Buletin Bulanan Keamanan Komputer

Empat Kiat Aman

Sekilas

Menggunakan teknologi secara tepat dan aman bukanlah hal sederhana. Apapun jenis pilihan teknologinya atau bagaimanapun penggunaannya, simak empat (4) kiat agar tetap aman berikut ini:

1. Anda: Perlu diingat, teknologi tidak mampu memberikan perlindungan secara menyeluruh, justru perlindungan terbaik adalah diri Anda sendiri. Pelaku peretasan paham bahwa cara termudah mendapatkan apa yang diinginkan adalah menyasar Anda dibanding komputer atau peralatan. Agar bisa mendapatkan sandi, kartu kredit atau kendali komputer Anda, mereka akan berupaya memperdaya Anda agar mau memberikan informasi tersebut, tidak jarang dengan cara menciptakan situasi serba tergesa-gesa. Contoh: mereka menelpon Anda, berpura-pura dari bagian layanan teknis Microsoft, menyatakan bahwa komputer Anda tertular virus; padahal itu hanya tipuan dari kriminalis siber supaya bisa mengakses komputer Anda. Bisa juga mereka mengirimkan surel perihal paket kiriman gagal proses dan meminta Anda untuk mengakses pranala tertentu guna memastikan alamat surel, padahal itu hanya pancingan agar Anda mengakses situs tertentu yang nantinya bakal dimanfaatkan untuk meretas komputer Anda. Pada akhirnya, pertahanan terbaik dari semua itu adalah diri Anda sendiri. Dengan menggunakan akal sehat, Anda akan mahir dan terlatih mengenal sekaligus menghentikan beragam macam serangan.

2. Frasa Sandi: Kemajuan dunia komputer menjadikan sandi 8 karakter ketinggalan jaman dan beresiko. Saat merancang sandi, upayakan agar menggunakan frasa sandi kuat dan berbeda. Frasa sandi pada dasarnya adalah sandi biasa tapi terdiri dari serangkaian kata agar mudah diingat seperti “pagi pergi pulang malam”. Semakin panjang rangkaian kata itu, tentu semakin aman. “Berbeda” artinya setiap peralatan atau akun daring menggunakan sandi berbeda. Dengan cara ini, bila satu frasa sandi diretas, peralatan dan akun lain tetap aman. Sulit mengingat semua frasa sandi? Gunakan pengelola sandi, sebuah program khusus untuk menyimpan frasa sandi dalam format terenkripsi (dan juga fitur lainnya).

Selanjutnya, gunakan verifikasi dua tahap (disebut juga verifikasi dua faktor atau multi faktor). Cara ini tetap menggunakan sandi, namun ditambah satu langkah lagi, yaitu kode tertentu yang dikirim ke gawai atau kode dari satu aplikasi tertentu.Verifikasi dua tahap mungkin merupakan langkah penting dalam perlindungan akun daring dan juga gampang digunakan.

3. Pembaruan: Pastikan semua komputer, gawai, program dan aplikasi menggunakan versi perangkat lunak teranyar. Penyerang siber selalu mencari kelemahan perangkat lunak. Dengan cara itu, mereka akan menggunakan program khusus untuk memanfaatkan peluang itu dan meretas peralatan Anda. Pihak produsen perangkat lunak juga tidak kalah sibuk menyempurnakan produknya dengan cara menyediakan pembaruan perangkat lunak (updates). Pastikan bahwa komputer dan gawai melakukan proses pembaruan perangkat lunak sesegera mungkin agar mempersulit orang lain melakukan peretasan. Bila memungkinkan, aktifkan proses pembaruan otomatis, Hal ini berlaku ke semua peralatan yang tersambung ke internet seperti TV, pemantau bayi, kamera keamanan, router rumah, peralatan gim dan bahkan mobil Anda.

4. Pencadangan dan Unduh-Balik: Terkadang, walaupun sudah berhati-hati, Anda tetap saja bisa diretas. Bila itu terjadi, mungkin satu-satunya cara untuk mendapatkan kembali semua informasi milik Anda adalah dari cadangan (backup). Pastikan Anda melakukan pencadangan informasi penting secara rutin dan juga bisa mengunduh-balik (recovery) informasi tersebut dengan benar. Umumnya sistem operasi dan gawai menyediakan fasilitas pencadangan otomatis, baik dengan menggunakan hard disk tambahan atau Cloud.

Versi Bahasa Indonesia

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

Editor Tamu

***Steve Anson**, instruktur bersertifikasi SANS, memberikan bimbingan kepada tim keamanan IT dan badan pemerintah secara global guna meningkatkan keamanan sistem. Steve sedang menulis buku Applied Incident Response dan memberikan layanan nir bayar ke praktisi keamanan di www.AppliedIncidentResponse.com.*

Sumber Pustaka

Rekayasa Sosial: https://www.sans.org/u/W3G
Penipuan Terfokus: https://www.sans.org/u/W3Q
Menyederhanakan Sandi: https://www.sans.org/u/W3V
Punya Cadangan: https://www.sans.org/u/W40