Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

Ya, Anda Memang Sasaran

Pengenalan

Ramai orang beranggapan bahawa mereka bukan sasaran jenayah siber- yakni mereka atau komputer mereka tidak bernilai kepada sesiapa. Ini adalah anggapan yang tidak benar. Jika anda mempunyai komputer, peranti mudah alih, akaun dalam talian, alamat e-mel, kad kredit, atau melakukan sebarang aktiviti dalam talian, anda sebenarnya sangat bernilai kepada penjenayah. Dalam newsletter ini kami akan menerangkan mengapa anda menjadi sasaran, bagaimana anda diserang dan apa yang boleh anda lakukan untuk melindungi diri anda.

Editor Jemputan

Eric Conrad adalah Presiden dan Ketua Pegawai Teknikal di Backshore Communications dan merupakan pengarang utama buku-buku CISSP Study Guide, Edisi Kedua dan Eleventh Hour CISSP, Edisi Kedua. Beliau juga merupakan pengarang bersama untuk kursus enam hari Continuous Monitoring and Security Operations (SEC511) di SANS.

Mengapa Anda Menjadi Sasaran

Jenayah seperti penipuan, kecurian identiti atau peras ugut telah wujud sejak bermulanya tamadun manusia, ia menjadi sebahagian daripada kehidupan seharian kita. Matlamat penjenayah tetap sama iaitu untuk menjana sebanyak wang yang mungkin, semudah yang mungkin dan dengan risiko yang terendah. Pada dasarnya, ia sesuatu yang sukar kerana faktor lokasi dan interaksi secara fizikal antara penjenayah dengan mangsa yang terhad. Bukan sahaja terhad kepada mangsa yang dicari malahan ia akan mendedahkan penjenayah kepada risiko yang besar. Walaubagaimanapun, jenayah telah banyak berubah dengan kehadiran internet dan teknologi dalam talian. Sekarang, penjenayah siber boleh menjadikan sesiapa sahaja di dunia ini sebagai sasaran dengan kos yang rendah atau amat minima dan dengan kadar risiko yang rendah. Selain itu, penjenayah siber kini teratur dan cekap serta lebih efektif berbanding dahulu.

Disamping itu, penjenayah siber tahu bahawa semakin banyak kad kredit yang mereka curi, semakin banyak akaun bank yang mereka godam, atau lebih banyak kata laluan yang mereka peroleh, maka lebih banyak wang yang boleh mereka curi. Mereka akan membuat cubaan untuk menggodam sesiapa sahaja yang berkait dengan internet, termasuk diri anda. Menggodam jutaan orang di serata dunia mungkin kelihatan seperti sesuatu kerja yang banyak, sebaliknya ia amat mudah kerana mereka menggunakan perisian automatik untuk melakukan kerja-kerja jenayah mereka. Sebagai contoh, mereka mungkin membina pangkalan data yang terdiri daripada jutaan alamat e-mel dan menggunakan peralatan automasi untuk menghantar pesanan phishing kepada setiap satu alamat e-mel tersebut. Kos untuk menghantar e-mel-e-mel tersebut hampir tiada: mereka menggunakan komputer lain yang telah digodam, mungkin juga kepunyaan anda, untuk melakukan kerja kotor mereka. Ini juga merupakan salah satu sebab mengapa peranti anda bernilai, dan boleh digunakan untuk meng-

Ya, Anda Memang Sasaran

godam atau membahayakan orang lain. Disamping itu, penjenayah ini tidak tahu siapa yang akan menjadi mangsa kepada serangan e-mel mereka, tetapi mereka tahu semakin banyak e-mel dihantar, semakin ramailah yang menjadi mangsa. Atau mungkin penjenayah akan mengimbas setiap komputer di internet (sekali lagi menggunakan komputer yang telah digodam untuk membuat imbasan), mencari sebarang komputer atau peranti yang boleh mereka godam. Ingat, anda tidak akan terlepas kerana anda istimewa. Sebaliknya, penjenayah menyasarkan kepada semua yang boleh, termasuklah diri anda.

Anda mungkin tidak menyedarinya, tetapi peranti anda dan maklumat anda mempunyai nilai yang tidak terhingga pada penjenayah siber di seluruh dunia.

Melindungi Diri Anda

Apabila penjenayah siber membuat cubaan untuk menggodam komputer di seluruh dunia, mereka hanya menggunakan kaedah yang mudah. Mujurlah, dengan menggunakan langkah yang hampir sama anda boleh melindungi diri anda. Antara langkah yang kami syorkan termasuk yang berikut:

- **Diri Anda**: Pucuk pangkalnya, terletak ditangan anda sendiri kerana andalah pertahanan paling terkehadapan dengan sebarang serangan siber. Kebanyakan serangan bermula dengan penjenayah siber cuba untuk menipu atau memperalatkan anda, seperti memperdayakan anda untuk membuka pautan e-mel atau memperalatkan anda untuk memberikan kata laluan anda di dalam telefon. Sebenarnya, logik akal merupakan pertahanan terbaik bagi anda: jika ada sesuatu yang kelihatan janggal, mencurigakan atau terlalu bagus untuk dipercayai, kemungkinan besar ia adalah satu serangan.

- **Kemas Kini**: Pastikan komputer atau peranti mudah alih yang anda gunakan telah dikemas kini dan mempunyai tampalan terkini. Ini bukan sahaja penting untuk sistem operasi anda, tetapi untuk sebarang aplikasi atau pemalam yang anda gunakan. Dengan memastikan sistem dan aplikasi anda terkini, anda membantu untuk melindungi diri anda daripada serangan lazim.

- **Kata Laluan**: Gunakan kata laluan yang unik dan kukuh untuk setiap akaun anda. Dengan itu jika laman sesawang yang anda gunakan digodam dan kesemua kata laluan telah dicuri (termasuk akaun anda) akaun anda yang lain masih selamat. Pastikan juga kesemua peranti anda dilindungi oleh kata laluan yang kukuh danunik, PIN atau sebarang mekanisme untuk mengunci. Untuk memantau kesemua kata laluan berbeza anda dengan selamat kami mengesyorkan anda menggunakan pengurus kata laluan.

Ya, Anda Memang Sasaran

- **Kad Kredit**: Semak penyata kewangan anda sekerap mungkin, kami mengesyorkan sekurang-kurangnya sekali seminggu (sebulan sekali tidak cukup). Sebaik sahaja anda melihat sebarang transaksi yang tidak dibenarkan dalam kad kredit anda, laporkan secepat mungkin pada bankanda. Jika bank membenarkan penghantaran makluman melalui e-mel atau pesanan teks untuk transaksi yang ganjil atau amaun yang banyak, gunakan penghantaran makluman tersebut untuk pemberitahuanyang lebih cepat sekiranya berlaku aktiviti yang mencurigai.

- **Rangkaian Anda**: Lindungi rangkaian pusat akses tanpa wayar rumah anda dengan kata laluan pentadbir yang kukuh dan pastikan rangkaian tanpa wayar anda memerlukan kata laluan untuk sesiapa menyertainya. Juga pastikan anda tahu peranti apa yang telah anda sambungkan kepada rangkaian rumah anda dan kesemua peranti tersebut di kemas kini.

- **Media Sosial**: Lebih banyak maklumat yang anda masukkan dalam talian bermakna anda lebih berisiko. Maklumat yang anda kongsi bukan sahaja menjadikannya lebih mudah untuk penjenayah menjadikan anda sebagai sasaran, tetapi sebarang maklumat yang anda pos menjadikan anda sasaran yang lebih bernilai.

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

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

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