technocom3

by Solichul Huda

Submission date: 29-Aug-2017 10:04AM (UTC+0700)
Submission ID: 840781736
File name: JURNAL3.pdf (210.13K)
Word count: 3340
Character count: 22087

Pengamanan Sistem Komputer dari Model *Social Engineering* dengan mengaktifkan program *Security Awareness*

Solichul Huda

Abstrak : *Gangguan keamanan sistem komputer yang sulit diprediksi adalah Model "Social engineering". Social enginnering konsep utamanya menggolah kelemahan manusia untuk mengganggu keamanan sistem. Manusia dalam organisasi adalah karyawan, pengelola perusahaan, vendor, dan relasi. Mengaktifkan program Security awareness diduga dapat mencegah terjadinya "Social engineering. Attacker selalu berimprovisasi untuk menyusup mencari celah kelemahan manusia untuk menganggu keamanan sistem, dan aktifitas attacker tersebut diimbangi dengan mengaktifan program "Security awareness". Security awareness dapat berbentuk pelatihan, seminar, pengarahan maupun berupa software aplikasi yang dapat mencegah terjadinya social engineering.*

Kata Kunci : Social engineering, Security awareness, manusia, attacker,mencegah

PENDAHULUAN

Tiga tahun belakang ini peristiwa kejahatan keamanan komputer tidak hanya terjadi pada pengelola jaringan computer, akan tetapi para pengguna yang lain seperti pemakai jasa jaringan computer juga mulai menjadi target utama. Ada pemilik kartu ATM yang kehilangan uang tabungannya setelah melakukan transaksi di anjungan ATM. Seorang nasabah Bank dikuras saldo tabungannya karena melakukan laporan ke nomor aduan palsu yang tertulis di anjungan ATM.

Kasus-kasus tersebut terlihat menyolok pada tahun 2009. Hal ini berarti para *attacker (hacker/cracker*) sudah mulai berganti target operasi dari semula sistem administrator berganti target menjadi pengguna jasa jaringan komputer. Mereka mengetahui bahwa yang mempunyai kemampuan menjaga keamanan sistem komputer adalah sistem administrator, sedangkan pengguna tidak memiliki kemampuan tersebut.

Pada kasus-kasus terakhir masuk dalam kategori "*social engineering*", dimana attacker berusaha mencari kelemahan manusia dari segi psikologi. Untuk menghindarinya diduga dapat menggunakan pengaktifan security awareness. Secara teori dengan *security awareness*, gangguan *social engineering* dapat dihindari atau diminimalisasi.

Solichul Huda adalah Dosen Fakultas Ilmu Komputer UDINUS Semarang

PEMBAHASAN

Social engineering adalah metode mendapatkan informasi atau data rahasia/sensitif dengan cara menipu pemilik informasi / data tersebut. *Social engineering* umumnya dilakukan melalui telepon atau internet *Social engineering* merupakan salah satu metode yang digunakan oleh attacker untuk memperoleh informasi tentang targetnya, dengan cara meminta informasi itu langsung kepada korban atau pihak lain yang mempunyai informasi / data tersebut.

Social engineering mengkonsentrasikan diri pada rantai terlemah pada sistem jaringan komputer, yaitu manusia. Secara teknis, sistem komputer yang tidak dapat beroperasi tanpa melibatkan brainware (manusia). Dan karena sistem komputer terdiri dari komponen dan prosedur operasi yang standar, celah keamanan menjadi bersifat universal, tidak tergantung platform, sistem operasi, protokol, software maupun hardware. Dengan kata lain setiap sistem mempunyai kelemahan yang sama pada faktor manusia. Setiap pengguna sistem Komputer yang mempunyai akses kedalam sistem secara fisik menjadi sebuah ancaman, bahkan jika pengguna tersebut tidak termasuk dalam kebijakan kemanan yang telah disusun. Seperti metoda attacker yang lain, social engineering juga memerlukan persiapan, bahkan sebagian besar pekerjaan meliputi persiapan itu sendiri.

Faktor utama

Didalam pengamanan sistem selain ada prosedur, model-model pengamanan , masih terdapat faktor lain yang sangat penting, yaitu : manusia. Wm. Athur Conklin dalam bukunya "*principles of computer security*" mengatakan bahwa faktor manusia merupaka rantai paling lemah dalam sebuah sistem keamanan. Sebuah sistem keamanan yang baik, akan menjadi tidak berguna jika ditangani oleh administrator yang kurang kompeten. Selain itu, biasanya pada sebuah jaringan yang cukup kompleks terdapat banyak user yang kurang mengerti masalah keamanan atau tidak cukup peduli tentang hal itu. Sebagai sebuah contoh di sebuah perusahaan, seorang network admin sudah menerapkan kebijakan keamanan dengan baik, namun ada user yang mengabaikan masalah kemanan itu. Misalnya user tersebut menggunakan password yang mudah ditebak, lupa logout ketika pulang kerja, atau dengan mudahnya memberikan akses kepada rekan kerjanya yang lain atau bahkan kepada kliennya. Hal ini dapat menyebabkan seorang penyerang memanfaatkan celah tersebut dan mencuri atau merusak datadata penting perusahaan.

Atau pada kasus di atas, seorang penyerang bisa berpura-pura sebagai pihak yang berkepentingan dan meminta akses kepada salah satu user yang ceroboh tersebut. Tindakan ini digolongkan dalam *Social Engineering*.

Metode

Metode pertama adalah metode yang paling dasar dalam *social engineering*, yaitu, penyerang tinggal meminta apa yang diinginkannya: password, akses ke jaringan, peta jaringan, konfigurasi sistem, atau kunci ruangan. Memang cara ini paling sedikit berhasil, tapi bisa sangat membantu dalam menyelesaikan tugas penyerang.

Metode kedua adalah dengan menciptakan situasi palsu dimana seseorang menjadi bagian dari situasi tersebut. Penyerang bisa membuat alasan yang menyangkut kepentingan pihak lain atau bagian lain dari perusahaan itu,

misalnya. Ini memerlukan kerja lanjutan bagi attacker untuk mencari informasi lebih lanjut dan biasanya juga harus mengumpulkan informasi tambahan tentang 'target'. Ini juga berarti attacker tidak harus selalu berbohong untuk menciptakan situasi tesebut, kadangkala fakta-fakta lebih bisa diterima oleh target.

Teknik yang populer sekarang adalah melalui e-mail, dengan mengirim e-mail yang meminta target untuk membuka attachment yang tentunya bisa kita sisipi worm atau trojan horse untuk membuat backdoor di sistemnya.

Teknik-teknik tersebut biasanya melibatkan faktor personal dari target: kurangnya tanggung jawab, ingin dipuji dan kewajiban moral. Kadang target merasa bahwa dengan tindakan yang dilakukan akan menyebabkan sedikit atu tanpa efek buruk sama sekali. Atau target merasa bahwa dengan memenuhi keinginan penyerang-yang berpura-pura akan membuat dia dipuji atau mendapat kedudukan ynag lebih baik. Atau dia merasa bahwa dengan melakukan sesuatu akan membantu pihak lain dan itu memang sudah kewajibannya untuk membantu orang lain. Jadi *attacker* bisa fokuskan untuk membujuk target secara sukarela membantu *Attacker*, tidak dengan memaksanya. Selanjutnya *Attacker* bisa menuntun target melakukan apa yang dinginkan, target yakin bahwa dirinya yang memegang kontrol atas situasi tersebut. Target merasa bahwa dia membuat keputusan yang baik untuk membantu kita dan mengorbankan sedikit waktu dan tenaganya. Semakin sedikit konflik semakin baik.

Riset psikologi juga menunjukkan bahwa seorang akan lebih mudah memenuhi keinginan jika sebelumnya sudah pernah berurusan, sebelum permintaan inti cobalah untuk meminta target melakukan hal-hal kecil terlebih dahulu

Dalam beberapa kasus *social engineering*, seorang *attacker* didalam menganggu keamanan sistem menggunakan 2 metode :

1. Shoulder surfing : prosedur untuk menyerang posisi transaksi , mengamati user yang berhak, pada waktu memasukkan kode dengan benar
2. Piggybacking : mengintip siapa yang baru transaksi dengan kartu /PIN. Biasanya dilakukan dengan kamera tembunyi di dalam anjungan ATM

Selain kedua teknik tersebut ada juga teknik yang yang lain :

1. **Pretexting**, yaitu penggunaan skenario tertentu untuk membujuk korban melakukan tindakan tertentu atau memberikan informasi tertentu.
2. **Phising**, yaitu penggunaan e-mail sedemikian rupa sehingga bisa membujuk orang untuk melakukan sesuatu atau memberikan informasi tertentu.
3. **Trojan Horse/Gimmes**, yaitu memanfaatkan rasa ingin tahu seseorang dan memberikan malware untuk keperluan itu.
4. **Road Apple**, yaitu menggunakan media fisik yang bisa memancing rasa ingin tahu seseorang dan memberikan malware sebagai isinya

Pretexting

Pretexting adalah aksi yang menggunakan sebuah skenario untuk membuat target memberitahu informasi atau melakukan tindakan dan umumnya dilakukan melalui telephone. lebih tepat seperti pembohongan sederhana akan

tetapi melibatkan beberapa penelitian atau kumpulan informasi (seperti :tanggal lahir, transaksi terakhir) untuk mendeviasi otak target.
Tehnik ini biasa dipakai untuk mengorek informasi pelanggan, dan digunakan oleh oleh penyelidik pribadi untuk memperoleh catatan telepon, catatan penggunaan, catatan bank untuk kemudian digunakan untuk tingkat yang lebih besar dengan pembicaraan 2 mata bersama managet (perubahan account, mendapat informasi saldo, dll).

Phising

Phishing adalah teknik tipuan untuk mendapat informasi pribadi. umumnya, phiser mengirim email yang tampak seperti perusahaan mapan, bank, atau perusahaan kartu kredit dan meminta verivikasi dan peringatan jika langkah lankah tersebut tidak diikuti. biasanya surat ini memiliki sebuah link ke halaman situs web tipuan yang tampak seperti perusahaan situs asli, dengan logo perusahaan dan isinya. dan memiliki form yang menanyakan alamat rumah serta nomor pin atm.
Sebagai sebuah contoh pada tahun 2003 berkembang penipuan menggunakan metode ***phishing***_ dimana users menerima email seperti dari ebay dan mengatakan bahwa account users tersebut disuspend kecuali dia mengklik link yang tersedia dan mengupdate nomor CC yang sudah ada di ebay asli. karena membuat tampilan web yang relatif mirip agak mudah dengan menjiplak kode html. penipuan ini menipu orang-orang yang mengira dirinya betul-betul dihubungi oleh ebay dan mengira dirinya ada di situs ebay asli untuk mengupdate nomor CC nya dengan menyepam banyak orang, phiser akan memprosentasekan jumlah orang yang membaca email dengan cc-nya.

IVR/phone phishing

Tehnik ini menggunakan Interactive Voice Response (IVR) sistem yang menjiplak mesin penjawab bank atau institusi. korban dihubungi (biasanya lewat email phishing) untuk menelpon ke “bank” melalui nomor bebas pulsa dan memberikan informasi. sistem tersebut mereject login beberapa kali untuk memastikan korban memasukan pin secara berulang-ulang, biasanya mendapatkan beberapa pasword berbeda. sistem yang lebih canggih akan menyambungkannya pada penyerang yang menyamar sebagai costumer service untuk bertanya. beberapa orang bahkan sampai merekam perintarh umum (”tekan satu untuk merubah password, tekan dua untuk berbicara dengan costumer service”…) dan memainkannya secara berulang ulang, hingga membuat IVR seperti tanpa biaya sama sekali.

Trojan horse/gimmes

Gimmes mengambil keuntungan dari keingintahuan korban dengan mengirimkan malware. juga dikenal sebagai trojan horse, contoh simple dari gimmes adalah “email bervirus” yang memiliki attachment dan menjanjikan apa saja yang wah, dari *screen saver* seksi, antivirus *upgrade* atau bahkah gosip terkini. ketika korban tergoda dan membuka sisipannya yang merupakan tombol untuk mengaktifkannya. ketika korban cukup naif untuk mendownload tanpa berfikir, teknik ini cukup efektif dan contoh simple yang mendunia adalah virus i love you. umumnya sebuah program yang memberi akses dengan bersembunyi didalam software lain (spyware) atau

berpura-pura menjadi sesuatu (copian gratis dari software terbaru). prilakunya seperti legenda terkenal kuda troya (trojan horse) yang berisi penyerang didalamnya.

Road apple

Road Apple adalah variasi lain dari Trojan Horse yang menggunakan media fisik dan membuat rasa ingin tahu yang sangat besar. nama ini diambil dari euphemisme untuk kata pupuk kuda. dalam serangan road apple, penyerang meninggalkan malware dalam sebuah disket, cd atau flashdisk di lokasi yang sangat mungkin ditemukan. (kamar mandi, lift, jalanan, dan tempat parkir) dengan memberikan label yang sangat membangkitkan rasa ingin tahu, dan setelah itu tinggal menunggu. sebagai contoh, penyerang menciptakan sebuah cd dengan logo perusahaan, dan memberikan label "gaji pegawai eksekutif tahun 2008" didepannya. kemudian penyerang meninggalkan cd itu di lantai sebuah lift atau di lobby perusahaan target. salah satu pegawai sangat mungkin menemukannya dan kemudian membukanya untuk memuaskan rasa ingin tahunya. seorang pegawai yang baik tentu mengembalikannya ke perusahaan. dalam kasus ini memasukan cd untuk melihat isinya secara otomatis menginstal malware ke dalam komputer, yang memberikan penyerang akses ke dalam komputer korban, atau bahkan ke dalam jaringan perusahaan. kecuali kontrol lain memblok infeksi tersebut, PC dengan sistem autorun akan menjadi sasaran empuk ketika sebuah cd dimasukan.

Quid pro quo

Sesuatu untuk sesuatu attacker menelpon nomor secara acak mengaku dari sebuah perusahaan yang menelpon untuk masalah teknis. ketika mereka mendapatkan korban dengan masalah yang serius, mereka akan menelpon kembali dan penyerang akan "menolong" memecahkan masalahnya dengan memerintahkan korban mengetikan kode perintah yang dapet memberikan akses atau mengaktifkan malware.

Beberapa tipe lain

Sewaktu Attacker memiliki skill untuk cracking, beberapa orang masih tetap menggunakan *social engineering* yang notabene mengacaukan keputusan dan memanipulasi orang, eksploitasi kelemahan seseorang untuk mendapatkan keuntungan. bentuk *social engineering* terkini termasuk mengintip dan mengambil id dari orang terkenal yang memiliki email yahoo. gmail, hotmail. Alasan attacker beragam. beberapa diantaranya : a. Phising nomor kartu kredit dan pasword. b hacking email pribadi, data pembicaraan dan memanipulasi menggunakan teknik edit yang sederhana kemudian menggunakannya untuk memeras uang dan menciptakan ketidakpercayaan diantara individu. c menghack website sebuah organisasi dan menghancurkan reputasi mereka. e. menciptakan ketidakharmonisan dalam lingkungan sosial.

Security Awareness

Security awareness adalah ilmu pengetahuan dan perilaku anggota organisasi/perusahaan dalam kesadaran dalam memproteksi pisik data dan informasi yang merupakan aset organisasi. Tujuan akhir *Security Awareness* adalah

membawa karyawan, relasi, vendor, manajer untuk memahami perlunya mereka menjaga sistem komputer yang dimiliki. Sehingga mereka akan menjaga penuh aset perusahaan baik informasi, pisik sistem computer maupun user atau manusia yang terlibat dalam sistem computer tersebut.

Fokus dari *security awareness* menanamkan sikap atau kesadaran perlunya keamanan sistem komputer secara mendalam sehingga menjadi budaya, kebiasaan mereka dalam perusahaan. Kebijakan perusahaan menjadi sesuatu yang terpenting dalam keberhasilan dalam pencegahan dan penanganan *social engineering* dengan teknik *security awareness*.

Teknik pengaktifan program ini dengan cara mengadakan trining/pelatihan secara periodik atau disesuaikan dengan waktu munculnya jenis gangguan baru.

Secara psikologis, semua orang mesti menginginkan sesuatu yang praktis, efesien, dan mudah. Kenyamanan menjadi ukuran dalam setiap melakukan suatu pekerjaan. Attacker mengetahui dengan persis kebiasaan manusia ini. Mereka dengan segala teknik dan strategi untuk melakukan sesuatu yang dapat menguntungkan dia. Kenyamanan berbanding terbalik dengan keamanan. Sesuatu yang pemakaiannya sangat nyaman, biasanya keamanannya terabaikan, begitu juga keamanan yang ketat membuat kenyamanan menjadi berkurang.

Security awareness harus mempertimbangkan keamanan secara proporsional, ketat atau longgarnya pengamanan sistem komputer tergantung dari nilai dari data/informasi dan volume penyerangan yang pernah muncul.

Tingkat keberhasilan *security awareness* tergantung kepada 2 hal :

1. Lingkungan organisasi/perusahaan
2. Level-level pengamanan yang ajarkan.

Lingkungan organisasi

Mungkin ini akan terasa membatasi kebebasan. Mungkin akan banyak yang merasa tidak puas.Untuk itu policy harus melalui proses pemikiran yang matang dalam pembuatannya dan proses sosialisasi yang baik saat akan dijalankan. Juga jangan lupa adanya program-program *Security awareness* yang rutin diadakan agar semua mengerti mengapa policy itu dibuat dan apa yang ingin dicapai dari pelaksanaan policy itu.

Organisasi memikirkan adanya sebuah kebijakan yang mempunyai aturan yang ketat didalam menghindari *social engineering*. Kebijakan ini akan mengatur kapan seseorang atau sebuah devisi boleh mengakses internet. Bagaimana membat password, bagaimana supaya komputer tetap aman sewaktu komputer tertinggal di kamar mandi. diatur semuanya

Level-level pengamanan

Level pengamanan yang diterap di masing-masing perusahaan berbeda. Penetapan level pengamanan sistem computer di perusahaan tergantung dari besar kecilnya perusahaan dan besar kecilnya nilai data/informasi yang perlu dilindungi. Perusahaan yang besar dengan banyak divisi biasanya memakai level keamanan lebih dari 3 level. Hal ini bertujuan supaya data/informasi terjamin keamanannya.

Masalah yang biasanya muncul adalah

- Banyak user yang kurang mengerti masalah keamanan atau tidak cukup peduli dengan hal itu.
- Administrator kurang kompeten
- Sifat manusia :
    1. Kurang bertanggung jawab
    2. Ingin dipuji
    3. Suka menolong / Kewajiban moral

Dari riset psikologi yang pernah dilakukan menghasilkan sebuah kesimpulan bahwa seseorang akan lebih memenuhi keianginan jika sebelumnya pernah berusuran dengan seseorang

Target utama dari program *security awareness* ini adalah

1. Keamanan perusahaan
2. Sumberdaya manusia
3. Teknologi Informasi (keamanan dan operasional)
4. Top Manajemen
5. Penanggung jawab *security awareness*

Tujuan pengaktifan *security awareness* adalah :

1. Menentukan praktek terbaik program *security awareness*
2. Sharing pengalaman dalam menangani *security awareness*
3. Pengembangan *security awareness* untuk semua bisnis dan membantu semua fungsi dalam perusahaan
4. *Security awareness* berada didalam control manajemen

IMPLEMENTASI

Awareness sendiri bertujuan mengarahkan individu untuk konsentrasi pada pengenalan keamanan dan meresponnya sewaktu gangguan keamanan terjadi. Dan target *security awareness* adalah karyawan, vendor dan partner.

Implementasi *security awareness* dilakukan dengan tahap-tahap sebagai berikut :

1. Identifikasi kebutuhan :

Visi perusahaan

Pelaksanaan pengamanan sebaiknya disesuaikan dengan visi perusahaan. Hal ini sangat perlu untuk menjaga efesiensi dalam menjaga keamanan sistem komputer

Misi perusahaan

Dari misi yang dimiliki oleh perusahaan pengamanan dapat disesuaikan dengan kebutuhan pengamanan. Keamanan berbanding terbail dengan kenyamanan. Supaya proporsional, penyusunan pengamanan disesuaikan dengan misi perusahaan

Strategi :

Dianalisis secara teliti strategi semua bagian dan semua jenis bisnis yang dimiliki perusahaan, sehingga ada kesesuaian atau keseimbangan antara keamanan sistem yang dibentuk dengan strategi perusahaan

Insiden

Untuk memperoleh hasil yang maksimal, materi *security awareness* harus up to date. Insiden-insiden gangguan keamanan sistem computer model baru harus dikaji penyebabnya, kerugian dan cara penyelesaiannya. Keberhasilan peserta *security awareness* dalam mengamankan sistem computer tergantung dari kebaruan materi *security awareness*. Pengetahuan yang diperolah up to date, user, operator, vendor relasi akan mampu mencegah atau menyelesaikan kasus *social engineering* yang terjadi.

Hukum

Dengan berlakunya Undang-undang ITE, pengetahuan mengenahi hokum ketika memakai jasa elektronik harus berhati-hati. Dalam *security awareness* harus melihat titik kelemahan yang bisa dilakukan oleh attacker tanpa terkena sanksi hukum. Penerapan hokum ITE di Indonesia sudah diberlakukan, sehingga pemahaman titik lemah yang akan dilakukan oleh attacker harus diperhatikan dan apa yang dilakukan sewaktu terjadi penyerangan juga jangan sampai melanggar hukum.

Diskusi dengan para eksekutuf, tenaga teknis pengamanan sistem komputer, tenaga teknologi informasi dan personalia

Penetapan prioritas

Dibuat prioritas program sehingga program berjalan efektif

Pengaturan target

Pengaturan target ini untuk disesuaikan antara ketersediaan perangkat lunak dan perangkat keras teknologi informasi yang dimiliki, sumberdaya manusia dengan target yang dbuat

2. Pengembangan
    1. Memilih topic awareness
    2. Menemukan hasil penyelesaian masalah, misalnya menghindari, menyelesaikan dan lain-lain
    3. Gunakan contoh kejadian yang masih riil baik di internal dan ekternal perusahaan
    4. Pemberian materi ke peserta dengan media yang tepat
3. Implementasi

    Didalam implementasinya kegiatan diatur sebagaia berikut :
    1. Buat pelatihan 1 minggu
    2. Kelas dibuat pagi dan sore
    3. Penjaminan pembagian kapasitas kelas tepat maksimal 20 orang
    4. Atur break 45 / 15 menit sekali

4. Pemeliharaan
    1. Update materi pelatihan /seminar setiap kali mulai training/seminar baru
    2. Lihat topic dan isu-isu baru gangguan model *social engineering*

Harus diakui bahwa tidak semua pemakai sistem komputer mempunyai kemampuan untuk menjaga data dan informasi yang ada didalamnya. Para karyawan, vendor, maupun relasi bisnis harus mempunyai kemampuan untuk gangguan *social engineering*. Teknik yang dipakai dalam menyusup, menyerang selalu berubah-ubah yang cenderung berimprovisasi , harus dengan kemampuan lebih jika ingin menangkal kejahatan model ini.

Karyawan, vendor, relasi, manajer selalu menjadi target utama dari attacker sewaktu akan membobol sistem. Manusia menjadi target utama karena secara psikologi banyak factor yang membuat manusia mudah terpengaruh oleh orang lain. Dalam kondisi normal hanya sedikit pemakai sistem komputer yang dapat menjaga keamanan sistem komputer apalagi jika attacker memakai metode tertentu tambah lepas pengamanan sistemnya.

Secara umum para attacker dalam melakukan aksi kejahatannya tidak menggunakan metode yang memerlukan keilmuan yang kuat, sehingga untuk menanggulanginya juga hanya perlu sedikit pengetahuan tentang komputer. Dan yang sangat penting diketahui oleh pemakaian sistem komputer adalah kerusakan atau kerugian yang ditimbulkan akibat olah para attacker.

Kesadaran akan bahaya dari kerusakan dan kerugian yang dialami pengguna komputer ini diharapkan akan menimbulkan kesiapan sikap dan selalu waspada akan kemungkinan pencurian maupun perusakan data. Penyadaran akan bahaya dan ketrampilan untuk mencegah dan menindak dapat diperoleh dengan pengaktifan program *security awareness*.

Hasil dari pelatihan program *Security awareness* ini adalah pemakai sistem komputer akan memperoleh ilmu pengetahuan tentang keamanan sistem komputer, kemungkinan gangguan – gangguan yang muncul pada sistem komputer dan tindakan mencegah dan menyelesaikan sewaktu gangguan terjadi.

Bentuk *security awareness* dapat berupa pelatihan dapat juga berupa seminar, diskusi kelompok dan lain-lain

Program *security awareness* akan dilakukan secara periodik sesuai dengan perkembangan dari jenis gangguan yang muncul dengan harapan setiap *social engineering* model baru muncul, karyawan sudah mengantisipasi untuk mengamankan aset-aset perusahaan secara maksimal.

Kasus-kasus *social engineering* terbaru dan hasil program *security awareness* :

1. Mengambil kertas hasil transaksi pembayaran di supermarket memakai kartu kredit. Seorang pengguna sistem komputer setelah mengikuti *security awareness* akan langsung merusak / menghancurkan kertas hasil transaksi setelah dicek kebenarannya. Kertas itu biasanya dipakai oleh attacker untuk transaksi di internet dengan menggunakan kartu kredit orang lain
2. Mencuri uang di anjungan ATM dengan modus kartu ATM tertelan. Seorang pengguna sistem komputer setelah mengikuti *security awareness* akan melakukan transaksi ATM di anjungan ATM yang terdapat di dekat kantor Bank atau di dekat keramaian, setelah mencoba tombol esc dan enter terlebih dahulu.
3. Mencari informasi dengan menggunakan nomor aduan palsu. Pengguna ATM akan selalu melakukan update data hanya di kantor Bank.

4. Pencurian password computer. Pengguna computer akan mengetahui dengan persis bagaimana memilih password, menyembuyikan password dan kapan menganti password.

Security awareness akan menghasilkan pengetahuan baru tentang keamanan sistem komputer dan munculnya sikap kehati-hatian untuk mengamankan data dan informasi yang dimiliki oleh perusahaan.

KESIMPULAN

Dari uraian di atas dapat disimpulkan sebagai berikut :

1. Gangguan keamanan sistem computer model *social engineering* akan muncul secara terus menerus dengan teknik yang berbeda-beda
2. Social engineering menggunakan factor psikologi untuk mengganggu keamanan sistem komputer
3. *Security awareness* akan memberikan pengetahuan tentang keamanan sistem komputer dan gangguan-gangguan yang muncul terutama yang menyerang dari factor psikologi manusia
4. *Security awareness* akan menumbuhkan sikap kesadaran akan keamanan data dan informasi pada penggunana sistem komputer dan selalu siaga terhadap gangguan yang muncul setiap saat .
5. Supaya efektif *security awareness* akan dilakukan secara periodik untuk mengantisipasi modus-modus baru gangguan sistem komputer.

DAFTAR PUSTAKA

1. Wm. Arthur Conklin, 2005, " Principles of computer security", Mc graw Hill, Singapure
2. Christopher Albert, 2003, "Managing Information Security Risk", Addison Wesley, Boston
3. Janner Simarta, 2006, "Pengamanan Sistem Komputer",Andi offset, Yogyakarta
4. Budi Raharjo, 2004, "Keamanan Sistem Informasi Berbasis Internet", PT. Insan Indonesia & PT. Indocisc
5. www.securityawareness.com

technocom3

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10