Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

- Sekilas
- Lima Langkah Utama

5 Langkah Tetap Aman

Sekilas

Seiring dengan meningkatnya peran teknologi dalam kehidupan manusia, teknologi juga menjadi semakin komplex. Ditengah perubahan teknologi yang demikian cepat, upaya untuk terus mengikuti beragam petunjuk pengamanan bisa membingungkan. Sepertinya selalu muncul petunjuk baru mengenai apa yang harus dilakukan atau dihindari. Walaupun langkah detil untuk tetap aman bisa berganti kapan saja namun ada beberapa hal mendasar yang selalu bisa diterapkan. Apapun teknologi yang dipakai dan dimanapun digunakan, simak lima (5) langkah utama ini dibawah ini.

Editor Tamu

Lenny Zeltser fokus pada pengamanan kegiatan IT pelanggan di NCR Corp serta pengajar penangkalan malware di Sans Institute. Lenny aktif di Twitter sebagai **@lennyzeltser** dan penulis blog keamanan komputer di **blog.zeltser.com**.

Lima Langkah Utama

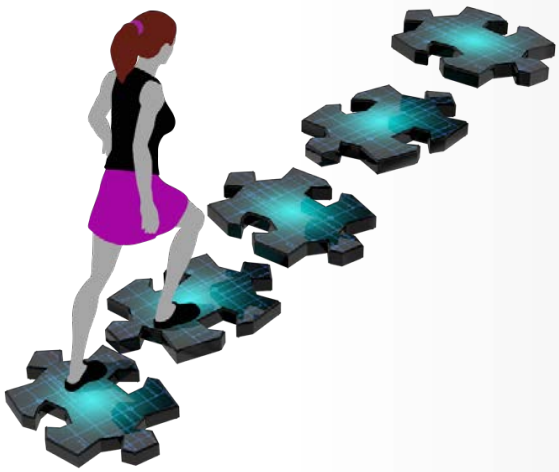
Setiap pokok bahasan dibawah ini hanya berupa ulasan singkat. Untuk mendapatkan bahasan yang lebih mendalam, simak sumber pustaka yang tercantum di bagian bawah buletin ini.

1. **Anda**: Penting untuk diingat bahwa teknologi itu sendiri tidak bisa memberikan perlindungan. Cara paling mudah bagi seorang peretas untuk membobol teknologi pengamanan adalah melalui Anda. Bila peretas ingin mendapatkan informasi sandi atau kartu kredit, cara termudah adalah dengan melakukan aksi tipuan agar Anda mau mengungkap informasi tersebut. Contohnya adalah dengan berpura-pura sebagai tenaga layanan teknis Microsoft dan menyatakan bahwa komputer Anda terinfeksi virus, padahal sebenarnya mereka adalah kriminalis siber yang ingin mendapatkan askes ke komputer Anda. Bisa juga mereka mengirimkan surel untuk menjelaskan pesanan yang tidak terkirim dan meminta Anda mengklik tautan (link) untuk melakukan konfirmasi alamat, padahal mereka berupaya menggiring Anda ke sebuah website yang siap melakukan peretasan. Pada akhirnya, pertahanan terampuh adalah Anda. Jangan mudah terperdaya, gunakan akal sehat untuk bisa mengenal dan menangkal bermacam ragam pengelabuan itu.

2. **Pembaruan**: Pastikan semua komputer, alat komunikasi, program aplikasi dan lainnya yang terhubung ke jaringan selalu menggunakan versi teranyar perangkat lunak. Kriminalis siber terus menerus mencari titik lemah disetiap teknologi yang Anda pakai. Saat ditemukan sebuah titik lemah, mereka akan menggunakan program

5 Langkah Tetap Aman

aplikasi khusus untuk memanfaatkan kelemahan itu dan meretas teknologi apapun yang dipakai termasuk jaringan, komputer dan alat komunikasi. Sementara itu, perusahaan pencipta teknologi tersebut akan berupaya keras agar produknya selalu mutakhir (up-to-date). Bila ditemukan kerentanan maka akan disiapkan program penyempurna (patch) untuk disebar ke publik. Dengan memastikan bahwa komputer dan peralatan komunikasi sudah diperbarui maka celah kelemahan bisa dikurangi dan bakal mempersulit siapapun dalam melakukan peretasan. Agar selalu terperbarui, aktifkan fasilitas pembaruan otomatis (auto update). Lakukan hal ini pada semua perangkat teknologi yang tersambung ke jaringan termasuk TV internet, alat monitor bayi, router rumah, peralatan permainan elektronik dan bahkan suatu saat mobilpun harus mendapat perlakuan yang sama. Jika sistem operasi komputer, alat komunikasi atau lainnya sudah tidak lagi mendapatkan dukungan layanan dan tidak bakal mendapatkan pembaruan lagi, disarankan untuk berpindah ke versi yang masih mendapatkan dukungan layanan.



Dengan patuh pada lima langkah utama ini, Anda akan senantiasa terlindungi sejalan dengan perkembangan teknologi.

3. **Sandi**: Langkah pengamanan selanjutnya adalah penggunaan sandi yang kuat dan unik disetiap piranti/ peralatan, akun online dan program aplikasi. Garis bawahi kata kuat dan unik. Sandi yang kuat berarti tidak mudah ditebak oleh peretas dan program otomatisnya. Jangan memakai kata tunggal, sebagai gantinya gunakan kalimat yang terbentuk dari beberapa kata serta dilengkapi dengan simbol dan bilangan didalamnya. Unik artinya setiap peralatan dan akun online menggunakan sandi yang berbeda. Dengan cara ini, bila salah satu akun diretas, akun dan peralatan lainnya masih tetap aman. Tidak sanggup menghafal demikian banyak kombinasi sandi? Jangan kuatir, semua orang juga berpikiran begitu. Atasi dengan menggunakan pengelola sandi (password manager), sebuah aplikasi khusus untuk alat komunikasi atau komputer yang berfungsi menyimpan semua sandi dalam bentuk terenkripsi. Selain itu, bila akun Anda memiliki fasilitas verifikasi dua tahap, gunakan fasilitas itu untuk mendapatkan perlindungan yang lebih baik.

4. **Enkripsi**: Saran berikutnya adalah penggunaan enkripsi. Enkripsi memastikan bahwa hanya Anda dan orang tertentu saja yang bisa mengakses informasi Anda. Data bisa dienkripsi dalam dua kondisi: kondisi statis atau transisi. Enkripsi statis bertujuan memberikan perlindungan pada saat informasi disimpan di hard-disk atau USB. Kebanyakan sistem operasi memungkinkan enkripsi seluruh data dengan menggunakan fasilitas Full Disk

5 Langkah Tetap Aman

Encryption. Aktifkan fasilitas ini bila tersedia. Enkripsi data transisi akan mengenkripsi data pada saat proses transmisi dari sebuah komputer ke peralatan lain, contohnya adalah pada saat menggunakan jasa online perbankan. Cara mudah memastikan bahwa enkripsi ini sudah aktif pada saat browsing adalah dengan memperhatikan penggunaan “https:” di alamat website yang dikunjungi serta adanya simbol kunci/gembok disebelahnya.

5. **Backup**: Terkadang, walaupun sudah sangat berhati-hati, bisa saja salah satu peralatan atau akun diretas. Bila hal ini terjadi, pilihan satu-satunya adalah memastikan komputer atau peralatan komunikasi tersebut bebas dari program merugikan (malware) dengan cara melakukan pembersihan (wipe) secara menyeluruh dilanjutkan dengan instalasi dari awal lagi. Peretas mungkin malah menghalangi akses ke berkas pribadi, foto atau informasi lainnya yang tersimpan didalam sistem yang sudah diretas. Pilihan terakhir adalah melakukan proses restore dari backup. Pastikan secara berkala melakukan backup informasi penting serta lakukan uji coba proses restore. Kebanyakan sistem operasi dan peralatan komunikasi mendukung proses backup otomatis.

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

Serangan Surel Palsu/Phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Mengamankan Peralatan Tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Sandi Kuat:	http://www.securingthehuman.org/ouch/2013#may2013
Kelola Sandi:	http://www.securingthehuman.org/ouch/2013#october2013
Verifikasi 2 Tahap:	http://www.securingthehuman.org/ouch/2013#august2013
Enkripsi:	http://www.securingthehuman.org/ouch/2014#august2014
Backup:	http://www.securingthehuman.org/ouch/2013#september2013

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