OUCH! | April 2014

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

- Sekilas
- Kenapa Anda Adalah Sasaran
- Perlindungan Anda

Ya, Anda adalah Sasaran

Sekilas

Umumnya orang beranggapan bahwa mereka bukanlah sasaran kriminal siber: bahwa mereka atau komputer mereka tidak memilik nilai yang berarti. Padahal, bila Anda memiliki sebuah komputer, piranti komunikasi, akun online, alamat surel, kartu kredit atau melakukan berbagai aktifitas online; Anda memiliki nilai ekonomis bagi kiriminalis siber. Dalam edisi ini akan dibahas kenapa Anda adalah sasaran, bagaimana Anda diserang dan langkah apa saja yang bisa Anda lakukan untuk perlindungan.

Editor Tamu

Eric Conrad adalah Presiden dan CTO Backshore Communication serta penulis utama buku The CISSP Study Guide, Second Edition dan Eleventh Hour CISSP, Second Edition. Beliau juga salah seorang pencipta kursus berdurasi 6 hari Continuous Monitoring and Security Operations (SEC511) di SANS.

Kenapa Anda Adalah Sasaran

Tidak kejahatan seperti penipuan, pencurian identitas atau pemerasan sudah ada sejak dahulu kala sebagai bagian dari kehidupan. Tujuan seorang kriminalis selalu sama: mendapatkan uang sebanyak-banyaknya dengan cara segampang mungkin disertai dengan resiko sekecil-kecilnya. Biasanya, itu bukan persoalan mudah karena ada keterbatasan tempat dan juga diperlukan interaksi dengan calon korban, akibatnya pilihan sasaran menjadi terbatas dan juga memberikan resiko yang tidak kecil bagi pelakunya. Namun, tindak kejahatan berubah drastis sejalan dengan kemajuan internet dan teknologi online. Sekarang kriminalis siber dengan mudah menentukan sasaran diseluruh dunia, disertai biaya murah atau bahkan gratis serta beresiko sangat kecil. Tambahan lagi, kriminalis siber kian hari kian terorganisir dan efisien, menjadikan mereka menjadi lebih efektif.

Alhasil, kriminalis siber paham bahwa dengan mencuri lebih banyak banyak kartu kredit, meretas (hack) lebih banyak akun bank atau menyadap lebih banyak sandi (password) berarti semakin banyak uang bisa diperoleh. Mereka pada dasarnya akan mencoba meretas siapa saja yang terhubung ke internet, termasuk Anda. Meretas jutaan orang diberbagai pelosok dunia terbayang seperti sebuah proses yang merepotkan namun sebenarnya tergolong sederhana karena mereka menggunakan alat bantu otomatis. Sebagai contoh: mereka membangun sebuah database yang berisi jutaan alamat surel dan menggunakan fasilitas otomatis untuk mengirim pesan Phishing kesetiap alamat yang ada. Mengirimkan surel bisa dilakukan nyaris tanpa biaya; caranya? Dengan menggunakan komputer yang diretas, mungkin malah menggunakan komputer Anda, sebagai alat bantu. Ini adalah salah satu contoh bahwa peralatan

Ya, Anda adalah Sasaran

Anda bernilai guna karena setidaknya bisa dipakai untuk meretas atau melakukan tindak kejahatan lain. Walaupun para pelaku tindak kriminal ini tidak tahu siapa saja korban dari serangan via surel tersebut, namun mereka tahu bahwa semakin banyak surel terkirim berarti akan bertambah banyak orang yang akan menjadi mangsa. Bisa juga kriminalis ini melakukan pencarian di jaringan internet (dengan bantuan komputer retasan), untuk mencari komputer dan peralatan yang bisa diretas. Ingat, kriminalis ini mengincar setiap orang tanpa kecuali, termasuk Anda.

Anda mungkin tidak menyadari bahwa peralatan dan informasi Anda sangat berharga bagi kriminalis siber diseluruh dunia.

Perlindungan Anda

Kriminalis siber menggunakan metode sederhana dalam upaya meretas diseluruh dunia. Jangan kuatir, dengan menggunakan berbagai langkah sederhana dibawah ini, Anda bisa terlindung dengan baik. Langkah tersebut adalah sbb:

- **Anda**: Pada akhirnya, Anda adalah garis pertahanan pertama terhadap serangan siber. Banyak serangan diawali dengan upaya mengelabuhi Anda, contohnya adalah dengan membuat Anda membuka lampiran surel atau meminta sandi (password) melalui telepon. Akal sehat adalah modal terbaik: Jika sesuatu terkesan tidak lazim/aneh, mencurigakan atau terlalu berlebihan, hampir pasti itu adalah sebuah upaya serangan.

- **Pembaruan**: Pastikan setiap komputer atau peralatan komunikasi yang dipakai selalu diperbarui dan dilengkapi dengan patches terbaru. Ini tidak saja penting bagi sistem operasi, namun juga untuk program aplikasi atau program tambahan (plugin). Dengan selalu menggunakan sistem dan aplikasi terkini, Anda akan terbantu dalam menghadapi upaya serangan.

- **Sandi**: gunakan sandi yang kuat dan unik untuk setiap akun Anda. Dengan cara ini, jika sebuah website yang biasa Anda gunakan diretas dan sandi Anda terungkap (dicuri) maka akun lainnya akan tetap aman. Juga pastikan semua ragam peralatan terlindungi oleh mekanisme pengunci akses melalui penggunaan sandi yang kuat & unik, gunakan PIN atau mekanisme lain. Agar beragam sandi Anda bisa dikelola dengan aman, disarankan menggunakan Password Manager.

Ya, Anda adalah Sasaran

- **Kartu Kredit**: Lakukan pengecekan laporan keuangan lebih sering, setidaknya setiap minggu (sebulan sekali tidaklah cukup). Segera setelah ditemukan transaksi tanpa otorisasi, laporkan kepenerbit kartu kredit Anda. Jika bank Anda memperbolehkan, untuk mempercepat proses, gunakan fasilitas pelaporan via surel atau pesan singkat (SMS) pada saat terjadi transaksi bernilai besar atau aktifitas mencurigakan.

- **Jaringan**: Amankan jaringan nir-kabel (Wi-Fi) rumah Anda dengan menggunakan sandi administrator yang kuat dan wajibkan setiap pengguna memasukkan sandi untuk bisa bergabung ke jaringan. Pastikan bahwa Anda mengetahui semua ragam peralatan yang tersambung ke jaringan rumah dan semua peralatan sudah terperbarui.

- **Media Sosial**: Semakin banyak Anda mengunggah informasi online, Anda akan terpapar pada resiko yang lebih besar. Informasi terunggah tersebut bukan hanya bisa mempermudah kriminalis siber dalam memperdaya dan menjadikan Anda sebagai sasaran, namun setiap informasi itu menjadikan Anda sebagai sasaran yang lebih berharga.

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

OUCH! Password Managers:
http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Securing Your Home Network:
http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Phishing Attacks:
http://www.securingthehuman.org/ouch/2013#february2013
Poster: You Are A Target:
http://www.securingthehuman.org/resources/posters

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