Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Enkripsi

Apa itu Enkripsi?

Mungkin Anda pernah mendengar istilah “enkripsi” serta bagaimana penggunaannya untuk melindungi diri Anda dan informasi. Enkripsi bisa sedikit membingungkan dan selayaknya dipahami berbagai keterbatasannya. Dalam edisi ini akan dibahas secara sederhana arti dari enkripsi, apa saja yang bisa dilindungi serta bagaimana menggunakannya dengan tepat.

Editor Tamu

Francesca Bosco (**@francibosco**) adalah seorang peneliti dan pengelola proyek, menangani banyak proyek kriminal-siber, keamanan-siber dan penyalah-gunaan teknologi. Bekerja di United Nations Interregional Crime and Justice Research Institute sekaligus pendiri The Tech and Law Center.

Anda memiliki seabrek informasi sensitif/penting di dalam peralatan, misalnya: dokumen pribadi, foto dan surel. Bila peralatan tersebut hilang atau tercuri, semua informasi sensitif di dalamnya bakal bisa diakses oleh pihak lain. Tambahan lagi, bisa jadi Anda melakukan transaksi online seperti layanan perbankan atau belanja on-line. Bila seseorang mencermati aktifitas online Anda, bisa saja mereka mencuri informasi penting seperti akun finansial atau nomer kartu kredit. Dalam situasi seperti itu, enkripsi memberikan perlindungan dengan tidak memperbolehkan sembarang orang mengakses atau mengubah informasi .

Enkripsi hadir sejak ribuan tahun lalu. Di jaman sekarang enkripsi tentu lebih canggih, dengan tujuan yang sama yaitu mengirimkan pesan rahasia dari satu tempat ke tempat lain namun hanya pihak berwenang saja yang bisa mengaksesnya. Informasi tanpa enkripsi disebut sebagai teks biasa. Artinya, setiap orang bisa membaca dan mengaksesnya. Enkripsi mengubah informasi ini kebentuk yang tidak mudah dibaca atau disebut juga sebagai teks bersandi. Dewasa ini, enkripsi menggunakan rumus matematika yang kompleks dan “kunci” khusus untuk mengubah teks biasa menjadi tesk bersandi. Kata kunci digunakan untuk mengunci dan membuka kunci informasi Anda. Biasanya, kunci tersebut bisa merupakan sandi atau kode tertentu.

Enkripsi Untuk Apa?

Secara umum ada dua jenis enkripsi yaitu enkripsi data tidak-bergerak (seperti data yang tersimpan di dalam alkom/mobile device) dan data bergerak (saat mengunduh email atau berkirim pesan ke teman).

Enkripsi

Enkripsi data tidak-bergerak bermanfaat untuk melindungi informasi di komputer atau alkom khususnya saat hilang atau dicuri. Sekarang ini, semua peralatan berkemampuan luar biasa dan menyimpan banyak informasi namun juga mudah hilang. Malahan, beberapa peralatan-simpan genggam bisa menyimpan informasi sensitif, misalnya USB Flash Drive atau hard disk external. Full Disk Encryption (FDE) merupakan metode enkripsi yang lazim digunakan untuk mengenkripsi seluruh isi media simpan. FDE menyiratkan bahwa semua informasi akan di-enkripsi tanpa terkecuali. Tidak perlu dilakukan pemilahan mana yang perlu di enkripsi dan mana yang tidak. Sekarang, kebanyakan komputer dilengkapi dengan kemampuan FDE, jika diperlukan cuma perlu diaktifkan saja. Sebagai contoh, komputer Mac dikenal dengan sebutan FileVault, sedangkan di Windows, tergantung dari versi yang dipilih, bisa menggunakan Bitlocker atau Device Encryption. Kebanyakan alkom juga dilengkapi FDE. iOS di iPhone dan iPad otomatis mengaktifkan FDE bila passcode diaktifkan. Mulai Android 6.0 (Marshmallow), Google mengharuskan FDE secara otomatis diaktifkan, asalkan perangkat keras yang dipakai memenuhi kebutuhan minimal.

Enkripsi sangat berguna melindungi informasi, namun harus disertai kunci yang kuat pula.

Informasi juga rentan penyalahgunaan saat dalam proses pengiriman. Jika tidak dienkripsi, mungkin saja diawasi, diubah dan diunduh ditengah jalan. Inilah alasan kenapa transaksi penting dan komunikasi perlu di enkripsi. Enkripsi online yang paling lazim dipakai adalah HTTPS. Artinya semua lalu-lintas data antara browser dan situs web sepenuhnya dienkripsi. Perhatikan kode https:// di alamat URL, simbol gembok pada browser atau baris tampilan URL berubah warna menjadi hijau. Contoh lain adalah saat Anda mengirim atau menerima surel. Kebanyakan program surel menyediakan fasilitas ini. Contoh enkripsi data-bergerak lainnya adalah disaat dua orang melakukan obrolan online (chatting) di iMessage, Wickr, Signal, WhatsApp atau Telegram. Semua program aplikasi tersebut menggunakan enkripsi menyeluruh (end-to-end) sehingga menghalangi pihak lain untuk mengakses data pada saat berlalu-lalang dari satu sistem atau peralatan kelainnya. Dengan cara ini, hanya Anda dan pihak yang diajak berkomunikasi saja yang bisa membaca apa yang dikirimkan.

Lakukan Dengan Benar

Untuk memastikan bahwa Anda terlindungi saat menggunakan enkripsi, haruslah benar penggunaannya:

Enkripsi

- Enkripsi sama pentingnya dengan kata kunci yang bagus. Bila seseorang bisa menebak atau mendapatkan akses ke kunci tersebut, data Anda akan bisa diakses. Lindungi kunci tersebut. Bila Anda menggunakan passcode atau sandi untuk kunci, pastikan cukup kuat dan unik. Semakin panjang sandi, semakin susah ditebak atau dibobol. Jangan lupa sandi tersebut, karena tanpa itu Anda tidak akan bisa membaca ulang informasi yang sudah di enkripsi. Bila tidak bisa mengingat semua sandi, disarankan menggunakan pengelola sandi (password manager).
- Manfaat enkripsi sejalan dengan kesiapan peralatan yang dipakai. Jika peralatan tersebut sudah dibobol atau terinfeksi malware maka peretas bisa saja menerobos enkripsi. Jadi peralatan perlu diamankan dengan menggunakan anti-virus, sandi yang kuat dan selalu terperbarui.
- Berbagai aplikasi alkom (mobile apps) dan komputer menawarkan enkripsi untuk melindungi data dan komunikasi. Bila program aplikasi yang hendak dipakai tidak memiliki fasilitas enkripsi, pertimbangan untuk menggunakan yang lain.

Selanjutnya

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

Versi Bahasa Indonesia

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

Sumber Pustaka

Encryption Explained:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Frasa Sandi:	https://securingthehuman.sans.org/ouch/2015#april2015
Pengelola Sandi:	https://securingthehuman.sans.org/ouch/2015#october2015
Apa itu Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Mengamankan Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

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