Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

Penyulitan

Apakah itu Penyulitan?

Anda mungkin pernah mendengar terma “penyulitan” (encryption) dan bagaimana ia boleh dijadikan sebagai pelindung diri dan maklumat anda. Walaubagaimanapun, konsep penyulitan ini sedikit mengelirukan. Tambahan pula, penyulitan tidak boleh menjadi pelindung untuk semuanya kerana ianya juga terbatas. Dalam surat berita ini kami akan memberi penerangan mengenai penyulitan dengan semudah yang mungkin, mengapa anda perlu menggunakannya dan bagaimana untuk melaksanakannya dengan betul.

Editor Jemputan

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) merupakan seorang perunding yang berpangkalan di Washington, DC. Beliau juga adalah seorang pengajar kanan di SANS Institute bagi kursus Mobile Device Security and Ethical Hacking (SEC575) dan pengarang Incident Response Team Management (MGT535).

Anda mempunyai terlalu banyak maklumat sensitif dalam peranti anda seperti dokumen kewangan, gambar, e-mel atau rekod perubatan. Jika salah sebuah peranti anda hilang atau dicuri, kesemua maklumat sensitif dalam peranti tersebut boleh diakses oleh sesiapa yang memilikinya. Tambahan pula, anda mungkin melakukan transaksi sensitif dalam talian seperti perbankan dan membeli-belah. Jika seseorang penyerang siber memantau aktiviti dalam talian anda, mereka boleh mencuri kesemua maklumat anda, seperti akaun kewangan atau nombor kad kredit. Penyulitan melindungi anda dalam situasi-situasi sebegini dengan memastikan mereka yang tiada kebenaran tidak mengakses atau mengubah maklumat anda.

Apabila maklumat tidak disulitkan, ia dipanggil teks-biasa (plain-text). Ini bermakna sesiapa sahaja boleh membaca atau mengaksesnya. Penyulitan akan menukar maklumat ini kepada format yang tidak boleh dibaca yang dipanggil cipher-text. Penyulitan berfungsi dengan menggunakan operasi matematik yang kompleks dan kekunci unik untuk menukar maklumat anda kepada cipher-text. Kekunci tersebutlah yang mengunci dan membuka maklumat anda sama seperti kunci untuk mengunci dan membuka pintu. Contoh kekunci yang biasa adalah kata laluan, hanya mereka yang mempunyai kata laluan boleh menyahsulit dan mengakses maklumat anda. Untuk melindungi maklumat yang telah disulitkan anda perlu melindungi kekunci anda. Secara amnya penyulitan berfungsi melalui dua cara; anda boleh menyulitkan maklumat dalam keadaan rehat (seperti data yang disimpan dalam komputer riba) dan data yang sedang bergerak (seperti maklumat yang sedang dihantar dalam talian).

Menyulitkan Maklumat Dalam Keadaan Rehat

Matlamat utama penyulitan data dalam keadaan rehat adalah untuk melindungi maklumat anda sekiranya komputer atau peranti mudah alih anda hilang atau dicuri. Lima belas tahun dahulu ini tidak menjadi isu kerana keban-

Penyulitan

yakkan komputer terlalu besar, berat dan amat sukar untuk dialihkan. Kebanyakan komputer riba kini beratnya hanya beberapa kilogram manakala peranti mudah alih beratnya hanya ratusan gram sahaja. Peranti-peranti ini berkuasa tinggi dan mampu menyimpan maklumat dengan banyak tetapi mudah hilang. Tambahan pula, medium mudah alih lain yang boleh menyimpan maklumat sensitif adalah seperti pemacu USB atau CD ROM. Teknik yang biasa digunakan untuk menyulitkan maklumat dalam medium sebegini dipanggil Penyulitan Penuh Cakera (Full Disk Encryption (FDE)). Ini bermakna apa yang ada dalam sistem tersebut akan disulitkan secara automatik, anda tidak perlu membuat pilihan antara apa yang perlu dan apa yang tidak perlu disulitkan. Kebanyakan sistem operasi sekarang tersedia dengan Penyulitan Penuh Cakera, anda hanya perlu mengaktifkannya. Sebagai contoh, Mac OS X mempunyai FileVault manakala sesetengah versi Windows mempunyai Bitlocker. Jika komputer anda mempunyai Penyulitan Penuh Cakera, kami mengesyorkan anda untuk mengaktifkannya. Lebih-lebih lagi, kebanyakan peranti mudah alih mempunyai Penyulitan Penuh untuk storan dalaman. Sebagai contoh iOS, sistem operasi untuk iPhone dan iPad, akan menggunakan Penyulitan Penuh Cakera secara automatik setelah kod laluan dimasukkan. Untuk mengetahui sama ada komputer atau peranti mudah alih di pejabat anda mempunyai Penyulitan Penuh Cakera atau tidak, tanyalah help desk atau penyelia anda. Untuk komputer peribadi, hubungi pengeluar komputer anda atau semak dokumen dalam talian.

Penyulitan merupakan cara yang sangat berkesan untuk melindungi maklumat anda, tetapi ia hanyalah sekuat kekunci anda.

Menyulitkan Maklumat Dalam Transit

Maklumat juga terdedah kepada serangan ketika ia dalam transit. Jika data tersebut tidak disulitkan, ia dapat dipantau dan tangkap dalam talian. Inilah antara sebab mengapa anda perlu pastikan sebarang komunikasi sensitif dalam talian seperti perbankan dalam talian, menghantar e-mel atau mungkin akses kepada media sosial disulitkan. Penyulitan dalam talian yang biasa digunakan adalah HTTPS. Ini bermakna kesemua lalu lintas antara pelayar dan laman sesawang disulitkan. Lihat sama ada terdapatnya https:// dalam URL, simbol kunci mangga pada pelayar anda atau warna bar URL anda bertukar kepada hijau. Ini semua adalah tanda-tanda komunikasi anda telah disulitkan. Bergantung kepada pelayar dan laman sesawang, anda mungkin akan melihat ketiga-tiganya sekali dalam masa yang sama. Selain itu, setiap kali anda berhubungan dengan rangkaian Wi-Fi terbuka, pastikan anda menggunakan penyulitan. Akhir sekali, apabila menghantar dan menerima e-mel pastikan e-mel klien anda ditetapkan menggunakan saluran yang disulitkan. Kebanyakan e-mel klien mempunyai penyulitan dan penyedia khidmat internet anda juga mungkin dapat membantu mengaktifkan penyulitan pada e-mel klien anda.

Penyulitan

Melaksanakan Penyulitan dengan Betul

Tidak kira apa jenis penyulitan yang anda gunakan atau bagaimana anda menggunakannya, hampir kesemuanya berkongsi cara yang sama untuk digunakan dengan betul.

- Penyulitan anda hanyalah sekuat kekunci anda. Jika seseorang meneka atau mengkompromikan kekunci anda, mereka boleh megakses maklumat anda. Anda perlu melindungi kekunci anda.
- Jika anda menggunakan kod laluan atau kata laluan untuk kekunci, pastikan ianya panjang, kata laluannya kukuh dan jangan hilangkan atau lupakannya. Jika anda terlupa, anda akan terkunci dari maklumat anda sendiri.
- Penyulitan anda hanya sekuat keselamatan komputer anda sendiri. Jika komputer anda telah di kompromi atau telah dijangkiti, penyerang siber boleh memintas penyulitan anda. Dengan itu, pastikan komputer atau peranti mudah alih anda berada dalam keadaan selamat.
- Jika anda diberi beberapa pilihan untuk penyulitan, sentiasa pilih cara yang paling kukuh.

Mari Belajar Lebih Lanjut!

Langganilah surat berita bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer OUCH!, akseslah arkib OUCH!, dan belajar lebih lanjut mengenai penyelesaian kesedaran keselamatan SANS dengan melayari laman sesawang kami di http://www.securingthehuman.org.

Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: http://snsc.skmm.gov.my/.

Sumber

Mac OS X FileVault:	http://support.apple.com/kb/ht4790
iOS Encryption:	http://support.apple.com/kb/ht4175
Android Encryption:	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
Windows Encryption:	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
Securing Your Computer:	http://www.securingthehuman.org/ouch/2012#december2012
Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013

Editor: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated by: Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie

