Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Enkripsi

Mengenal Enkripsi

Dalam obrolan, tidak jarang dibahas soal “enkripsi” serta bagaimana penggunaannya untuk perlindungan Anda dan informasi. Sesungguhnya, konsep enkripsi terkadang cukup membingungkan, lagi pula enkripsi tidak bisa memberikan perlidungan menyeluruh karena keterbatasannya. Dalam edisi ini akan dijelaskan secara gamblang, apa itu enkripsi, kenapa diperlukan dan bagaimana penggunaannya secara benar.

Editor Tamu

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) adalah konsultan di Washington DC. Beliau merupakan instruktur utama di SANS Institute dibidang Mobile Device Security dan Ethical Hacking (SEC575), serta perancang modul Incident Response Team Management (MGT535).

Anda memiliki banyak informasi sensitif didalam peralatan, misalnya: dokumen finansial, foto, surel dan data rekam medis. Bila peralatan tersebut hilang atau dicuri, semua informasi sensitif didalamnya akan bisa diakses oleh pihak lain. Tambahan lagi, bisa jadi Anda melakukan transaksi online seperti layanan perbankan atau belanja on-line. Jika kriminalis siber mencermati aktifitas online Anda, bisa saja mereka mencuri informasi penting seperti akun finansial atau nomer kartu kredit. Dalam situasi seperti itu, enksripsi memberikan perlindungan dengan tidak memperbolehkan sembarang orang mengakses atau mengubah informasi .

Informasi tanpa enkripsi dikenal sebagai teks-biasa; dalam format ini sembarang orang dengan mudah bisa membaca dan mengaksesnya. Enkripsi mengubah informasi kebentuk lain yang tidak bisa dibaca yakni teks-bersandi. Enkripsi menggunakan rumus matematika rumit dan kunci-unik untuk mengubah sebuah informasi menjadi teks-bersandi. Kunci (“key”) berfungsi sebagai pembuka informasi didalamnya, seperti halnya kunci pintu. Kunci tersebut bisa saja berupa sandi dan hanya orang yang tahu sandi itu yang bisa melakukan proses dekripsi dan mengakses informasi. Untuk melindungi informasi terenkripsi, adalah penting untuk melindungi Kunci. Secara umum enkripsi bekerja dalam dua cara yaitu enkripsi data-statis (seperti data yang tersimpan di dalam laptop) dan data transisi (pengiriman informasi online).

Enkripsi Statis

Enkripsi statis bertujuan memberikan perlindungan seandainya komputer atau peralatan komunikasi hilang atau menjadi obyek pencurian. 15 tahun yang lalu, pencurian komputer bukanlah persoalan lantaran ukuran komputer pada

Enkripsi

saat itu tergolong besar sehingga susah dipindahkan. Di jaman sekarang, laptop dengan mudah bisa dijinjing dan alat komunikasi juga tidak kalah ringan. Semua peralatan itu berdaya-olah tinggi serta bisa menyimpan informasi dalam jumlah besar tapi lebih mudah hilang. Tambahan lagi, berbagai piranti tambahan seperti USB Flash drive dan CD-ROM bisa menyimpan informasi sensitif juga.

Metode yang sering dipakai dalam enkripsi dinamakan Full Disk Encryption (FDE). FDE menyiratkan bahwa semua informasi yang ada akan di-enkripsi. Tidak perlu dilakukan pemilahan mana yang perlu di enkripsi dan mana yang tidak. Kebanyakan sistem operasi dilengkapi dengan kemampuan FDE, jika diperlukan cuma perlu diaktifkan saja. Sebagai contoh, MAC OS X memiliki FileVault, sedangkan beberapa versi Windows menyertakan Bitlocker. Jika komputer Anda dilengkapi kemampuan FDE, disarankan untuk didaya gunakan. Beberapa alkom (alat komunikasi) dilengkapi pula fasilitas FDE media simpan internal. iOS sebagai misal, sistem operasi untuk iPhones dan iPads, secara otomatis melakukan FDE begitu "passcode" sudah ditentukan. Untuk mengetahui apakah komputer atau alat komunikasi yang digunakan untuk melakukan aktifitas perusahaan/ organisasi memiliki kemampuan FDE, hubungi staff helpdesk atau pihak yang berwenang. Untuk komputer pribadi, hubungi pihak produsen atau dapatkan dokumentasi secara online.

Enkripsi merupakan cara ampuh melindungi informasi, namun perlu juga Kunci yang kuat.

Enkripsi Transisi

Informasi juga rentan penyalahgunaan pada saat dalam proses pengiriman. Jika tidak dienkripsi, mungkin saja diawasi dan dicegat ditengah jalan. Oleh sebab perlu dipastikan adanya enkripsi komunikasi sensitif online seperti pada jasa perbankan, pengiriman surel atau bahkan akses ke media sosial. Enkripsi online yang paling lazim dipakai adalah HTTPS. Dengan cara ini semua lalu-lintas data antara browser dan website sepenuhnya dienkripsi. Perhatikan kode https:// di alamat URL, simbol gembok pada browser atau baris tampilan URL berubah warna menjadi hijau. Ini adalah tanda bahwa komunikasi dilakukan dengan enkripsi. Tergantung dari browser dan website, bisa saja semua tanda-tanda tadi tertampilkan sekaligus. Selain itu, pada saat Anda terhubung ke jaringan nir-kabel (wireless), pastikan menggunakan enkripsi jika dimungkinkan. Pada saat mengirim atau menerima surel pastikan program email yang dipakai menggunakan jalur terenkripsi. Sebagian besar program surel menyediakan fasilitas enkripsi dan penyedia jasa layanan internet (ISP) mungkin bisa membantu mengaktifkannya.

Enkripsi

Tepat Menerapkan Enkripsi

Apapun jenis enkripsi yang digunakan, hampir semuanya memiliki aturan umum agar tepat guna.

- Enkripsi berkaitan erat dengan Kunci ("key"). Kebocoran Kunci akan menyebabkan data Anda bisa diakses pihak lain. Kunci tersebut wajib dilindungi.
- Jika menggunakan "Passcode" atau sandi sebagai Kunci, pastikan cukup panjang, aman dan tidak sampai hilang atau terlupakan. Bila terlupakan, data tidak akan bisa diakses.
- Enkripsi juga tergantung pada pengamanan komputer yang dipakai. Jika komputer tersebut berhasil dibobol atau tertular program merugikan, bisa saja perlindungan enkripsi juga bobol. Oleh sebab itu pastikan komputer dan alat komunikasi selalu aman.
- Jika ada beberapa pilihan enkripsi, selalu pilih yang berunjuk kerja terbaik.

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

Mac OS X Filevault:	http://support.apple.com/kb/ht4790
Enkripsi iOS:	http://support.apple.com/kb/ht4175
Enkripsi Android:	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
Enkripsi Windows:	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
Pengamanan Komputer:	http://www.securingthehuman.org/ouch/2012#december2012
Pengaturan Sandi:	http://www.securingthehuman.org/ouch/2013#october2013

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

