Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

Pengendalian Sosial

Pengenalan

Tanggapan salah orang ramai tentang penyerang siber ialah mereka hanya menggunakan peralatan menggodam canggih dan berteknologi tinggi untuk memecah masuk komputer, akaun dan peranti mudah alih. Ini tidak betul sama sekali. Penyerang siber telah arif bahawa cara yang paling mudah untuk mencuri maklumat atau menggodam komputer anda adalah semudah bercakap dan mengelirukan anda. Di dalam surat berita ini, kita akan mempelajari bagaimana serangan yang dipanggil pengendalian sosial berfungsi dan langkah yang boleh diambil untuk melindungi diri anda.

Editor Jemputan

Alissa Torres merupakan pengajar SANS yang diiktiraf dan juga pakar dalam bidang forensik komputer lanjutan dan tindak balas terhadap insiden. Pengalaman beliau dalam industri termasuklah berkhidmat di barisan hadapan sebagai pengendali insiden dan bekerja sebagai penyiasat forensik digital di dalam kumpulan keselamatan dalaman. Alissa lebih dikenali di laman sosial Twitter sebagai **@sibertor**.

Pengendalian Sosial

Pengendalian sosial merupakan sejenis serangan psikologi di mana penyerang mengelirukan anda untuk melakukan sesuatu yang mereka kehendaki secara rela. Pengendalian sosial telah wujud sejak beribu tahun yang lalu, menunjukkan bahawa ide untuk menipu dan memperdayakan seseorang bukanlah baharu. Walaubagaimanapun, penyerang siber mempelajari bahawa teknik tersebut sangat berkesan jika digunakan di internet dan ia boleh disasarkan kepada jutaan pengguna. Cara termudah untuk memahami bagaimana pengendalian sosial berfungsi adalah dengan melihat contoh sebenar yang berlaku di sekeliling anda.

Anda menerima panggilan daripada seseorang yang mengakui mereka dari syarikat sokongan komputer, penyedia perkhidmatan internet atau mungkin juga dari khidmat sokongan Microsoft. Pemanggil kemudian menerangkan bahawa mereka telah mengesan sesuatu yang aneh telah berlaku kepada komputer anda, seperti membuat imbasan di internet atau menghantar spam, dan mereka percaya komputer anda telah dijangkiti. Mereka ditugaskan untuk menyiasat perkara ini dan membantu melindungi komputer anda. Mereka kemudiannya menggunakan terma teknikal dan langkah-langkah yang mengelirukan untuk meyakinkan anda bahawa komputer anda telah dijangkiti.

Sebagai contoh, mereka mungkin akan meminta anda menyemak fail tertentu di dalam komputer dan mengajar anda bagaimana untuk mencarinya. Apabila anda menjumpai fail tersebut, pemanggil akan meyakinkan anda bahawa fail tersebut adalah tanda komputer anda telah dijangkiti, sedangkan realitinya fail tersebut merupakan fail biasa yang terdapat di dalam setiap komputer. Setelah mereka berjaya meyakinkan anda bahawa komputer anda telah dijangkiti, mereka akan memberi tekanan supaya anda membeli perisian keselamatan mereka atau meminta supaya anda membenarkan mereka membuat capaian kepada komputer anda supaya mereka boleh membetulkannya. Walaubagaimanapun, perisian yang mereka jual sebenarnya merupakan program yang berniat jahat. Jika anda beli perisian

Pengendalian Sosial

tersebut, bukan sahaja mereka berjaya menipu anda untuk menjangkiti komputer anda, malah anda membayar mereka untuk melakukannya. Jika anda memberikan kebenaran untuk melakukan capaian jarak jauh kepada komputer anda untuk diperbaiki, realitinya mereka akan menjangkitinya.

Perlu diingat bahawa serangan pengendalian sosial seperti ini tidak terhad kepada panggilan telefon sahaja; ia boleh dilakukan dengan hampir kesemua teknologi, termasuk serangan phishing melalui e-mel, khidmat pesanan ringkas, pesanan Facebook, pos Twitter atau perbualan dalam talian. Kuncinya adalah untuk mengetahui apa yang perlu dicari.

Mempelajari cara-cara menghalang, mengesan dan menghentikan serangan pengendalian sosial merupakan salah satu langkah paling efektif yang boleh anda ambil untuk melindungi diri anda.

Mengesan/Menghentikan Serangan Pengendalian Sosial

Cara paling mudah untuk melindungi diri anda daripada serangan pengendalian sosial ini adalah dengan menggunakan akal fikiran. Jika sesuatu kelihatan mencurigakan atau tidak kena, berkemungkinan ia merupakan satu serangan. Beberapa petunjuk serangan pengendalian sosial termasuklah:

- Seseorang mencipta situasi yang amat tertekan. Anda perlu berwaspasa jika anda digesa untuk membuat sesuatu keputusan dengan segera.
- Seseorang meminta maklumat yang mereka tidak sepatutnya mempunyai akses atau maklumat yang sepatutnya mereka sudah tahu.
- Sesuatu yang terlalu baik untuk dipercayai. Contoh biasa adalah apabila anda dimaklumkan bahawa anda memenangi loteri, walaupun anda tidak pernah menyertainya.

Jika anda mengesyaki sesorang cuba menjadikan anda mangsa serangan pengendalian sosial, berhenti berkomunikasi dengannya. Jika seseorang itu menelefon anda, tamatkan perbualan. Jika seseorang itu berbual dengan anda di dalam talian, putuskan talian. Jika ianya e-mel yang anda tidak percaya, padamkannya. Jika serangan cenderung di tempat kerja anda, pastikan anda melaporkannya kepada meja sokongan atau kumpulan keselamatan maklumat dengan serta merta.

Menghalang Serangan Pengendalian Sosial Di Masa Depan

Terdapat beberapa langkah yang boleh diambil untuk melindungi diri anda daripada serangan pengendalian sosial di masa depan.

- **Jangan Sekali-kali Berkongsi Kata Laluan**. Sesebuah organisasi tidak akan menghubungi anda dan meminta kata laluan anda. Jika seseorang bertanyakan kata laluan anda, ia adalah satu serangan.

Pengendalian Sosial

- **Jangan Kongsi Terlalu Banyak**. Semakin banyak penyerang tahu tentang anda, semakin mudah untuk mereka memperdayakan anda untuk melakukan apa yang mereka mahukan. Walaupun dengan hanya berkongsi sedikit maklumat tentang diri anda, lama kelamaan maklumat tersebut boleh digabungkan untuk menghasilkan maklumat lengkap tentang diri anda.

- **Sahkan Kenalan**. Kadang-kala anda mungkin akan dihubungi oleh pihak bank, syarikat kad kredit, penyedia perkhidmatan mudah alih atau organisasi lain untuk tujuan yang sah. Jika anda ragu-ragu sama ada permintaan untuk mendapatkan maklumat anda itu adalah sah, minta nama dan nombor sambungan pegawai tersebut. Kemudian cari nombor telefon syarikat berkenaan dari sumber yang boleh dipercayai seperti nombor yang tertera di belakang kad kredit anda, nombor pada penyata bank anda atau nombor daripada laman sesawang syarikat tersebut (pastikan anda menaip sendiri URL di dalam pelayar). Dengan cara ini, apabila anda menghubungi organisasi tersebut, anda tahu bahawa anda sedang bercakap dengan pegawai mereka yang sah. Ia kelihatan agak rumit tetapi langkah tambahan untuk menjaga identiti dan maklumat peribadi anda adalah amat berbaloi.

Mari Belajar Lebih Lanjut!

Langganilah surat berita bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer OUCH!, akseslah arkib OUCH!, dan belajar lebih lanjut mengenai penyelesaian kesedaran keselamatan SANS dengan melayari laman sesawang kami di http://www.securingthehuman.org.

Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: http://snsc.skmm.gov.my/.

Sumber

Email Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
Social Networking Safely:	http://www.securingthehuman.org/ouch/2013#march2013
Avoid Scams:	http://www.onguardonline.gov/topics/avoid-scams

Editor: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated by: Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie