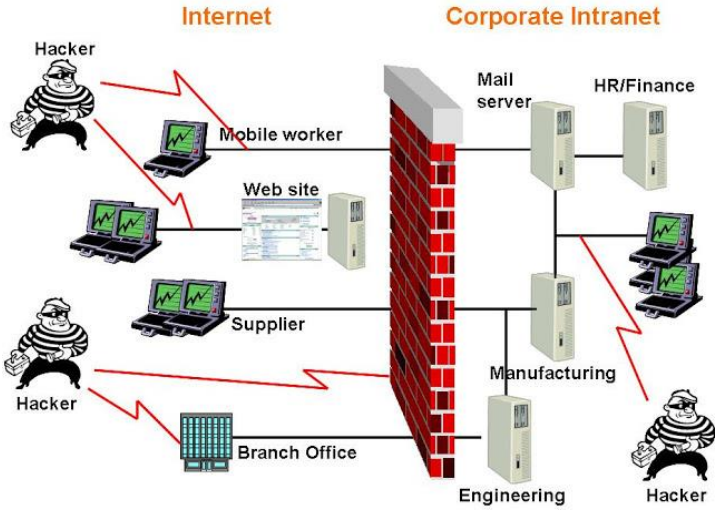
C. Wide Area Network (WAN)

Wide Area Network (WAN) adalah jaringan yang biasanya sudah menggunakan media tanpa kabel (wireless), sarana satelit ataupun kabel serat optik, karena jangkauannya yang lebih luas, bukan hanya meliputi satu kota atau antar kota dalam suatu wilayah, tetapi mulai menjangkau area/wilayah otoritas negara lain. WAN biasanya lebih rumit dan sangat kompleks bila dibandingkan LAN maupun MAN. WAN menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN kedalam komunikasi global seperti internet, meski demikian antara LAN, MAN dan WAN tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda satu diantara yang lainnya.

Gambar Wide Area Network (WAN)

D. Internet dan Intranet

Internet yang merupakan gabungan dari LAN, MAN, dan WAN adalah sebuah sistem komunikasi global yang menghubungkan komputer-komputer dan jaringan-jaringan komputer di seluruh dunia. Setiap komputer dan jaringan terhubung secara langsung maupun tidak langsung terhubung ke beberapa jalur utama yang disebut internet backbone dan dibedakan satu dengan yang lainnya menggunakan alamat unik yang biasa disebut dengan alamat Internet Protocol (IP).



Gambar Jaringan Internet dan Intranet

Aplikasi pada jaringan internet dapat juga diterapkan pada sebuah LAN yang memiliki server. Sebagai contoh di perusahaan yang memiliki jaringan client-server. Bila aplikasi yang ada pada internet, seperti mail server, diterapkan pada perusahaan tersebut, maka jaringan ini dapat disebut sebagai intranet. Client dapat mengakses server tersebut seperti mengakses internet pada umumnya. Client juga dapat mengakses aplikasi lain di luar server perusahaan (internet).

IV. Merancang Sekuriti Jaringan

A. Strategi Merancang Sekuriti Jaringan Komputer

Dalam tulisan ini akan diuraikan strategi-strategi dasar dalam merancang sekuriti jaringan komputer. Strategi dasar ini bisa dijadikan basis untuk penerapan hingga pengembangan sekuriti sistem.

1. Hak Akses

Hak akses adalah hak yang diberikan kepada user untuk mengakses sistem. Mungkin hak akses adalah hal yang paling mendasar di bidang sekuriti. Dalam strategi sekuriti, setiap objek dalam sistem (*user*, administrator, software, sistem itu sendiri, dsb) harus diberikan hak akses yang berguna untuk menunjang fungsi kerja dari objek tersebut. Dengan kata lain, objek hanya memperoleh hak akses minimum. Dengan demikian, aksi objek terhadap sistem dapat dibatasi sehingga objek tidak akan melakukan hal-hal yang membahayakan sekuriti jaringan komputer. Hak akses minimum akan membuat para penyusup dari Internet tidak dapat berbuat banyak saat berhasil menembus sebuah *user account* pada sistem jaringan komputer. Selain itu, hak akses minimum juga mengurangi bahaya ”musuh dalam selimut” yang mengancam sistem dari dalam. Itulah beberapa keuntungan yang dapat diperoleh dari strategi ini.

Kerugian yang ada pada strategi hak akses ini adalah keterbatasan akses yang dimiliki *user* sehingga dapat menimbulkan ketidaknyamanan pada saat *user* sedang menjalankan tugasnya. Penyelesaian masalah ini bergantung kepada dua hal yaitu segi perangkat dan segi administrator jaringan dan keduanya saling berkaitan. Seorang administrator jaringan harus pandai-pandai menyiasati rancangan hak akses yang akan diberikan kepada *user* agar kebutuhan *user* dapat terpenuhi tanpa harus mengorbankan tingkat sekuriti. Bila perangkat yang dijalankan memiliki keluwesan dalam hal *setting*, hal ini akan memudahkan tugas administrator. Bila tidak, administrator harus pandai-pandai untuk menyiasatinya. Bila usaha tersebut telah maksimal dan hasilnya tetap tidak seperti yang diharapkan, ada dua pilihan yang bisa dilakukan yaitu mengganti perangkat atau memberikan pengertian kepada *user* akan keterbatasan yang ada (biasanya pilihan kedua sulit dilaksanakan). Kebutuhan *user* yang tidak terpenuhi akan dapat menimbulkan efek-efek yang kadangkala sulit diprediksi. Ia mungkin dapat berubah dari *user* biasa menjadi “musuh dalam selimut”.

2. Lapisan Sekuriti

Lapisan sekuriti adalah seberapa banyak mekanisme sekuriti yang akan digunakan dan tingkatannya. Hal ini juga menjadi pemikiran di bidang sekuriti secara umum. Kita tidak bisa mempertaruhkan seluruh sekuriti jaringan komputer pada satu mekanisme sekuriti saja. Bila satu mekanisme itu gagal melindungi sistem, habislah semua. Oleh karena itu, mekanisme sekuriti harus dibuat lebih dari satu mekanisme. Selain itu, mekanisme-mekanisme tersebut dipasang secara bertingkat/berlapis. Mekanisme sekuriti dapat berupa *network security*, *host/server security*, dan *human security*. Di antara mekanisme tersebut, dapat pula dikombinasikan sesuai dengan keperluan.

Dalam jaringan komputer, *network security* dapat dibangun dengan beberapa lapisan. Sebagai contoh, kita bisa membangun *firewall* dengan dua sub-mekanisme yaitu *packet filtering* dan *proxy system*. Mekanisme *packet filtering* pun dapat dipilah-pilah lagi menjadi beberapa bagian, seperti *filtering* berdasarkan layanan dan protokol.

Setelah lapisan pertama di atas, kita dapat pula membangun lapisan mekanisme selanjutnya. Contohnya, kita bisa menerapkan mekanisme autentifikasi pada setiap paket yang diterima.

Saat kita memberikan layanan baik ke dalam maupun ke luar jaringan, *host/server* yang memberikan layanan menjadi titik penting dalam sekuriti jaringan komputer. Pada *host security*, komponen pada *host/server* tersebut terutama perangkat lunak perlu dikonfigurasi dengan hati-hati. Layanan Internet seperti SMTP, NFS, Web Service, FTP, dlsb. hanya boleh memberikan layanan sesuai dengan yang direncanakan. Segi-segi (*features*) yang tidak utama tidak usah ditampilkan. Sebelum kita tahu pasti tingkat keamanan dari sebuah segi dalam software, sebaiknya tidak kita gunakan. Jika kita terpaksa menggunakan segi tersebut, kita dapat melakukan monitoring yang intensif terhadap segi tersebut.

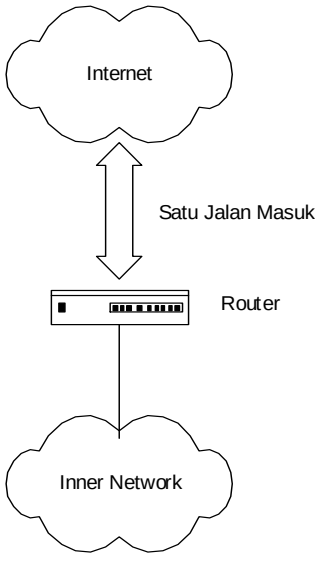
Human security menyangkut *user* dan administrator jaringan itu sendiri. Kita dapat memberikan pengarahan tentang sekuriti kepada *user* dan menanamkan sikap hati-hati ke dalam diri setiap *user*. Ada baiknya pula bila *user-user* juga ikut berpartisipasi dalam menjaga dan meningkatkan sekuriti jaringan komputer karena mereka juga bagian dari sistem itu sendiri. Dengan begitu, akan tumbuh rasa memiliki di dalam diri setiap *user*. Para administrator pun seharusnya lebih berhati-hati dalam bertugas sebab di tangan mereka sekuriti jaringan komputer diletakkan.

3. Satu Jalur Masuk

Strategi satu jalur masuk adalah cara membuat hanya satu jalan masuk menuju jaringan komputer yang kita miliki. Dengan demikian, hanya satu jalan yang perlu kita awasi dengan penuh dan ketat. Strategi ini mirip dengan membuat benteng. Benteng yang dibangun biasanya hanya akan memiliki sebuah pintu masuk dimana ditempatkan pengawasan yang paling ketat.

Inti dari strategi ini adalah pengawasan terpusat. Kita bisa mencurahkan sebagian besar daya pengawasan ke titik tersebut sehingga penyusup akan kesulitan menembus jalur tersebut. Tentunya strategi ini akan gagal apabila kita memiliki jalur masuk lain. Jika kita ingin menerapkan strategi ini sepenuhnya, usahakan tidak ada jalur masuk lain selain yang akan kita awasi ketat.

Kelemahan strategi ini adalah bila jalur masuk tersebut berhasil ditembus oleh para penyusup, ia akan langsung mengobrak-abrik jaringan komputer kita. Resiko ini dapat dikurangi dengan membuat pertahanan jalur menjadi berlapis-lapis sehingga memaksa para penyusup untuk menghentikan aksinya.



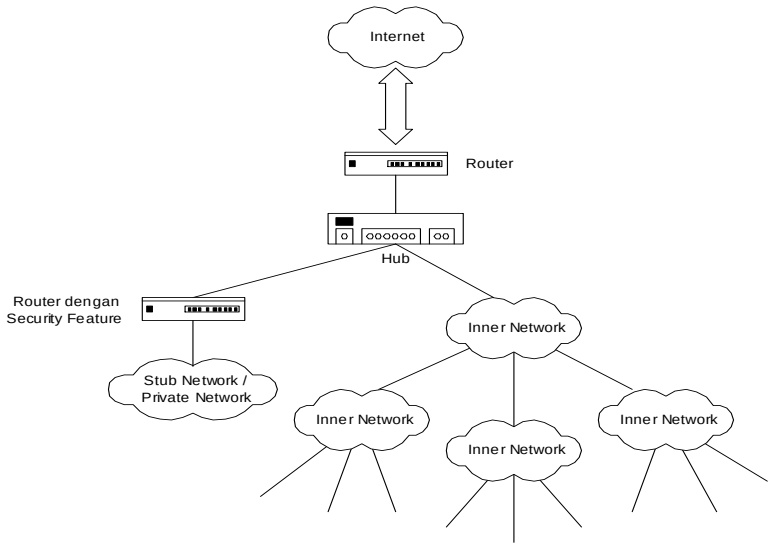
4. Enkripsi Data dan *Digital Signature*

Salah satu strategi yang paling sering digunakan dalam sekuriti jaringan adalah

enkripsi data dan *digital signature*. Digital signature menggunakan prinsip seperti tanda tangan manusia pada lembar dokumen dan dilakukan secara digital. Ia menyatakan keabsahan si pengirim data bahwa data yang dikirimkan benar-benar berasal dari si pengirim. Pada saat ini, enkripsi data dapat dilakukan di perangkat lunak maupun di perangkat keras. Berbagai jenis metoda enkripsi data pada tingkat aplikasi telah dikembangkan seperti RSA, MD-5, IDEA, SAFER, Skipjack, Blowfish, dlsb. Dengan strategi ini, transfer data dari dan ke jaringan komputer berlangsung secara konfidensial.

5. Stub Sub-Network

Stub sub-network adalah sub-jaringan komputer yang hanya memiliki satu jalur keluar masuk sub-jaringan tersebut. Strategi ini digunakan untuk mengisolasi sub-jaringan komputer yang benar-benar memerlukan perlindungan maksimal. Jalur keluar-masuk sub-jaringan tersebut diawasi dengan (bila perlu) lebih ketat daripada strategi satu jalur masuk. Contohnya, data-data rahasia perusahaan yang tersimpan dalam sebuah komputer perlu diakses secara langsung oleh beberapa bagian tertentu. Solusinya tentu saja jaringan komputer. Tetapi salah satu bagian tersebut memerlukan hubungan ke jaringan komputer perusahaan yang telah terhubung ke Internet tanpa harus pindah komputer. Nah, di sinilah strategi *stub sub-network* diperlukan. Jaringan pengakses data rahasia dirancang hanya memiliki satu jalur masuk melalui komputer yang memiliki akses Internet tersebut. Pengawasan lalu lintas data yang melalui komputer tersebut harus dipantau dengan baik dan dapat pula diberlakukan sistem *packet filtering* pada komputer tersebut.



6. Cari Titik Lemah

Sebagaimana sekuriti pada umumnya, jaringan komputer tidak terlepas dari titik-titik lemah. Titik ini akan lebih banyak tumbuh apabila jaringan komputer yang ada dikoordinir oleh lebih dari satu orang. Jaringan komputer yang besar umumnya berkembang dari jaringan-jaringan komputer yang lebih kecil yang kemudian menggabungkan diri. Selain itu, kadangkala seorang administrator akan mengalami kesulitan bila mengelola sebuah jaringan komputer skala besar seorang diri. Untuk itu, diperlukan koordinasi yang baik antar tiap administrator agar setiap jaringan yang mereka kelola terjamin sekuritinya.

7. Dua Sikap Umum

Dua sikap umum yang harus kita perhitungkan di dalam membuat rancangan jaringan komouter adalah sikap menolak secara umum (*prohibitive*) dan sikap menerima secara umum (*permissive*). Sikap menolak secara umum mendefinisikan dengan rinci layanan/paket yang diperbolehkan dan menolak lainnya. Strategi ini cukup aman tetapi kadangkala menimbulkan ketidaknyamanan pada *user*. Untuk itu, administrator yang berniat menjalankan strategi ini perlu mengetahui dengan rinci kebutuhan *user* dan seberapa jauh pengaruhnya terhadap sekuriti jaringan pada umumnya. Sikap menerima secara umum mendefinisikan dengan rinci layanan/paket yang ditolak dan menerima lainnya. Strategi ini tidak terlalu dianjurkan oleh para ahli karena dengan strategi ini kita mengambil resiko terbukanya berbagai jalan untuk merongrong sekuriti sistem.

8. Keanekaragaman Perangkat

Perangkat lunak dan keras yang ada saat ini memiliki bermacam konfigurasi dan keunggulan. Kita bisa memanfaatkan keanekaragaman perangkat-perangkat ini dalam membangun jaringan komputer kita sesuai dengan kebutuhan. Dengan adanya keanekaragaman perangkat ini, bila terjadi penyusupan terhadap sebuah komputer, ia membutuhkan usaha yang lain untuk menembus komputer yang berbeda. Sebelum kita menggunakan perangkat terutama perangkat lunak, ada baiknya bila kita juga mengetahui sejauh mana tingkat sekuriti yang disediakan oleh perangkat tersebut. Dengan begitu, kita akan memiliki data yang lengkap untuk menentukan kombinasi rancangan sekuriti jaringan komputer kita.

B. Pengamanan Jaringan Nirkabel

1. Ubahlah Sistem ID (Identitas)

Biasanya suatu layanan nirkabel dilengkapi dengan suatu standar pengamanan identitas atau yang sering disebut SSID (Service Set Identifier) or ESSID (Extended Service Set Identifier). Sangat mudah bagi seorang *hacker* untuk mencari tahu identitas default dari suatu layanan atau jaringan, jadi sebaiknya segera mengubahnya menjadi suatu identitas yang unik, yang tidak mudah ditebak orang lain.

2. Mematikan identitas pemancar

Dengan membertahukan bahwa pengguna memiliki suatu jaringan nirkabel akan membuat para hacker penasaran untuk membobol jaringan nirkabel pengguna. Mempunyai suatu jaringan nirkabel bukan berarti harus memberitahukannya kepada semua orang. Perangkat yang dipakai keras dapat diperiksa secara manual perangkat pada jaringan nirkabel tersebut, dan

dapat dipelajari bagaimana cara mematikannya.

3. Sediakanlah enkripsi

WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) dapat meng-enkripsi data pengirim sehingga hanya penerima saja yang diharapkan dapat membaca data tersebut. WEP (Wired Equivalent Privacy) mempunyai banyak kelemahan yang membuatnya mudah disusupi. Kunci 128-bit hanya mempunyai tingkat pencapaian yang relatif rendah tanpa peningkatan keamanan yang signifikan, sedangkan untuk 40-bit atau 64-bit pada beberapa perlengkapan lainnya, mempunyai enkripsi yang sama baiknya. Dengan cara pengamanan yang standart saja pastilah tetap akan mudah bagi hacker untuk menyusup, namun dengan cara enkripsi ini pastilah akan membuat jaringan pengguna lebih aman dari hacker. Jika memungkinkan, ada baiknya untuk menggunakan enkripsi WPA (peralatan yang lebih tua dapat diupgrade terlebih dahulu agar compatible dengan WPA). WPA dapat sangat menjanjikan dalam menjamin keamanan jaringan nirkabel Anda, namun masih tetap dapat dikalahkan oleh serangan DOS (denial of services).

4. Membatasi dari penggunaan traffic yang tidak perlu

Banyak router jaringan kabel maupun nirkabel yang dilengkapi firewalls. Bukan bermaksud mengedepankan firewalls, namun firewalls telah membantu dalam pertahanan keamanan jaringan. Bacalah petunjuk manual dari perangkat keras dan pelajarilah cara pengaturan konfigurasi router, sehingga hanya traffic yang sudah mendapatkan ijin saja yang dapat dijalankan.

5. Ubahlah 'kata sandi' default Administrator milik Anda

Hal ini baik untuk semua penggunaan perangkat keras maupun perangkat lunak. Kata sandi default sangat mudah disalahgunakan, terutama oleh para hacker. Oleh karena itu sebaiknya ubahlah kata sandi Anda, hindari penggunaan kata dari hal-hal pribadi Anda yang mudah diketahui orang, seperti nama belakang, tanggal lahir, dan sebagainya.

6. Kunci dan lindungilah komputer Anda

Hal ini merupakan cara pengamanan terakhir untuk komputer Anda. Gunakanlah firewall, perangkat lunak Anti Virus, Zone Alarm, dan lain sebagainya. Setidaknya setiap satu minggu perbaharuilah Anti Virus yang Anda pakai.

DAFTAR PUSTAKA

Chapman, D.B & Zwicky, E.D.; *Building Internet Firewalls*; O'Reilly & Associates; Inc., 1995

Cheswick, W.R & Bellovin, S.M.; *Firewalls and Internet Security*; Addison-Wesley Publishing Co.; 1994

Scarfone, Karen; Hoffman Paul; *Guidelines on Firewalls and Firewall Policy*; National Institute of Standards and Technology; Guithersburg; 2009

Stiawan, Deris; Sistem Keamanan Komputer; PT. Elex Media Komputindo; Jakarta; Cetakan ke Dua; 2006

Syafrizal, Melwin; Pengantar Jaringan Komputer; CV. Andi offset; Yogyakarta; 2005

_____; Tips Jitu Optimalisasi Jaringan Wifi; CV. Andi Offset; Semarang; 2010

Zwicky, Elisabeth D.; Cooper, Simon & Chapman, D. Brent; *Building Internet Firewalls;* 2nd Edition; O' Reilly & Associates Inc.; USA; 2000

*) Penulis adalah Widyaiswara PPSDM MIGAS