Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Belajar Dari WannaCry

Sekilas

Baru-baru ini, mungkin Anda mengamati demikian banyak ulasan mengenai serangan siber “WannaCry”. “WannaCry” menginfeksi lebih dari 200,000 komputer, memotong/ mengunci akses data diberbagai organisasi termasuk rumah sakit di Inggris. Kenapa serangan ini menyita demikian banyak perhatian? Pertama, penyebaran terjadi antar komputer melalui titik lemah Windows. Kedua, ini merupakan malware jenis “Ransomware”; artinya bekerja dengan cara mengenkripsi semua berkas sehingga tidak bisa diakses. Cara mendapatkan kembali data tersebut adalah menggunakan cadangan (backup) atau dengan membayar $300 agar data didekripsi. Ketiga, sebagai hal terpenting, serangan ini sebenarnya bisa dicegah. Kelemahan Windows yang dimanfaatkan “WannaCry” sudah diketahui Microsoft dan juga program perbaikan sudah disebarluaskan beberapa bulan sebelumnya. Kenyataannya, banyak organisasi tidak memasang program perbaikan ini atau menggunakan sistem operasi seperti Windows XP yang tergolong sangat tua sehingga tidak lagi memiliki program penyempurnaan lagi. Berikut adalah tiga langkah sederhana agar terhindar dari infeksi “WannaCry”.

Editor Tamu

Dr. Johanes Ullrich adalah pimpinan riset SANS Technology Institute serta pendiri DShield.org. Berkarya di **SANS Internet Storm Center** yang mengawasi ancaman keamanan siber terbaru. Staff pengajar Web Application Security (**DEV522**), Intrusion Detection (**SEC503**) and IPv6 (**SEC546**).

Perbaikan

Adalah sangat penting memastikan komputer, alkom, program aplikasi dan apa saja yang tersambung ke internet menggunakan program termutakhir. Kriminalis siber selalu mencari kelemahan perangkat lunak sebuah peralatan. Bila ditemukan titik kelemahan, dipakailah program khusus untuk meretas peralatan. Dilain pihak, produsen peralatan juga menciptakan perangkat lunak untuk menyempurnakan peralatan dengan cara menyebar paket perbaikan (update). Dengan memastikan semua komputer dan alkom tidak lupa menggunakan paket perbaikan, upaya peretasan akan menjadi lebih sulit. Kasus WannaCry sebenarnya tidak perlu menjadi demikian parah. Perangkat lunak perbaikan untuk penyempurnakan dan menghentikan peretasan sudah disebar Microsoft hampir dua bulan sebelumnya. Bila semua organisasi tertib menggunakan paket perbaikan ini, niscaya peretasan tidak akan pernah terjadi. Untuk menjamin semua peralatan selalu

Belajar Dari WannaCry

menggunakan perangkat lunak terkini, sebisa mungkin aktifkan fasilitas perbaikan otomatis. Hal itu juga berlaku bagi semua peralatan yang tersambung ke jaringan, tidak hanya komputer dan alkom tapi juga televisi, router di rumah, peralatan game dan mungkin suatu saat juga mobil. Bila sistem operasi atau peralatan sudah terlalu tua dan tidak lagi ditunjang layanan berkelanjutan, Windows XP contohnya, gantilah dengan yang lebih baru.

Tiga kiat aman tolak serangan (contoh: WannaCry); selalu perbarui komputer, waspada terhadap serangan pengelabuan dan melalukan pencadangan.

Pencadangan

Dalam beberapa kasus, sebuah ransomware bahkan bisa menerobos sistem yang sudah diperbarui. Cara perlindungan tambahan ialah dengan membuat cadangan (backup) data. Berkas cadangan adalah salinan informasi yang disimpan di luar komputer dan alkom. Pada saat data penting hilang, perbaikan bisa dilakukan dengan menggunakan file cadangan. Sayangnya, banyak orang tidak melakukannya, walaupun prosesnya mudah dan tidak mahal. Ada dua cara pencadangan: media simpan biasa atau solusi cloud. Masing-masing memiliki keunikan tersendiri. Bisa saja semua cara tersebut dilakukan bila tidak yakin mana yang terbaik/akan digunakan.

Media biasa bisa dijamah dan dikendalikan seperti USB external atau media simpan yang terhubung jaringan di kantor atau rumah. Keunggulan media biasa adalah kemampuan menyimpan dan membaca data dalam kecepatan tinggi. Cara ini rentan terhadap sergapan malware seperti Ransomware, bisa saja berkas cadanganpun terkontaminasi. Selain itu, diperlukan pelabelan yang akurat disetiap media yang digunakan serta wajib disimpan di tempat yang aman (tidak satu lokasi dengan rumah/kantor). Solusi pencadangan berbasis cloud menggunakan internet sebagai tempat penyimpanan data. Biasanya diawali dengan memasang sebuah aplikasi di komputer. Program aplikasi ini akan menjalankan semua proses secara otomatis. Tentu hal ini mengusung banyak kemudahan. Ransomware biasanya tidak bisa mengakses berkas cadangan di cloud. Kekurangan solusi ini terletak pada lamanya selang waktu yang diperlukan guna melakukan pencadangan data berukuran besar. Pastikan membaca aturan privasi dan keamanan pencadangan cloud. Periksa apakah penyedia jasa layanan dilengkapi dengan fasilitas keamanan seperti enkripsi dan otentifikasi yang baik.

Belajar Dari WannaCry

Pengelabuan

Pelaku kejahatan tidak pernah berhenti menyempurnakan dan mengubah metode serangan. Satu metode yang sering digunakan adalah pengelabuan. Hal ini dilakukan dengan mengirim surel (email) dan mencoba mengelabui Anda agar membuka sebuah lampiran yang berisi program atau mengklik situs web berbahaya. Bila ini terjadi, sebuah komputer bisa terinfeksi. Walaupun "WannaCry" tidak menggunakan cara ini, pengelabuan sering dipakai oleh jenis serangan lain. Tambahan lagi, pengembang program "WannaCry" pasti akan mengembangkan teknik penyerangan di masa depan agar bisa menginfeksi semakin banyak perangkat. Agar aman dari serangan berbasis surel, gunakan akal sehat. Bila ada surel atau pesan aneh, mencurigakan atau sangat mengada-ada, hampir pasti itu adalah sebuah upaya pengelabuan.

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

Daftar Pustaka

Mengenal Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
Backups and Recovery:	https://securingthehuman.sans.org/ouch/2015#august2015
Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Aman Menggunakan Cloud:	https://securingthehuman.sans.org/ouch/2016#november2016

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

