KEAMANAN JARINGAN NIRKABEL

Penggunaan jaringan Internet yang kian marak dewasa ini telah mendorong pertumbuhan teknologi koneksi jaringan Internet itu sendiri, sehingga kemudian lahirlah suatu teknologi jaringan nirkabel *(Wireless Network)*, yang sangat memudahkan penggunanya dalam mengakses Internet. Namun begitu ada beberapa hal yang harus diperhatikan agar dalam penggunaan jaringan nirkabel ini dapat berjalan dengan aman.

Lahirnya Jaringan Nirkabel untuk Rumah

Dahulu komputer lebih dianggap sebagai sebuah kemewahan daripada sebuah kebutuhan. Hanya orang-orang kaya dan beruntung saja yang dapat mempunyai sebuah komputer, sedangkan jaringan merupakan hal yang hanya dapat disediakan untuk perusahaan besar.

Namun sejalan dengan kemajuan yang pesat pada dekade ini, maka sekarang setiap orang masing-masing dapat mempunyai komputernya sendiri. Seperti yang banyak kita temui, biasa nya setiap orang tua mempunyai komputernya sendiri, begitu pula dengan si anak dapat mempunyai komputernya sendiri walaupun mungkin hanya digunakan untuk bermain dan mengerjakan tugas-tugas sekolah. Para pengguna rumahan juga telah berkembang dari yang semula tidak mempunyai akses Internet, kemudian mulai memakai koneksi *dial-up* Internet dengan kecepatan 9600 kbps melebihi 56 kbps *dial up* akses, dan kini berkembang menjadi koneksi *broadband* menyaingi koneksi T1 yang sering dinikmati orang saat bekerja.

Sebagaimana Internet dan *World Wide Web* telah menjadi *trend* dalam kebudayaan kita dan menggantikan format media massa lainnya dalam menyampaikan informasi yang dicari, mulai dari informasi pemberitaan, olahraga, cuaca, resep, *yellow* pages (buku telepon), dan masih banyak hal lainnya yang kesemuanya itu merupakan sebuah cara baru, bukan hanya dalam pemakaian komputer di dalam rumah, tapi juga dalam hal pemakaian koneksi Internet.

Sementara itu perusahaan perangkat keras maupun perangkat lunak kini telah menawarkan berbagai solusi yang memungkinkan para pemakai Internet di rumah saling berbagi koneksi antara lebih dari dua komputer. Meskipun semua komputer tersebut harus terhubung jaringan.

Untuk menghubungkan satu komputer dengan komputer yang lainnya biasanya membutuhkan berbagai macam media fisik, seperti kabel telepon, kabel *coaxial*, ataupun kabel CAT5 kabel telegram yang ada di mana-mana. Namun baru-baru ini telah ditemukan cara baru pemakaian Internet tanpa menggunakan berbagai macam media penghubung terseut, teknologi ini kini lazim disebut koneksi jaringan Nirkabel (tanpa kabel). Pemakaian Internet dengan menggunakan koneksi jaringan nirkabel ini tentu saja sangat memudahkan pemakainya dalam

mengakses Internet, tanpa melalui proses installasi dan pemasangan kabel yang memusingkan.

Adapun susunan koneksi jaringan nirkabel ini sangat sederhana. Koneksi Internet masuk dari *Internet* Provider kemudian dihubungkan dengan suatu titik penerus akses nirkabel atau *router* yang memancarkan sinyal. Ketika Anda terhubung dengan memakai kartu atau antena jaringan nirkabel untuk menerima sinyal, begitu pula sebaliknya, maka koneksi Anda telah berhasil.

Masalah yang sering timbul pada saat menikmati koneksi sinyal nirkabel ini adalah sulitnya mengetahui sampai sejauh mana sinyal ini dapat diterima. Jika sinyal tersebut dapat ditangkap dari lantai atas sebuah kantor, maka seharusnya juga dapat ditangkap dari basement yang berada 100 kaki di bawah tanah. Ini dapat saja membuat seorang *hacker* mencari celah dari koneksi nirkabel tersebut untuk mendapatkan berbagai informasi penting mengenai Anda.

Namun itu bukan berarti tidak menyarankan penggunaan jaringan nirkabel. Hanya saja Anda harus cermat dalam menggunakan jaringan nirkabel ini, serta mengambil beberapa pencegahan dasar agar pemakaian teknologi ini dapat benar-benar aman. Berikut ini merupakan beberapa langkah sederhana yang dapat dijalankan untuk mengamankan jaringan nirkabel yang Anda pakai.

6 Langkah Pengamanan Dasar Jaringan:

1. Ubahlah Sistem ID (Identitas). Biasanya suatu layanan nirkabel dilengkapi dengan suatu standart pengamanan identitas atau yang sering disebut SSID (Service Set Identifier) or ESSID *(Extended Service Set Identifier)*. Sangat mudah bagi seorang *hacker u*ntuk mencari tahu identitas *default* dari suatu layanan atau jaringan, jadi sebaiknya Anda segera mengubahnya menjadi suatu identitas yang unik, yang tidak mudah ditebak orang lain.
2. Mematikan identitas pemancar. Dengan mengumumkan kepada umum bahwa Anda memiliki suatu jaringan nirkabel akan membuat para *hacker* penasaran untuk membobol jaringan nirkabel Anda. Mempunyai suatu jaringan nirkabel bukan berarti harus memberitahukannya kepada semua orang. Periksalah secara manual perangkat keras yang Anda pakai untuk jaringan nirkabel tersebut, dan pelajarilah bagaimana cara mematikannya.
3. Sediakanlah enkripsi. WEP *(Wired Equivalent Privacy)* and WPA *(Wi-Fi Protected Access)* dapat meng-enkripsi data Anda 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 Anda lebih aman dari *hacker.* Jika memungkinkan, ada baiknya untuk menggunakan enkripsi WPA (peralatan yang lebih tua dapat di*upgrade* 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 Anda dan pelajarilah cara pengaturan konfigurasi *router* Anda, sehingga hanya *traffic* yang sudah seijin Anda 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.('dna)