Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

- **Mengenal Rekayasa Sosial**
- **Mengenal/Menghentikan Rekayasa Sosial**

Rekayasa Sosial

Sekilas

Salah satu pemikiran keliru perihal penyerang siber adalah bahwa mereka hanya menggunakan perangkat dan teknologi mutakhir untuk meretas komputer, akun atau alat komunikasi multiguna (alkom/mobile device). Hal ini kurang tepat. Penyerang siber tahu benar bahwa cara termudah mencuri informasi, membobol akun dan menyerang sistem komputer adalah dengan cara mengelabui penggunanya agar bertindak sembrono. Dalam edisi ini akan dibahas bagaimana cara kerja serangan rekayasa sosial serta apa yang bisa dilakukan agar terhindar dari upaya itu.

Editor Tamu

James Lyne (**@jameslyne**) adalah instruktur SANSbersertifikat serta pemimpin Research di Sophos. Beliau menganalisa dan mendalami hasil kreasi terbaru kriminalis siber. James juga perancang modul Metaploit (SEC580) dan Social Engineering (SEC567) di SANS.

Mengenal Rekayasa Sosial

Rekayasa sosial adalah serangan phikologis dengan tujuan mengecoh seseorang untuk melakukan hal yang seharusnya tidak dilakukan. Konsep itu bukanlah baru, sudah ada sejak ribuan tahun. Bayangkan aja para penipu atau pencoleng, kira-kira sama aksinya. Apa yang membuat teknologi sekarang menjadi lebih efektif digunakan oleh penyerang siber adalah karena tidak adanya kontak langsung, mereka sanggup menjelma menjadi apa saja dan jutaan orang diseluruh dunia menjadi sasarannya, salah satunya adalah Anda. Selain itu, gempuran rekayasa sosial ini sanggup menembus berbagai teknologi keamanan. Mari menyimak dua contoh berikut mengenai cara kerja sebuah retasan dan bagaimana pencegahannya.

Anda mendapatkan telepon dari seseorang yang mengaku bekerja di perusahaan layanan servis komputer, penyedia jasa layanan internet atau bahkan Microsoft Tech Support. Penelpon menjelaskan bahwa komputer Anda terus menerus memindai internet sehingga dikuatirkan terinfeksi virus dan mereka diperbantukan untuk mengatasi hal tersebut. Mereka menggunakan berbagai istilah teknis sekaligus menuntun Anda melakukan berbagai langkah rumit untuk memastikan bahwa komputer tidak aman. Sebagai contoh, bisa saja mereka meminta Anda mencari keberadaan berkas (file) tertentu di dalam komputer dan memberikan tuntuntan cara melakukannya. Bila berkas itu ditemukan, mereka akan berkilah bahwa itu adalah bukti komputer yang tertular program berbahaya, padahal sebenarnya itu berkas biasa yang memang ada disemua komputer di dunia ini. Bila mereka sukses ditahap ini, langkah berikutnya adalah menawarkan perangkat

Rekayasa Sosial

lunak keamanan atau meminta akses jarak jauh ke dalam komputer Anda untuk membantu proses perbaikan. Sebenarnya, perangkat lunak yang dijual adalah program berbahaya. Bila Anda membeli dan memasang perangkat lunak itu, Anda tidak hanya tertipu sebab menjadikan komputer malah terinfeksi, dan juga secara tidak langsung membayar mereka untuk semua itu. Bila akses jarak jauh diberikan, mereka akan mengambil alih kendali, mencuri data yang ada atau menggunakan komputer tersebut untuk melakukan aksi lainnya.

Akal sehat adalah perlindungan terbaik dalam mengenali dan menghentikan serangan rekayasa sosial.

Contoh lain ini sering terjadi di tempat kerja, metode serangan lewat surel yang dikenal sebagai Tipu Daya CEO (CEO Fraud). Penyerang siber mempelajari sebuah organisasi dari dunia internet, mengenali para pejabat dan karyawan. Mereka merancang surel sedemikian rupa sehingga seakan-akan berasal dari pejabat/rekan kerja di organisasi. Surel ini meminta Anda melakukan tindakan darurat, bisa saja transfer dana atau mengirimkan informasi karyawan yang sensitif. Tidak jarang malah mendorong Anda untuk mengabaikan prosedur keamanan, misalnya dengan meminta informasi sensitif dikirimkan ke alamat surel pribadi di @gmail. Cara tipu daya seperti ini sangat berbahaya karena pelaku mengerjakannya dengan sangat terstruktur. Tambahan pula, teknologi keamanan seperti anti-virus dan firewall tidak sanggup mendeteksi dan menghentikannya karena memang tidak menggunakan program komputer seperti biasa

Ingat, rekayasa sosial seperti itu tidak terbatas pada percakapan telepon atau surel, bisa saja melalui SMS yang dikirim ke alkom (alat komunikasi multiguna), melalui media sosial atau interaksi pribadi. Yang terpenting adalah bagaimana Anda menyikapinya, itulah cara pertahanan yang terbaik.

Mengenal/Menghentikan Rekayasa Sosial

Jangan kuatir, tidak susah mencegah berbagai rupa serangan itu., selalu gunakan akal sehat. Bila ada yang mencurigakan dan tidak meyakinkan, bisa saja itu upaya peretasan. Ciri-ciri serangan rekayasa sosial adalah sbb:

- Terciptanya suasana serba tergesa-gesa dengan harapan Anda teledor dan berbuat kesalahan.
- Seseorang meminta informasi yang rahasia atau sudah selayaknya mereka sudah tahu, seperti akun bank.
- Seseorang meminta sandi, tidak ada organisasi yang sah akan melakukan hal itu.

Rekayasa Sosial

- Seseorang memaksa Anda mengabaikan prosedur keamanan di tempat kerja.
- Sesuatu yang mengada-ada. Contoh: pemberitahuan Anda menjadi pemenang lotere, atau mendapatkan iPad walaupun Anda tidak pernah membeli lotere.
- Anda menerima surel yang tidak biasa dari teman kerja atau sahabat, dengan isi dan kalimat yang tidak lazim. Bisa saja peretas berhasil membobol akun mereka dan menggunakannya untuk mengelabui Anda. Agar terhindar dari hal ini, periksa ulang permintaan itu lewat percakapan lewat telepon atau tatap muka.

Bila Anda merasa ada pihak yang mencoba mengelabui atau memperdaya, hentikan komunikasi dengan orang tersebut. Bila hal ini berhubungan dengan pekerjaan di kantor, laporkan ke bagian layanan umum atau tim keamanan informasi. Ingat, akal sehat adalah pertahanan terbaik.

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

Sumber Pustaka

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Tipu Daya CEO:	https://securingthehuman.sans.org/ouch/2016#july2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH Archives:	https://securingthehuman.sans.org/ouch/archives

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