Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Tipu Daya CEO

Mengenal Tipu Daya CEO

Pelaku kejahatan siber cukup lihai, selalu berupaya menggunakan cara baru untuk memperoleh apa yang diinginkan. Salah satu cara paling efektif adalah dengan menjadikan Anda sebagai sasaran. Penyerang Siber percaya bahwa orang yang tidak sadar akan hal ini merupakan titik terlemah sebuah organisasi, namun mereka lupa bahwa orang yang paham benar seperti Anda para pembaca OUCH! bisa menjadi benteng perlindungan terpercaya sebuah organisasi.

Editor Tamu

Angela Pappas adalah direktur pelatihan dan kesadaran keamanan informasi di Thomson Reuters. Dalam tugasnya, Angela menangani program ambassador, eLearning dan mendidik karyawan perihal pengelabuan surel (phishing).

Kriminalis siber mengembangkan metode serangan baru yang dikenal sebagai Tipu Daya CEO, atau dikenal juga dengan sebutan Business Email Compromise (BEC – Pembobolan Surel Bisnis). Dalam model serangan ini, kriminalis siber berpura-pura menjadi seorang CEO atau eksekutif senior sebuah organisasi. Mereka akan mengirimkan surel ke karyawan agar melakukan sesuatu yang sepatutnya tidak dilakukan.Serangan ini biasanya sangat efektif karena pelaku sudah melakukan penelitian yang mendalam sebelum menjalankan aksinya. Mereka mempelajari situs web organisasi dan menggali banyak informasi seperti lokasi, nama-nama pimpinan eksekutif dan juga rekan bisnis organisasi. Selanjutnya dipelajari pula rekan kerja atau karyawan melalui situs seperti LinkeIn, Facebook dan Twitter. Begitu struktur organisasi sudah bisa dikenal, mulailah dipilih karyawan yang bisa menjadi sasaran jitu. Sasaran ditentukan sesuai dengan tujuan yang ingin diraih. Seandainya mengincar uang, mungkin staf bagian pembayaran akan menjadi sasaran. Bila menyasar urusan pajak, staf personalia bakal dijadikan sasaran. Bila menginginkan akses ke server database, bisa saja staff IT akan menjadi korbannya.

Segera setelah tahu apa yang diinginkan dan siapa yang akan dijadikan sasaran, mulailah dibuat rencana serangan. Biasanya menggunakan pengelabuan terarah (spear phishing). Pengelabuan (phishing) umumnya dilakukan dengan cara mengirimkan surel ke jutaan orang dengan tujuan memperdaya penerimanya agar membuka lampiran atau mengunjungi situs web yang terinfeksi. Pengelabuan terarah sebenarnya tidak banyak berbeda dengan phishing biasa, tapi dilakukan dengan tidak mengirimkan surel secara masal, sebagai gantinya digunakan surel khusus yang dialamatkan ke orang-

© SANS Institute 2016

Tipu Daya CEO

orang tertentu saja. Surel itu dibuat dengan tampilan yang menyakinkan dan tampak asli. Terkadang muncul seakan-akan berasal dari teman, rekan kerja atau bahkan atasan Anda. Surel ini diracik dengan gaya dan istilah yang lazim dipakai sesama rekan kerja, bahkan menggunakan logo organisasi dan bisa saja mencomot tandatangan resmi pejabat organisasi. Surel seperti ini akan membuat penerimanya merasa perlu melakukan sebuah aksi/ tindakan tanpa sepengetahuan pihak lain. Dalam kondisi mendesak ini diharapkan penerima surel akan melakukan sebuah keteledoran/kekeliruan. Berikut ini skenario yang sering dipakai:

Tipu Daya CEO tergolong ampuh dan sanggup menerobos pertahanan keamanan. Pada akhirnya, Anda adalah perlindungan terbaik.

Transfer Dana: Tujuannya adalah uang. Artinya pelaku kejahatan akan mencari tahu dan mempelajari orang-orang yang bekerja di bagian pembayaran atau tim pengelola keuangan organisasi. Selanjutnya mereka akan merancang dan mengirimkan surel seakan-akan dari pihak atasan, menyatakan adanya kondisi darurat serta perlunya dana untuk ditransfer ke rekening tertentu.

Penipuan Pajak: Kriminalis siber ingin mendapatkan informasi rekan kerja agar bisa menggunakan identitasnya untuk tujuan penipuan pajak. Mereka mempelajari organisasi untuk menentukan siapa saja yang menangani informasi karyawan, sebagai misal seseorang dibagian personalia. Selanjutnya, mereka akan mengirimkan surel palsu seakan-akan berasal dari pejabat senior atau bagian hukum yang meminta dokumen tertentu dengan segera.

Pengacara Gadungan: Tidak semua tipu daya CEO dalam bentuk surel, metode lain seperti penggunaan telpon bisa saja dipakai. Dalam skenario ini, pelaku kejahatan akan mengirimkan surel dengan berpura-pura sebagai pimpinan senior, menyatakan bahwa seorang pengacara akan menelpon untuk membicarakan satu hal yang mendesak. Selanjutnya pelaku akan menelpon Anda dan berpura-pura sebagai pengacara. Mereka akan menciptakan suasana krisis pada saat membicarakan hal-hal yang bersifat penting dan rahasia. Kondisi krisis inilah yang membuat Anda bertindak tanpa berpikir lebih panjang.

Perlindungan Diri

Apa yang dapat dilakukan untuk melindungi diri dan organisasi? Akal sehat adalah perlindungan terbaik. Bila menerima pesan dari atasan atau rekan kerja namun diragukan kebenarannya, mungkin saja itu sebuah upaya serangan. Ciri-cirinya

Tipu Daya CEO

adalah upaya untuk menciptakan kondisi tergesa-gesa/krisis, pencantuman tandatangan yang tidak dikenal atau nada bicara yang aneh dan bisa juga nama yang digunakan dalam surel tidak sesuai dengan orang yang menelpon Anda. Tanda lainnya adalah penggunaan alamat surel dan nomer telpon yang belum pernah Anda kenal atau bisa juga menggunakan alamat surel yang hampir mirip dengan alamat surel rekan kerja atau atasan. Bila ada keraguan, telponlah orang tersebut dengan menggunakan nomer telpon terpercaya atau lakukan tatap muka (jangan membalas surel) dan lakukan pengecekan apakah memang melakukan pengiriman surel. Jangan pernah melanggar aturan dan prosedur keamanan. Organisasi Anda mungkin memiliki aturan dalam hal otorisasi pengiriman dana atau pengungkapan informasi rahasia. Permintaan untuk melanggar aturan tersebut apapun alasannya, harus dicurigai dan dikaji ulang sebelum sebuah tindakan dilakukan. Bila Anda menerima permintaan seperti itu dan tidak yakin apa yang harus dilakukan, hubungi segera atasan, help desk atau staf keamanan informasi.

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

Rekayasa Sosial:	https://securingthehuman.sans.org/ouch/2014#november2014
Surel Pengelabuan:	https://securingthehuman.sans.org//ouch/2015#december2015
Mengenal Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Verifikasi 2 Tahap:	https://securingthehuman.sans.org/ouch/2015#september2015
Tip harian:	https://www.sans.org/tip-of-the-day

OUCH! diterbitkan oleh SANS “Securing The Human” dan didistribusikan sesuai lisensi Creative Commons BY-NC-ND 4.0. Anda diperkenankan menyebarkan buletin ini atau menggunakannya di dalam program pembelajaran sejauh tidak melakukan pengubahan isi buletin. Untuk keperluan alih bahasa atau informasi lainnya, silakan menghubungi ouch@securingthehuman.org.

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