Seluk Beluk Teknik Social Engineering

Prof. Richardus Eko Indrajit

Ada prinsip dalam dunia keamanan jaringan yang berbunyi "kekuatan sebuah rantai tergantung dari atau terletak pada sambungan yang terlemah" atau dalam bahasa asingnya "the strength of a chain depends on the weakest link". Apa atau siapakah "the weakest link" atau "komponen terlemah" dalam sebuah sistem jaringan komputer? Ternyata jawabannya adalah: manusia. Walaupun sebuah sistem telah dilindungi dengan piranti keras dan piranti lunak canggih penangkal serangan seperti firewalls, anti virus, IDS/IPS, dan lain sebagainya – tetapi jika manusia yang mengoperasikannya lalai, maka keseluruhan peralatan itu tidaklah ada artinya. Para kriminal dunia maya paham betul akan hal ini sehingga kemudian mereka mulai menggunakan suatu kiat tertentu yang dinamakan sebagai "social engineering" untuk mendapatkan informasi penting dan krusial yang disimpan secara rahasia oleh manusia.

Kelemahan Manusia

Menurut definisi, "social engineering" adalah suatu teknik 'pencurian' atau pengambilan data atau informasi penting/krusial/rahasia dari seseorang dengan cara menggunakan pendekatan manusiawi melalui mekanisme interaksi sosial. Atau dengan kata lain social engineering adalah suatu teknik memperoleh data/informasi rahasia dengan cara mengeksploitasi kelemahan manusia. Contohnya kelemahan manusia yang dimaksud misalnya:

- Rasa Takut – jika seorang pegawai atau karyawan dimintai data atau informasi dari atasannya, polisi, atau penegak hukum yang lain, biasanya yang bersangkutan akan langsung memberikan tanpa merasa sungkan;
- Rasa Percaya – jika seorang individu dimintai data atau informasi dari teman baik, rekan sejawat, sanak saudara, atau sekretaris, biasanya yang bersangkutan akan langsung memberikannya tanpa harus merasa curiga; dan
- Rasa Ingin Menolong – jika seseorang dimintai data atau informasi dari orang yang sedang tertimpa musibah, dalam kesedihan yang mendalam, menjadi korban bencana, atau berada dalam duka, biasanya yang bersangkutan akan langsung memberikan data atau informasi yang diinginkan tanpa bertanya lebih dahulu.

Tipe Social Engineering

Pada dasarnya teknik social engineering dapat dibagi menjadi dua jenis, yaitu: berbasis interaksi sosial dan berbasis interaksi komputer. Berikut adalah sejumlah teknik social engineering yang biasa dipergunakan oleh kriminal, musuh, penjahat, penipu, atau mereka yang memiliki intensi tidak baik. Dalam skenario ini yang menjadi sasaran penipuan adalah individu yang bekerja di divisi teknologi informasi perusahaan. Modus operandinya sama, yaitu melalui medium telepon.

Skenario 1 (Kedok sebagai User Penting)

Seorang penipu menelpon help desk bagian divisi teknologi informasi dan mengatakan hal sebagai berikut "*Halo, di sini pak Abraham, Direktur Keuangan. Saya mau log in tapi lupa*

password saya. Boleh tolong beritahu sekarang agar saya dapat segera bekerja?". Karena takut – dan merasa sedikit tersanjung karena untuk pertama kalinya dapat berbicara dan mendengar suara Direktur Keuangan perusahaannya – yang bersangkutan langsung memberikan password yang dimaksud tanpa rasa curiga sedikitpun. Si penipu bisa tahu nama Direktur Keuangannya adalah Abraham karena melihat dari situs perusahaan.

Skenario 2 (Kedok sebagai User yang Sah)

Dengan mengaku sebagai rekan kerja dari departemen yang berbeda, seorang wanita menelepon staf junior teknologi informasi sambil berkata *"Halo, ini Iwan ya? Wan, ini Septi dari Divisi Marketing, dulu kita satu grup waktu outing kantor di Cisarua. Bisa tolong bantu reset password-ku tidak? Dirubah saja menjadi tanggal lahirku. Aku takut ada orang yang tahu passwordku, sementara saat ini aku di luar kantor dan tidak bisa merubahnya. Bisa bantu ya?"*. Sang junior yang tahu persis setahun yang lalu merasa berjumpa Septi dalam acara kantor langsung melakukan yang diminta rekan sekerjanya tersebut tanpa melakukan cek dan ricek. Sementara kriminal yang mengaku sebagai Septi mengetahui nama-nama terkait dari majalah dinding "Aktivitas" yang dipajang di lobby perusahaan – dan nomor telepon Iwan diketahuinya dari Satpam dan/atau receptionist.

Skenario 3 (Kedok sebagai Mitra Vendor)

Dalam hal ini penjahat yang mengaku sebagai mitra vendor menelepon bagian operasional teknologi informasi dengan mengajak berbicara hal-hal yang bersifat teknis sebagai berikut: *"Pak Aryo, saya Ronald dari PT Teknik Alih Daya Abadi, yang membantu outsource file CRM perusahaan Bapak. Hari ini kami ingin Bapak mencoba modul baru kami secara cuma-cuma. Boleh saya tahu username dan password Bapak agar dapat saya bantu instalasi dari tempat saya? Nanti kalau sudah terinstal, Bapak dapat mencoba fitur-fitur dan fasilitas canggih dari program CRM versi terbaru."* Merasa mendapatkan kesempatan, kepercayaan, dan penghargaan, yang bersangkutan langsung memberikan username dan passwordnya kepada si penjahat tanpa merasa curiga sedikitpun. Sekali lagi sang penjahat bisa tahu nama-nama yang bersangkutan melalui berita-berita di koran dan majalah mengenai produk/jasa PT Teknik Alih Daya Abadi dan nama-nama klien utamanya.

Skenario 4 (Kedok sebagai Konsultan Audit)

Kali ini seorang penipu menelpon Manajer Teknologi Informasi dengan menggunakan pendekatan sebagai berikut: *"Selamat pagi Pak Basuki, nama saya Roni Setiadi, auditor teknologi informasi eksternal yang ditunjuk perusahaan untuk melakukan validasi prosedur. Sebagai seorang Manajer Teknologi Informasi, boleh saya tahu bagaimana cara Bapak melindungi website perusahaan agar tidak terkena serangan defacement dari hacker?"*. Merasa tertantang kompetensinya, dengan panjang lebar yang bersangkutan cerita mengenai struktur keamanan website yang diimplementasikan perusahaannya. Tentu saja sang kriminal tertawa dan sangat senang sekali mendengarkan bocoran kelemahan ini, sehingga mempermudah yang bersangkutan dalam melakukan serangan.

Skenario 5 (Kedok sebagai Penegak Hukum)

Contoh terakhir ini adalah peristiwa klasik yang sering terjadi dan dipergunakan sebagai pendekatan penjahat kepada calon korbannya: *"Selamat sore Pak, kami dari Kepolisian yang bekerjasama dengan Tim Insiden Keamanan Internet Nasional. Hasil monitoring kami memperlihatkan sedang ada serangan menuju server anda dari luar negeri. Kami bermaksud untuk melindunginya. Bisa tolong diberikan perincian kepada kami mengenai topologi dan spesifikasi jaringan anda secara detail?"*. Tentu saja yang bersangkutan biasanya langsung

memberikan informasi penting tersebut karena merasa takut untuk menanyakan keabsahan atau keaslian identitas penelpon.

Sementara itu untuk jenis kedua, yaitu menggunakan komputer atau piranti elektronik/digital lain sebagai alat bantu, cukup banyak modus operandi yang sering dipergunakan seperti:

Skenario 1 (Teknik Phishing – melalui Email)

Strategi ini adalah yang paling banyak dilakukan di negara berkembang seperti Indonesia. Biasanya si penjahat menyamar sebagai pegawai atau karyawan sah yang merepresentasikan bank. Email yang dimaksud berbunyi misalnya sebagai berikut:

"Pelanggan Yth. Sehubungan sedang dilakukannya upgrade sistem teknologi informasi di bank ini, maka agar anda tetap mendapatkan pelayanan perbankan yang prima, mohon disampaikan kepada kami nomor rekening, username, dan password anda untuk kami perbaharui. Agar aman, lakukanlah dengan cara me-reply electronic mail ini. Terima kasih atas perhatian dan koordinasi anda sebagai pelanggan setia kami.

Wassalam,

Manajer Teknologi Informasi"

Bagaimana caranya si penjahat tahu alamat email yang bersangkutan? Banyak cara yang dapat diambil, seperti: melakukan searching di internet, mendapatkan keterangan dari kartu nama, melihatnya dari anggota mailing list, dan lain sebagainya.

Skenario 2 (Teknik Phishing – melalui SMS)

Pengguna telepon genggam di Indonesia naik secara pesat. Sudah lebih dari 100 juta nomor terjual pada akhir tahun 2008. Pelaku kriminal kerap memanfaatkan fitur-fitur yang ada pada telepon genggam atau sejenisnya untuk melakukan social engineering seperti yang terlihat pada contoh SMS berikut ini:

"Selamat. Anda baru saja memenangkan hadiah sebesar Rp 25,000,000 dari Bank X yang bekerjasama dengan provider telekomunikasi Y. Agar kami dapat segera mentransfer uang tunai kemenangan ke rekening bank anda, mohon diinformasikan user name dan passoword internet bank anda kepada kami. Sekali lagi kami atas nama Manajemen Bank X mengucapkan selamat atas kemenangan anda…"

Skenario 3 (Teknik Phishing – melalui Pop Up Windows)

Ketika seseorang sedang berselancar di internet, tiba-tiba muncul sebuah "pop up window" yang bertuliskan sebagai berikut:

"Komputer anda telah terjangkiti virus yang sangat berbahaya. Untuk membersihkannya, tekanlah tombol BERSIHKAN di bawah ini."

Tentu saja para awam tanpa pikir panjang langsung menekan tombol BERSIHKAN yang akibatnya justru sebaliknya, dimana penjahat berhasil mengambil alih komputer terkait yang dapat dimasukkan virus atau program mata-mata lainnya.

Jenis Social Engineering Lainnya

Karena sifatnya yang sangat "manusiawi" dan memanfaatkan interaksi sosial, teknik-teknik memperoleh informasi rahasia berkembang secara sangat variatif. Beberapa contoh adalah sebagai berikut:

- Ketika seseorang memasukkan password di ATM atau di PC, yang bersangkutan "mengintip" dari belakang bahu sang korban, sehingga karakter passwordnya dapat terlihat;
- Mengaduk-ngaduk tong sampah tempat pembuangan kertas atau dokumen kerja perusahaan untuk mendapatkan sejumlah informasi penting atau rahasia lainnya;
- Menyamar menjadi "office boy" untuk dapat masuk bekerja ke dalam kantor manajemen atau pimpinan puncak perusahaan guna mencari informasi rahasia;
- Ikut masuk ke dalam ruangan melalui pintu keamanan dengan cara "menguntit" individu atau mereka yang memiliki akses legal;
- Mengatakan secara meyakinkan bahwa yang bersangkutan terlupa membawa ID-Card yang berfungsi sebagai kunci akses sehingga diberikan bantuan oleh satpam;
- Membantu membawakan dokumen atau tas atau notebook dari pimpinan dan manajemen dimana pada saat lalai yang bersangkutan dapat memperoleh sejumlah informasi berharga;
- Melalui chatting di dunia maya, si penjahat mengajak ngobrol calon korban sambil pelan-pelan berusaha menguak sejumlah informasi berharga darinya;
- Dengan menggunakan situs social networking – seperti facebook, myspace, friendster, dsb. – melakukan diskursus dan komunikasi yang pelan-pelan mengarah pada proses "penelanjangan" informasi rahasia;
- dan lain sebagainya.

Target Korban Social Engineering

Statistik memperlihatkan, bahwa ada 4 (empat) kelompok individu di perusahaan yang kerap menjadi korban tindakan social engineering, yaitu:

1. Receptionist dan/atau Help Desk sebuah perusahaan, karena merupakan pintu masuk ke dalam organisasi yang relatif memiliki data/informasi lengkap mengenai personel yang bekerja dalam lingkungan dimaksud;
2. Pendukung teknis dari divisi teknologi informasi – khususnya yang melayani pimpinan dan manajemen perusahaan, karena mereka biasanya memegang kunci akses penting ke data dan informasi rahasia, berharga, dan strategis;
3. Administrator sistem dan pengguna komputer, karena mereka memiliki otoritas untuk mengelola manajemen password dan account semua pengguna teknologi informasi di perusahaan;

4. Mitra kerja atau vendor perusahaan yang menjadi target, karena mereka adalah pihak yang menyediakan berbagai teknologi beserta fitur dan kapabilitasnya yang dipergunakan oleh segenap manajemen dan karyawan perusahaan; dan

5. Karyawan baru yang masih belum begitu paham mengenai prosedur standar keamanan informasi di perusahaan.

Solusi Menghindari Resiko

Setelah mengetahui isu social engineering di atas, timbul pertanyaan mengenai bagaimana cara menghindarinya. Berdasarkan sejumlah pengalaman, berikut adalah hal-hal yang biasa disarankan kepada mereka yang merupakan pemangku kepentingan aset-aset informasi penting perusahaan, yaitu:

- Selalu hati-hati dan mawas diri dalam melakukan interaksi di dunia nyata maupun di dunia maya. Tidak ada salahnya perilaku "ekstra hati-hati" diterapkan di sini mengingat informasi merupakan aset sangat berharga yang dimiliki oleh organisasi atau perusahaan;

- Organisasi atau perusahaan mengeluarkan sebuah buku saku berisi panduan mengamankan informasi yang mudah dimengerti dan diterapkan oleh pegawainya, untuk mengurangi insiden-insiden yang tidak diinginkan;

- Belajar dari buku, seminar, televisi, internet, maupun pengalaman orang lain agar terhindar dari berbagai penipuan dengan menggunakan modus social engineering;

- Pelatihan dan sosialisasi dari perusahaan ke karyawan dan unit-unit terkait mengenai pentingnya mengelola keamanan informasi melalui berbagai cara dan kiat;

- Memasukkan unsur-unsur keamanan informasi dalam standar prosedur operasional sehari-hari – misalnya "clear table and monitor policy" - untuk memastikan semua pegawai melaksanakannya; dan lain sebagainya.

Selain usaha yang dilakukan individu tersebut, perusahaan atau organisasi yang bersangkutan perlu pula melakukan sejumlah usaha, seperti:

- Melakukan analisa kerawanan sistem keamanan informasi yang ada di perusahaannya (baca: *vulnerability analysis*);

- Mencoba melakukan uji coba ketangguhan keamanan dengan cara melakukan "penetration test";

- Mengembangkan kebijakan, peraturan, prosedur, proses, mekanisme, dan standar yang harus dipatuhi seluruh pemangku kepentingan dalam wilayah organisasi;

- Menjalin kerjasama dengan pihak ketiga seperti vendor, ahli keamanan informasi, institusi penanganan insiden, dan lain sebagainya untuk menyelenggarakan berbagai program dan aktivitas bersama yang mempromosikan kebiasaan perduli pada keamanan informasi;

- Membuat standar klasifikasi aset informasi berdasarkan tingkat kerahasiaan dan nilainya;

- Melakukan audit secara berkala dan berkesinambungan terhadap infrastruktur dan suprastruktur perusahaan dalam menjalankan keamanan inforamsi; dan lain sebagainya.