OUCH! | November 2014

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

- Mengenal Rekayasa Sosial
- Kenali / Hentikan upaya Rekayasa Sosial
- Tindakan Pencegahan

Rekayasa Sosial

Sekilas

Apakah benar anggapan bahwa penyerang siber hanya menggunakan perangkat dan teknologi mutakhir untuk membobol komputer, akun atau alat komunikasi (alkom/ mobile device)? Hal ini jelas tidak tepat. Penyerang siber paham bahwa cara termudah mendapatkan informasi atau membobol komputer adalah dengan cara berkomunikasi dan mengelabui penggunanya. Dalam edisi ini akan dibahas bagaimana cara kerja serangan rekayasa sosial serta apa yang bisa dilakukan agar terhindar dari serangan itu.

Editor Tamu

Alissa Torres adalah instruktur bersertifikat di SANS dengan bidang spesialisasi forensik komputer tingkat lanjut dan penanganan insiden. Pernah bertugas digaris depan peperangan untuk menangani berbagai insiden serta bekerja di bagian pengamanan internal sebagai penyelidik forensik. Alissa hadir di Twitter sebagai **@sibertor**.

Mengenal Rekayasa Sosial

Rekayasa sosial merupakan ragam serangan psikologis dimana seseorang berupaya mengelabui Anda agar mau melakukan apa yang diinginkan pelaku. Rekayasa sosial sudah ada sejak ribuan tahun lalu, tindakan penipuan dan mengelabui orang lain bukanlah hal baru. Namun, penyerang siber tahu bahwa penggunaan metode ini di internet sangatlah efektif sekaligus jutaan orang bisa menjadi sasaran. Simaklah contoh dibawah ini untuk mengenal bagaimana aksi rekayasa sosial dilakukan.

Anda mendapatkan panggilan telepon dari seseorang yang mengaku berasal dari bagian layanan sebuah perusahaan komputer, layanan jasa internet atau layanan teknis Microsoft. Penelepon tersebut menjelaskan bahwa komputer Anda bekerja dengan tidak semestinya lantaran memindai Internet secara acak dan mengirimkan spam, oleh sebab itu diyakini bahwa komputer itu telah terinfeksi program berbahaya. Mereka menyatakan ditunjuk untuk menyelidiki persoalan tersebut dan membantu mengamankan komputer Anda. Selanjutnya, mereka menggunakan berbagai istilah teknis dan memandu Anda melakukan beberapa langkah membingungkan untuk meyakinkan bahwa komputer Anda telah terinfeksi.

Misalnya, mereka bisa saja meminta Anda untuk mencari berkas tertentu di komputer serta menjelaskan cara untuk menemukannya. Apabila berkas itu berhasil ditemukan, sang penelepon akan mengatakan bahwa berkas tersebut merupakan pertanda bahwa sebuah komputer telah terinfeksi. Kenyataannya, berkas itu hanyalah berkas biasa yang lazim ada disetiap komputer. Bila upaya itu bisa menyakinkan Anda bahwa komputer sudah terinfeksi, mereka akan menggiring Anda untuk mengunjungi sebuah situs web yang menjual perangkat lunak keamanan atau meminta agar diperbolehkan melakukan akses jarak jauh ke komputer Anda agar bisa melakukan perbaikan. Sebenarnya, perangkat

Rekayasa Sosial

lunak yang dijual adalah program berbahaya. Bila Anda membeli dan memasang perangkat lunak itu, mereka bukan hanya memperdaya Anda dengan menjadikan komputer terinfeksi, namun Anda juga mengeluarkan biaya untuk itu. Bila akses jarak jauh diberikan, mereka juga akan membuat komputer Anda malah terinfeksi program berbahaya.

Ingat, serangan rekayasa sosial seperti ini tidak hanya dilakukan lewat telepon namun bisa juga lewat aneka ragam teknologi lainnya seperti surel, pesan instan, SMS, pengiriman pesan di Facebook, posting Twitter atau obrolan online. Yang terpenting disini adalah waspada terhadap semua hal itu.

Salah satu upaya terbaik agar terhindar dari serangan rekayasa sosial adalah dengan memahami cara mencegah, mengenali dan menghentikannya.

Kenali / Hentikan upaya Rekayasa Sosial

Cara termudah untuk melindungi diri dari upaya rekayasa sosial adalah dengan selalu berpikir jernih. Jika sesuatu tampak mencurigakan atau tidak biasa maka bisa saja itu merupakan sebuah serangan. Beberapa indikasi adanya serangan rekayasa sosial adalah:

- Seseorang membuat situasi menjadi serba tergesa-gesa. Jika Anda ada harus membuat sebuah keputusan dalam situasi seperti itu, berhati-hatilah.
- Seseorang meminta informasi yang tidak seharusnya diakses atau malah sebaliknya sudah selayaknya diketahui.
- Sesuatu yang berlebihan atau muluk-muluk. Contoh: tiba-tiba Anda mendapatkan informasi menjadi pemenang lotere walaupun tidak pernah membelinya.

Jika ada kecurigaan karena seseorang berusaha menjadikan Anda korban serangan rakayasa sosial, berhentilah berkomunikasi dengan orang tersebut. Jika hal tersebut dilakukan via telepon, jangan lanjutan percakapan. Bila dilakukan melalui obrolan online, hentikan segera. Jika dilakukan melalui surel, hapus saja surel tersebut. Seandainya terjadi di lingkup kerja/kantor, laporkan segera ke bagian layanan atau team keamanan informasi.

Mencegah serangan Rekayasa Sosial

Jangan kuatir, ada beberapa tindakan pencegahan yang bisa dilakukan untuk mencegah upaya serangan rekayasa sosial di masa depan.

- **Jangan Pernah Berbagi Sandi**. Sebuah organisasi tidak akan pernah meminta sandi Anda. Bila seseorang meminta sandi Anda: Waspadalah.

Rekayasa Sosial

- **Sedikit Berbagi**. semakin banyak yang bisa diungkap tentang Anda, semakin mudah untuk melakukan pengelabuan dan upaya lainnya. Walaupun hanya berbagi sedikit informasi, lama kelamaan akan bisa memberikan gambaran lengkap mengenai Anda. Semakin sedikit informasi yang diungkap/diunggah, termasuk ke situs media sosial, review produk, forum diskusi dan milist akan memperkecil kemungkinan terjadinya serangan.

- **Periksa Dulu**. Kapan saja Anda bisa mendapatkan panggilan telepon dari bank, perusahaan kartu kredit, perusahaan jasa komunikasi atau organisasi lainnya. Jika ada keraguan akan kebenarannya, mintalah nama dan nomer telepon orang tersebut. Cari nomer telepon perusahaan tersebut dari sumber terpercaya, mungkin dari nomer telepon yang tercetak di balik kartu kredit, di rincian tagihan bulanan atau bisa juga dari website perusahaan (pastikan URL nya benar). Ini penting untuk memastikan bahwa Anda berhubungan dengan pihak yang benar. Langkah diatas tampak merepotkan namun itu perlu dilakukan demi keamanan identitas dan informasi pribadi 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

Serangan Surel Pengelabuan:	http://www.securingthehuman.org/ouch/2013#february2013
Keamanan Media Sosial:	http://www.securingthehuman.org/ouch/2013#march2013
Hindari Penipuan (Scams):	http://www.onguardonline.gov/topics/avoid-scams

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