OUCH! | Februari 2015

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Aman Bekerja di Perjalanan

Sekilas

Bahasan kali ini adalah bagaimana Anda bisa tersambung ke internet dan bekerja dengan aman pada saat bepergian/ dalam perjalanan.

Editor Tamu

Steve Amstrong adalah Technical Director CyberCPR di Logically Secure, instruktur bersertifikat SANS dan perancang pelatihan di SANS. Aktif di Twitter sebagai **@Nebulator** dan di Google plus sebagai **+SteveAmstrongSecurity**.

Persiapan

Meskipun jaringan komputer di rumah atau kantor boleh dibilang aman, pada saat bepergian Anda tidak boleh percaya begitu saja pada semua koneksi jaringan komputer yang ada. Anda tidak pernah tahu siapa yang pernah menggunakannya dan bahaya apa yang mungkin ada. Beberapa persiapan sebelum melakukan perjalanan akan bermanfaat dalam melindungi data Anda. Satu atau dua minggu sebelum perjalanan, lakukan hal sbb:

- Tentukan dan singkirkan data yang tidak diperlukan dari peralatan yang dibawa. Ini bertujuan untuk mengurangi dampak yang mungkin terjadi bila peralatan tersebut hilang atau ditahan (disita) petugas bea cukai atau kemanan. Dalam perjalanan bisnis, mintalah atasan Anda agar menyediakan peralatan yang khusus digunakan pada saat bepergian.
- Untuk perjalanan internasional, pelajari jenis colokan/steker listrik di negara tujuan, mungkin diperlukan adaptor listrik tambahan. Selain itu, pelajari jenis jasa layanan telepon yang disediakan oleh penyedia jasa komunikasi Anda. Tidak jarang penyedia jasa komunikasi memasang tarip tinggi pemakaian di luar negeri, Anda malah mungkin berpikir untuk menghentikan jasa layanan data telepon genggam selama bepergian ke negara lain, atau pilihlah jenis layanan yang sesuai dengan kebutuhan perjalanan luar negeri.
- Pasang perangkat lunak yang bisa melacak keberadaan perangkat Anda dan bahkan melakukan penghapusan data, jika peralatan tersebut hilang atau dicuri. Banyak peralatan komunikasi yang memiliki fasilitas diatas, Anda hanya perlu mengaktifkannya saja (ingat, untuk ini diperlukan akses internet).

Satu atau dua hari sebelum perjalanan

Aman Bekerja di Perjalanan

- Perbarui peralatan, aplikasi dan anti-virus agar terpasang versi terbaru.
- Aktifkan pengaturan keamanan yang dibutuhkan, misalnya firewalls.
- Lindungi alat komunikasi dengan kunci sandi yang kuat. Dengan cara ini, bila peralatan tersebut hilang atau dicuri, orang lain tidak akan bisa mengakses informasi di dalamnya.
- Lakukan enkripsi data agar pada saat hilang atau dicuri, data tidak dapat diakses. Beberapa peralatan seperti iPhones melakukan hal ini secara otomatis pada saat Anda memasang sandi atau passcode.
- Lakukan backup peralatan. Jika sesuatu terjadi pada peralatan tersebut selama dalam perjalanan, semua data masih ada dan tersimpan ditempat aman.

Agar tetap aman saat bepergian adalah dengan menyiapkan semua peralatan dengan baik sebelum berangkat, menjaga keamanan peralatan tersebut dan melakukan enkripsi disemua aktifitas online.

Peralatan Hilang / Dicuri

Dalam perjalanan, jaga keamanan semua peralatan. Misalnya, jangan pernah meninggalkan peralatan di dalam mobil dan bisa dilihat dari luar, dengan hanya memecahkan kaca mobil, penjahat bisa mengambil semua barang berharga didalamnya. Bisa juga menggunakan kabel berkunci (cable lock) untuk mengikat peralatan Anda, seperti misalnya laptop, pada saat ditinggalkan. Walaupun tindak kejahatan bisa terjadi setiap saat, namun Anda perlu tahu bahwa ternyata kasus peralatan hilang lebih banyak terjadi dibanding kasus pencurian. Berdasar penelitian Verizon selama periode sepuluh tahun, kemungkinan seseorang kehilangan peralatan adalah 15x lebih besar dibanding pencurian. Oleh sebab itu, upayakan tidak sembrono dalam membawa peralatan saat bepergian seperti pada waktu melewati pemeriksaan keamanan di lapangan udara, saat meninggalkan taxi atau restoran, keluar dari hotel atau saat sebelum melangkah ke dalam pesawat terbang.

Akses Wi-Fi

Pada saat bepergian sering kali akses internet dilakukan melalui titik akses Wi-Fi umum, seperti yang ditemui di lobby hotel, café atau lapangan terbang. Persoalan dengan titik akses Wi-Fi umum adalah ketidak-jelasan pemilik peralatan tersebut serta juga siapa saja yang terhubung. Itulah sebabnya, peralatan seperti itu dikategorikan sebagai peralatan tidak aman, sebenarnya justru karena hal-hal seperti inilah yang menjadikan Anda melakukan banyak langkah untuk menyiapkan peralatan yang aman digunakan sebelum berangkat. Selain itu, Wi-Fi menggunakan gelombang radio sebagai media komunikasi antara sebuah peralatan dan titik akses nir-kabel. Artinya, siapa saja yang dekat dengan Anda berpotensi mencegat dan mengawasi komunikasi yang terjadi.

Aman Bekerja di Perjalanan

Bila Anda menggunakan Wi-Fi umum, pastikan semua aktifitas online terenkripsi. Sebagai contoh,pada saat melakukan jelajah internet, pastikan website yang dikunjungi terenkripsi (akan tampil “https://’ disebelah alamat url dan tampil gambar gembok terkunci). Selain itu bisa juga gunakan akun VPN (Virtual Private Network) yang akan melakukan enkripsi semua aktifitas online Anda. Ini bisa disediakan oleh perusahaan dimana Anda bekerja atau membelinya sendiri untuk keperluan pribadi. Bila Anda kuatir tidak ada akses Wi-Fi yang aman, bisa juga menggunakan telepon genggam. (Ingat: tagihan bisa mahal sekali khususnya di perjalanan internasional, periksa dulu tarif dan ketentuannya).

Fasilitas Umum

Jangan gunakan komputer umum, seperti yang ada di lobby hotel, perpustakaan atau café siber. Anda tidak pernah tahu siapa pengguna komputer itu, bisa saja komputer tersebut tanpa sengaja sudah terinfeksi atau memang sengaja dibuat terinfeksi. Sebisa mungkin gunakan peralatan yang jelas-jelas aman untuk melakukan aktifitas online. Bila harus menggunakan komputer umum, jangan melakukan aktifitas yang mengharuskan login atau memasukkan sandi.

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

Sandi:	http://www.securingthehuman.org/ouch/2013#may2013
Verifikasi Dua Langkah:	http://www.securingthehuman.org/ouch/2013#august2013
Enkripsi:	http://www.securingthehuman.org/ouch/2014#august2014
Amankan Tablet Anda:	http://www.securingthehuman.org/ouch/2013#december2013
Verizon DBIR 2014:	http://www.verizonenterprise.com/DBIR/2014/

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