OUCH! | Desember 2014

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

- Sekilas
- Cara Kerja Anti-Virus
- Tips Anti-Virus

Apa Itu Anti-Virus?

Sekilas

Anti-virus adalah perangkat lunak keamanan yang dipasang di sebuah komputer atau alat komunikasi (alkom) agar terhindar dari infeksi malware (program berbahaya). Istilah "malware" digunakan untuk menerangkan beragam "malicious software" (program berbahaya) seperti virus, worm, trojan dan spyware. Kata malware itu sendiri terbentuk dari gabungan dua kata yaitu malicious (berbahaya) dan software (perangkat lunak/program). Bila sebuah komputer terinfeksi malware, penjahat siber bisa saja mendapatkan rekaman semua akifitas penggunaan keyboard, mencuri dokumen dan bahkan menggunakan komputer tersebut untuk menyerang komputer lain. Bertolak belakang dari anggapan selama ini, perlu dipahami bahwa semua sistem operasi, termasuk Mac OS X dan Linux bisa terinfeksi malware.

Editor Tamu

Jake Williams adalah pendiri Rendition Infosec (**www.renditioninfosec.com**) dan juga instruktur bersertifikat SANS sekaligus perancang modul pelatihan. Aktif di Twitter sebagai **@MalwareJake** dan penulis blog **malwarejake.blogspot.com**.

Perangkat lunak anti-virus bisa dibeli secara terpisah atau ada pula yang digabungkan ke dalam paket perangkat keamanan. Dalam kenyataan, anti-virus tidak mampu lagi mengimbangi ulah penjahat siber dalam mengembangkan dan melahirkan malware jenis baru. Demikian banyak versi baru muncul setiap hari membuat tidak ada satupun anti-virus sanggup melakukan deteksi dan perlindungan terhadap semuanya. Perlu diingat, anti-virus akan melindungi komputer Anda namun tidak akan bisa mendeteksi atau menghentikan kerja semua malware. Kenapa demikian? Simak penjelasan dibawah ini.

Cara Kerja Anti-Virus

Secara umum anti-virus menggunakan dua (2) cara dalam mengenal malware yaitu deteksi pengenal unik dan deteksi perilaku. Deteksi pengenal unik ini mirip dengan sistem ketahanan tubuh manusia, bekerja dengan cara memindai (scan) komputer guna menemukan karakteristik atau pengenal unik malware. Metode ini dilakukan dengan bantuan kamus/daftar malware yang pernah ada; bila di sebuah komputer ditemukan pengenal unik persis seperti yang ada di dalam kamus/daftar malware maka program anti-virus akan menetralisirnya. Tidak berbeda dengan tubuh manusia, kamus/daftar malware juga perlu pembaruan (seperti halnya suntikan vaksin flu) agar malware baru bisa terdaftar didalamnya. Anti-virus ini hanya bisa memberikan perlindungan terhadap sesuatu yang terbukti merugikan. Dilain pihak, penjahat siber dengan gesit terus mengembangkan berbagai malware baru sehingga menyebabkan anti-virus

Apa Itu Anti-Virus?

kewalahan. Oleh sebab itu meskipun program anti-virus Anda sudah diperbarui, tetap saja akan ada malware baru yang berpotensi menembusnya.

Dalam deteksi perilaku, anti-virus melakukan aksinya tidak berdasar dari malware yang sudah pernah ada, namun mengamati tingkah laku perangkat lunak yang terpasang di sebuah komputer. Jika sebuah program bertindak mencurigakan seperti mencoba mengakses berkas yang terproteksi atau mencoba mengubah program lain maka perangkat lunak anti-virus akan memunculkan peringatan. Cara ini memberikan perlindungan terhadap malware baru yang belum terdaftar. Terkadang bisa saja metode ini memicu kekeliruan dalam memberikan peringatan. Pengguna komputer juga bisa bingung dalam menentukan tindakan selanjutnya dan bahkan lama kelamaan menjadi tidak terlalu peduli terhadap peringatan yang muncul. Mungkin saja Anda menjadi kurang teliti dan mengabaikan setiap peringatan sehingga malah membuat komputer menjadi rentan terhadap serangan dan infeksi virus. Selain itu, saat anti-virus menemukan perilaku mencurigakan, kemungkinan malware itu sudah mendekam di dalam komputer dan tidak ada yang tahu apa saja yang telah dilakukan malware tersebut sebelum diketahui keberadaannya oleh program anti-virus.

Walaupun anti-virus merupakan bagian penting keamanan namun tidak akan sanggup mendeteksi dan menghentikan semua jenis serangan. Manusia adalah perlindungan terbaik, melebihi teknologi.

Anti-virus merupakan bagian penting pengamanan komputer dan alkom, sebisa mungkin disarankan untuk selalu menggunakan dan mengaktifkannya. Namun perlu diingat bahwa bagaimanapun sebuah anti-virus bekerja, tidak akan sanggup memberikan perlindungan terhadap semua jenis malware. Pada akhirnya, Anda merupakan perlindungan terbaik dalam menghadapi penjahat siber.

Tips Anti-Virus

1. Dapatkan perangkat lunak anti-virus hanya dari sumber dan penjual terpercaya. Salah satu modus penjahat siber adalah dengan menyebarkan program anti-virus palsu yang sebenarnya adalah malware.
2. Pastikan Anda selalu menggunakan versi terbaru anti-virus, membayar iuran berlangganan, teraktifasi dan dikonfigurasi untuk melakukan pembaruan otomatis (auto-update).
3. Pastikan anti-virus melakukan pemindaian (scan) peralatan tambahan (seperti memori USB) serta selalu aktif.
4. Berikan perhatian khusus pada setiap tampilan pesan dan tanda bahaya yang diberikan anti-virus. Kebanyakan tanda bahaya itu disertai pilihan untuk mendapatkan informasi atau rekomendasi tindakan selanjutnya. Jika tanda bahaya tersebut muncul di komputer kantor/kerja, pastikan segera menghubungi staff help desk atau atasan Anda.

Apa Itu Anti-Virus?

5. Jangan pernah menon-aktifkan atau menghapus perangkat lunak anti-virus karena alasan memperlambat kerja komputer, terblokirnya akses ke situs web atau adanya larangan penambahan aplikasi atau program baru. Menon-aktifkan program anti-virus memicu kerentanan terhadap beragam resiko sekaligus bisa menimbulkan persoalan keamanan yang serius. Jika permasalahan itu muncul di komputer kantor/kerja, laporkan kebagian help desk. Untuk komputer pribadi, coba hubungi penjual anti-virus, kunjungi situs web anti-virus tersebut untuk mendapatkan informasi tambahan atau mengganti anti-virus tersebut dengan produk lain.
6. Hindari memasang beberapa program anti-virus sekaligus di sebuah komputer. Hal itu malah menyebabkan permasalahan antar sesama anti-virus dan mengurangi keamanan komputer.
7. Kenali peringatan yang dimunculkan oleh program anti-virus. Penjahat siber bisa saja membuat situs web berbahaya yang memajang peringatan asli tapi palsu dari anti-virus serta menawarkan bantuan untuk "memperbaiki" komputer Anda. Mengunjungi tautan (link) atau mengklik salah pilihan di situs web itu malah bisa merugikan Anda.

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

Perbandingan Produk Anti-Virus:	http://www.av-test.org/en/
Rekayasa Sosial:	http://www.securingthehuman.org/ouch/2014#november2014
Serangan Surel Phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Saya Diretas, Selanjutnya Bagaimana?:	http://www.securingthehuman.org/ouch/2014#may2014

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