**Setting Security pada Wireless**

**Iman Wibisono**

*Iman.wibi@yahoo.co.id*

*http://hahaiseng.blogspot.com*

***Lisensi Dokumen:***

*Copyright © 2003-2007 IlmuKomputer.Com*

*Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.*

Wireless tidak membutuhkan kabel yang terkadang sangat sulit untuk dipasang, namun kemudahan ini juga harus dibayar dengan permasalahan keamanan yang lebih kritis karena media udara merupakan media publik yang tidak bisa dikontrol. Bagaimana jaringan wireless melindungi dirinya dari masalah semacam ini ?

Untuk menggunakan jaringan kabel, Anda harus menghubungkan kabel UTP ke dalam port hub/switch. Setelah terhubung Anda langsung mempunyai hak untuk mengirimkan ataupun menerima data melalui hub/switch tersebut. Bagaimana bila ada orang asing yang membawa kabel UTP sendiri kemudian ia menghubungkan komputernya dengan hub/switch ? Yah, orang tersebut otomatis secara fisik sudah terhubung ke dalam jaringan Anda, ia bisa mengirimkan data ke semua komputer, ia bisa mengintip paket-paket data yang ada di dalam jaringan dan lain sebagainya.

Fada jaringan kabel Anda bisa berdalih”saya mempunyai peraturan yang sangat ketat sehingga tidak semua orangbisa memasukkan kabel ke dalam switch”. Anda mungkin benar walaupun saya tidak yakin sama sekali, lalu bagaimana dengan koneksi wireless ? Bagaimana koneksi wireless mengamankan data yang lalu-lalang di udara ? Bisakah Anda menjaga data yang ada di udara agar tidak dicuri ?

Berikut adalah 5 langkah cepat untuk membantu Anda mengamankan jaringan wireless / nirkabel Anda dari akses yang tidak sah. Langkah-langkah ini disediakan sebagai pedoman umum. bantuan rinci, silakan hubungi vendor perangkat keras Anda. Lihat bagian bawah halaman ini untuk link ke beberapa vendor jaringan nirkabel umum.

1. Download firmware terbaru untuk perangkat Anda.  
2. Mengubah password administrator.  
3. Ubah SSID Anda dan nonaktifkan SSID Broadcasting  
4. Aktifkan WPA / WPA2  
5. Batasi akses dengan alamat MAC ( MAC Address )

**1. Download firmware terbaru untuk router nirkabel Anda.**

Firmware adalah software yang tertanam dalam sebuah perangkat keras – dalam hal ini, router nirkabel Anda. Firmware yang datang dengan router nirkabel Anda atau jalur akses nirkabel dapat kadaluarsa. Download firmware terbaru untuk menjamin keamanan dan kinerja terbaik.

Berbagai kerentanan keamanan ditemukan, patch untuk menghentikan mereka lalu dikembangkan. Patch ini sering disertakan dalam update firmware. Jika Anda menggunakan firmware default yang datang dengan router nirkabel Anda, mungkin ada beberapa lubang keamanan yang dikenal yang dapat memungkinkan seseorang untuk membajak koneksi Internet Anda, melihat file pada setiap komputer jaringan Anda dan bahkan mencuri password atau nomor kartu kredit.

Sebagian besar router nirkabel saat ini memungkinkan untuk mengupdate firmwarenya , dan proses ini cukup sederhana. Periksa situs web untuk produsen perangkat nirkabel Anda untuk instruksi mendapatkan firmware terbaru dan bagaimana cara menginstalnya. Situs dukungan Linksys  dapat ditemukan di sini dan situs dukungan Netgear dapat ditemukan di sini. situs vendor dukungan hardware tambahan dapat ditemukan di bagian bawah halaman ini.

**2. Mengubah sandi administrator**

Password default, atau password asli router nirkabel Anda harus segera diganti. Semua router nirkabel dikirimkan dengan nama pengguna administrator dan password yang sama. Mengubah nama pengguna dan sandi tidak hanya untuk perubahan yang paling penting, adalah yang paling mudah. Pada halaman konfigurasi router nirkabel Anda, cari link atau pengaturan berjudul “Admin” Jika Anda memiliki kesulitan mengubah pengaturan ini., Periksa panduan pengguna router nirkabel Anda.

**3. Ubah SSID Anda dan nonaktifkan SSID Broadcasting**

Router wireless / nirkabel Anda dilengkapi dengan default SSID (nama jaringan nirkabel), dan salah satu hal pertama yang harus Anda lakukan adalah mengubah nama SSID itu. Dengan memiliki SSID non-standar, Anda bisa mempersulit untuk koneksi yang tidak sah ke jaringan Anda.

Dengan membiarkan SSID Anda untuk menyiarkan sinyal wireless, ia memudahkan Anda untuk menambahkan perangkat tambahan untuk jaringan nirkabel Anda. Namun, Anda juga membuatnya mudah bagi siapa saja dengan perangkat nirkabelnya untuk mendapatkan akses ke jaringan Anda. Membiarkan aksi penyiaran ini layaknya seperti meninggalkan kunci mobil Anda di mesin mobil yang masih menyala pada saat Anda berjalan kedalam toko.

Bila Anda menonaktifkan SSID broadcasting, perangkat nirkabel Anda harus dikonfigurasikan dengan SSID yang sama pada settingan yang ditetapkan di router nirkabel Anda. Jadi tidak ada yang tahu bahwa kita mempunyai jaringan wireless sendiri.

**4. Aktifkan WPA / WPA2**

Kebanyakan kartu nirkabel baru dan router mendukung keamanan wireless jenis WPA atau WPA2. Pakailah salah satunya yang Anda yakinkan semua hardware anda mendukung untuk ini. metode WEP tidak lagi dianggap sebagai cara yang aman untuk mengamankan data Anda.

**5. Batasi akses dengan alamat MAC ( MAC Address )**

Setiap kartu jaringan, baik kabel dan nirkabel, memiliki sebuah alamat unik yang diberikan untuk itu dari produsen hardwaenya. Tanda pengenal ini disebut alamat MAC. Dengan pengaturan router nirkabel yang Anda hanya mengizinkan koneksi dari alamat MAC tertentu, Anda sangat meningkatkan keamanan jaringan nirkabel Anda. Untuk membantu mencari tahu apa kartu jaringan anda, alamat MAC, lihatlah FAQ. Setelah Anda mengetahui setiap alamat MAC untuk kartu jaringan Anda, kunjungi dukungan situs Web produsen router nirkabel untuk mendapatkan petunjuk tentang cara menggunakan keamanan alamat MAC.

**Biografi Penulis**

**Nur Iman Wibisono**. Berdomisili di Semarang sejak lahir hingga sekarang. Sedang melanjutkan pendidikan D3 di Politeknik Negeri Semarang Program Studi Teknik Telekomunikasi. Tertarik dengan komputer khususnya networking dan pemrograman.