OUCH!

SANS SECURITY AWARENESS

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

CEO Gadungan / BEC

Mengenal CEO Gadungan / BEC

Penyerang siber terus menyempurnakan jenis serangan yang dikenal sebagai CEO Gadungan atau Pembobolan Surel Bisnis (Business Email Compromise – BEC). Ini adalah serangan melalui surel dengan tujuan agar sasaran melakukan tindakan yang seharusnya tidak dilakukan. Pelaku sering kali bertujuan untuk mendapatkan uang. Yang menjadikan serangan jenis ini berbahaya adalah bagaimana pelaku tidak sembarangan (tidak acak) menentukan sasaran sebelum melakukan tindakan. Selain itu, sangat sulit dilakukan pencegahan karena serangan jenis ini tidak menggunakan surel berisi lampiran terinfeksi atau upaya berbahaya lainnya. Berikut ini adalah cara kerjanya:

Penyerang siber menggunakan internet untuk meneliti calon sasaran dan orang-orang yang berinteraksi dengannya. Contoh, bila Anda sebagai sasaran, mereka akan meniliti siapa atasan Anda di kantor atau mungkin agen property mitra kerja Anda. Kemudian mereka merancang surel, berpura-pura sebagai salah satu dari orang yang Anda kenal itu dan mengirimkannya ke Anda. Surel tersebut bersifat penting, mewajibkan Anda segera melakukan sebuah tindakan, seperti pemrosesan tagihan, mengubah penerima pembayaran atau dengan meyakinkan meminta Anda menjawab seurel disertai lampiran dokumen sensitif (rahasia). Esensi isi surel itu adalah memaksa Anda melakukan apa yang mereka mau. Ini ada dua (2) contoh bagaimana hal itu bisa terjadi.

Transfer Dana: Sasaran kriminalis siber adalah uang. Mereka meneliti perusahaan dimana Anda bekerja, misalnya mencari tahu siapa yang bekerja dibagian pembayaran hutang atau orang yang bertanggung jawab mentransfer dana. Kemudian mereka merancang dan mengirim surel ke orang-orang itu,berpura-pura sebagai atasan atau eksekutif senior. Surel itu menjelaskan adanya sebuah situasi sangat mendesak dan sejumlah dana harus segera ditransfer ke rekening baru. Surel tersebut mendesak pembacanya agar teledor dan bertindak salah dengan mengirim dana tersebut ke rekening pelaku kejahatan.

Penggelapan Pajak: Kriminalis siber mencari informasi pribadi seseorang untuk melakukan penggelapan pajak. Cara paling cepat adalah mencuri data karyawan sebuah perusahaan. Kriminalis siber mencari tahu siapa yang bekerja dibagian personalia/HR. Mereka akan mengirim surel palsu ke orang-orang itu, berpura-pura sebagai eksekutif senior atau dari bagian Hukum. Surel itu menimbulkan kepanikan tersendiri karena meminta informasi pajak semua karyawan harus segera dikirim. Orang di bagian personalia/HR mengira mengirimkan informasi sensitif itu ke eksekutif senior padahal sebenarnya dikirim ke kriminalis siber.

Lindungi Diri

Jadi apa yang harus dilakukan untuk perlindungan diri? Berpikir logis adalah pilihan terbaik. Berikut adalah ciri-ciri yang bisa diamati:

- **Isi surel sangat singkat dan penting (hanya beberapa kalimat), dibagian bawah tercantum bahwa surel ini dikirim dari gawas/alkom.**
- **Muncul keadaan tergesa-gesa, memaksa Anda mengabaikan atau melanggar aturan yang ada. Selalu ikuti aturan dan prosedur pekerjaan, bahkan bila surel itu tampak berasal dari atasan atau bahkan CEO.**
- **Surel untuk tujuan bisnis namun menggunakan alamat surel pribadi seperti @gmail.com atau @hotmail.com.**
- **Surel itu tampak berasal dari pimpinan senior, rekan kerja atau rekanan yang Anda kenal atau tahu, namun surel tersebut tidak seperti biasanya/terkesan aneh.**
- **Perintah pembayaran dijelaskan namun perintah ini berbeda dari biasanya, mungkin meminta pembayaran secepatnya ke nomer akun bank berbeda.**

Bila Anda curiga telah menjadi sasaran di tempat kerja, hentikan semua interaksi dengan pelaku dan laporkan ke atasan Anda. Bila Anda menjadi sasaran di rumah, atau sudah menjadi korban karena telah mengirim dana, laporkan hal tersebut ke bank dan ke pihak berwajib.

Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: http://www.bipimax.net

Editor Tamu

Don Cavender *adalah mantan Agen Khusus FBI, dengan lebih dari 22 tahun pengalaman di bidang forensik digital dan kejahatan siber. Sebagai koordinator Washing DC BEC, tidak asing lagi dengan kejahatan siber. Beliau memberikan pelatihan serta melakukan penelitian di bidang forensik digital dan investigasi siber. Don hadir di Twitter sebagai* @don_cavender https://www.linkedin.com/in/donald-cavender

Sumber Pustaka

Rekayasa Sosial:	https://www.sans.org/u/HE3
Stop Pengelabuan:	https://www.sans.org/u/HE8
Menangkal Malware:	https://www.sans.org/u/HEd
Amankan Akun Anda:	https://www.sans.org/u/HEi