Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

- **Jaringan Nirkabel Anda**
- **Peralatan Anda**

Mengamankan Jaringan Di Rumah

Sekilas

Beberapa tahun lalu, jaringan di rumah tergolong sederhana, lazimnya tidak lebih dari jaringan nirkabel ditambah satu atau dua komputer untuk menjelajah internet, berbelanja online atau bermain game. Belakangan ini jaringan di rumah berkembang menjadi semakin rumit. Banyak peralatan baru terhubung ke jaringan dan digunakan tidak sekedar untuk menjelajah internet atau sarana tontonan saja. Dalam edisi ini akan dibahas bagaimana cara menciptakan jaringan yang aman di rumah bagi Anda dan seluruh keluarga.

Editor Tamu

CherylConley adalah pimpinan Security Education and Awareness di Lockheed Martin, menggelontorkan program The I Campaign™ ke 100.000 karyawan. Ini mencakup kerja sama dan penyuluh diskusi kelompok di dalam perusahaan selain program global phishing. Cheryl hadir di **@conleychera**.

Jaringan Nirkabel Anda

Hampir setiap jaringan di rumah diawali dengan jaringan nirkabel (disebut juga jaringan Wi-Fi). Ini menjadikan setiap peralatan terhubung tanpa kabel ke jaringan Internet, mulai dari laptop dan tablet hingga peralatan game dan televisi. Umumnya jaringan nirkabel dikendalikan oleh router internet yang dipasang oleh penyedia jasa layanan internet di rumah Anda. Namun, dibeberapa situasi, jaringan nirkabel Anda dikendalikan oleh sistem lain yaitu Titik Akses Nirkabel (wireless access point) yang dihubungkan ke router internet. Tidak peduli mana yang dipakai, semuanya memancarkan sinyal nirkabel. Beragam peralatan di rumah Anda tersambung melalui sinyal ini. Dengan cara ini semua peralatan bisa terhubung ke internet sekaligus tersambung kesemua peralatan yang ada di jaringan rumah. Artinya, menjaga keamanan jaringan nirkabel merupakan hal penting dalam perlindungan rumah Anda. Dibawah ini ada beberapa langkah yang penting untuk disimak.

- Ubah sandi administrator di router internet atau titik akses nirkabel yang mengendalikan jaringan nirkabel. Akun admin memberi Anda kewenangan untuk melakukan konfigurasi jaringan nirkabel. Banyak router internet dikirim ke pelanggan dengan disertai login admin dan sandi yang diketahui banyak orang dan malah sering juga diunggah ke internet. Untuk itu, pastikan untuk mengubah sandi admin serta gunakan sandi yang kuat, unik serta hanya Anda yang tahu.

Mengamankan Jaringan Di Rumah

Untuk melindungi jaringan di rumah, amankan jaringan nirkabel, perbarui dan gunakan sandi disetiap peralatan di jaringan.

- Ubah nama jaringan nirkabel (dikenal juga sebagai SSID). Ini merupakan nama jaringan yang dikenal peralatan pada saat mencari jaringan nirkabel. Beri nama yang unik agar mudah dikenali, namun pastikan tidak mengandung informasi pribadi. Tidak banyak gunanya menyembunyikan nama jaringan tersebut karena nama jaringan dengan mudah bisa dilacak dengan bantuan berbagai peralatan pemindai jaringan atau oleh orang yang ahli dibidangnya.
- Pastikan hanya orang terpercaya yang bisa terhubung dan menggunakan jaringan nirkabel serta yakinkan koneksi terenkripsi. Lakukan ini dengan mengaktifkan sistem keamanan yang kuat. Saat ini pilihan terbaik mekanisme keamanan dikenal sebagai WPA2. Dengan mengaktifkannya, setiap orang yang hendak terhubung akan diminta memasukkan sandi serta setiap sambungan akan dienkripsi. Jangan gunakan metode keamanan lama seperti WEP atau bahkan tidak menggunakannya sama sekali (jaringan terbuka). Jaringan terbuka memperbolehkan siapa saja terhubung ke jaringan tanpa proses otentifikasi.
- Pastikan menggunakan sandi yang kuat dan berbeda dengan sandi admin. Ingat, biasanya hanya perlu satu kali saja memasukkan sandi disetiap peralatan, selanjutnya sandi tersebut akan tersimpan di dalam peralatan tersebut.
- Banyak jaringan nirkabel menyediakan jaringan khusus untuk tamu (Guest Network). Ini memungkinkan tamu tersambung ke internet tapi tetap memberikan perlindungan ke jaringan rumah sehingga tamu tersebut tidak bisa tersambung ke peralatan di rumah. Bila ada fitur jaringan tamu, jangan lupa mengaktifkan WPA2 dan juga menggunakan sandi yang unik.
- Non aktifkan WiFi Protected Setup atau mekanisme lain yang memperbolehkan sebuah perangkat terhubung ke jaringan tanpa sandi dan pilihan konfigurasi.
- Bila dirasa susah mengingat beragam sandi, disarankan untuk menggunakan pengelola sandi (password manager) sebagai sarana penyimpan.

Kurang paham cara melakukan berbagai langkah diatas? Coba hubungi penyedia jasa layanan internet, pelajari dokumentasi router internet atau titik akses nirkabel, bisa juga kunjungi situs webnya.

Mengamankan Jaringan Di Rumah

Peralatan Anda

Langkah berikutnya adalah mengetahui apa saja yang tersambung ke jaringan rumah dan memastikan semua peralatan tersebut aman. Dulu mudah sekali melakukan hal ini karena cuma segelintir peralatan yang terhubung. Sekarang dijaman dimana semua selalu terkoneksi, apa saja bisa terhubung ke jaringan rumah, mulai dari TV, peralatan game, monitor bayi, pengeras suara, pengatur suhu dan bahkan mungkin mobil Anda. Satu cara termudah untuk mengetahui apa saja yang tersambung ke jaringan rumah adalah menggunakan pemindai sederhana seperti Fing. Aplikasi yang bisa dijalankan di komputer atau alkom, berfungsi dengan cara memindai jaringan nirkabel dan melaporkan peralatan apa saja yang tersambung. Setelah semua peralatan yang tersambung ke jaringan rumah diketahui, perlu dipastikan bahwa setiap peralatan tersebut sudah aman. Cara paling gampang adalah dengan menjamin bahwa setiap peralatan menggunakan versi terbaru sistem operasi/firmware. Jika memungkinkan, aktifkan fasilitas pembaruan otomatis. Bila ada peralatan yang memerlukan sandi, pakailah sandi yang unik dan kuat. Selain itu, kunjungi situs web penyedia jasa internet Anda, mungkin saja ada beberapa fasilitas tambahan yang bisa dipakai untuk mengamankan jaringan rumah.

Selanjutnya

Untuk berlangganan buletin bulanan OUCH! Kesadaran Keamanan, mengakses arsip buletin OUCH! dan mengetahui lebih banyak solusi kesadaran keamanan SANS, silakan kunjungi http://www.securingthehuman.org.

Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: http://www.bipimax.net

Sumber Pustaka

Frasa Sandi:	https://securingthehuman.sans.org/ouch/2015#april2015
Manager Sandi:	https://securingthehuman.sans.org/ouch/2015#october2015
Mengamankan Tablet Anda:	https://securingthehuman.sans.org/ouch/2016#january2016
Pemetaan Jaringan Rumah Anda:	http://l.rud.is/home-network-mapping

Dewan Redaksi: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Diterjemahkan oleh: T. Gunawan