ANALISIS PENYERANGAN *SOCIAL ENGINEERING*

Onny Rafizan
Peneliti Bidang Teknologi Informatika di Puslitbang Aptika & IKP
Balitbang SDM Kominfo

ABSTRACT

In the era of Information where the Information itself has became one of valuable asset for an organization so, an organization will tried to protect the information that they have. But, even the thickest wall of security can fall if the people inside the security wall make mistake that leads to security hole. This kind of mistake usually can be exploit by hacker using Social Engineering. This research is trying to explore this type of attack by analyzing, gathering literature, and finding similar incident that already happen before, to give other people information about Social Engineering and the threat that this type of attack can pose. The result of this research will be recommendation that can be used to protect the company's information from the threat that comes from Social Engineering.

Keywords: *Social Engineering, Hacker, Threat, User, Information Security*

ABSTRAK

Di era Informasi ini, informasi sendiri sudah menjadi salah satu aset yang berharga bagi sebuah organisasi, karenanya sebuah perusahaan akan berusaha untuk melindungi informasi yang mereka milliki. Namun, dinding keamanan terkuat sekalipun dapat runtuh jika orang di dalamnya membuat kesalahan yang mengakibatkan adanya lubang di dinding keamanan tersebut. Kesalahan seperti ini biasanya di eksploitasi oleh hacker dengan menggunakan Social Engineering. Karena itulah penelitian ini berusaha untuk mengeksploarasi tentang tipe penyerangan ini dengan cara menganalisa, mengumpulkan literatur, dan mencari permasalahan yang pernah terjadi, agar dapat memberi informasi kepada orang lain tentang Social Engineering dan ancaman yang dapat disebabkan oleh tipe penyerangan seperti ini. Hasil akhir dari penelitian ini akan berupa rekomendasi yang dapat digunakan untuk melindungi informasi yang dimiliki perusahaan dari ancaman Social Engineering.

Kata-kata kunci: Social Engineering, Hacker, Ancaman, Pengguna, Keamanan Informasi

PENDAHULUAN

Latar Belakang

Menurut Malcolm Allen dalam tulisannya di *SANS InfoSec Reading Room, Social Engineering* merupakan ancaman yang sering diabaikan namun dapat dieksploitasi setiap saat, untuk mengambil kesempatan dari adanya kelemahan di dalam sebuah jaringan keamanan, yaitu manusia atau pengguna dari sistem itu sendiri.[1] Dimana dari dulu manusia atau pengguna dianggap sebagai bagian terlemah dalam sebuah keamanan jaringan. Seperti yang juga dikemukakan oleh Prof. Richardus Eko Indrajit, Kepala ID-SIRTII, bahwa dalam dunia keamanan jaringan ada prinsip 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"*.[2] Dimana dalam berbagai buku keamanan jaringan juga selalu mengemukakan *"People is the weakest link"* atau "manusia adalah komponen yang terlemah"

Hacker sekarang ini tidak hanya beroperasi di balik computer untuk menyerang targetnya, mereka juga menghampiri targetnya secara langsung dan berusaha memenangkan kepercayaan mereka untuk mendapatkan informasi berharga yang mereka butuhkan untuk dapat mengakses system yang terlindungi oleh dinding keamanan dan membuat penanganan keamanan apapun menjadi tidak berguna, cara seperti inilah yang biasa disebut sebagai *Social Engineering* dan *hacker* yang menggunakan cara seperti ini biasa disebut sebagai *Social Engineering Hacker.* Menurut acuan keamanan jaringan yang dikeluarkan oleh *Microsoft,* perusahaan pembuat *Operating System Windows*, *Social Engineering Hacker* dapat menjadikan kecerobohan, kemalasan, kesopanan, bahkan antusiasme dari seorang staff di sebuah organisasi sebagai targetnya.[3] Karena, mungkin korban itu sendiri tidak menyadari kalau mereka telah ditipu atau bahkan mereka kadang tidak mau mengakui hal tersebut kepada orang lain. Tujuan dari *Social Engineering Hacker* sama seperti hacker yang lainnya, yaitu untuk mendapatkan akses ke dalam sebuah sistem, dimana mereka bisa mengincar uang, informasi, atau asset IT yang ada. Berdasarkan tulisan yang dikeluarkan oleh *Cisco,* salah satu perusahaan penjual perangkat jaringan, *Social Engineering* sendiri sudah berevolusi dengan sangat cepat sehingga membuat solusi dari teknologi, kebijakan keamanan, dan standar operasi saja tidak dapat melindungi asset berharga yang dimiliki perusahaan.[4] Dimana sekali lagi hal ini disebabkan karena *Social Engineering Hacker* menjadikan staff/pengguna sebagai targetnya, untuk mendapatkan akses ke dalam sistem. Tujuan dari dibuatnya tulisan ini adalah untuk memberikan pemahaman yang jelas kepada masyarakat mengenai *Social Engineering*, dengan didasarkan atas tiga hal:

(1). Pemahaman sebagian masyarakat Indonesia masih mengenal *hacker* dengan cara operasinya yang lama. Dimana jika dulu *hacker* berusaha menyerang

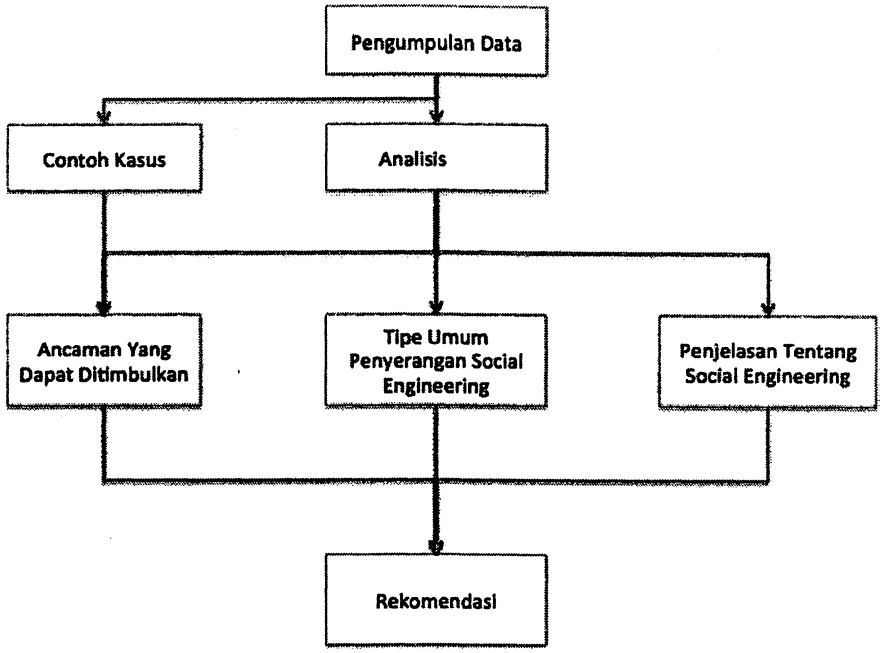
targetnya hanya dibalik komputer melalui jaringan internet, sekarang ini mereka memiliki cara lain yang memungkinkan bagi mereka untuk dapat mengakses sistem yang menjadi sasaran mereka tanpa mengandalkan seluruh kemampuan *technical* yang dimiliki.

(2). Sebagian besar masyarakat Indonesia belum mengenal tentang *Social Engineering*, bahkan beranggapan bahwa ini adalah kasus yang baru. Jika kita melihat sebelum tahun 2000 sudah ada cukup banyak kasus *Social Engineering*, hanya saja jarang tercatat karena faktor sulitnya untuk mengidentifikasi sebuah insiden yang terjadi dalam keamanan jaringan sebagai akibat dari *Social Engineering*. Kesulitan untuk mengidentifikasi insiden yang disebabkan oleh *Social Engineering* juga sering diakibatkan karena user yang menjadi korban jarang yang mau melaporkan insiden tersebut, karena sebab utama dari terjadinya insiden tersebut dikarenakan karena kesalahan user itu sendiri.

(3). Meningkatkan kewaspadaan masyarakat dengan memberi pemahaman yang jelas mengenai *Social Engineering* dan ancaman yang dapat ditimbulkannya. Dengan adanya pemahaman mengenai *Social Engineering* diharapkan masyarakat dapat lebih waspada akan adanya ancaman yang nyata ini.

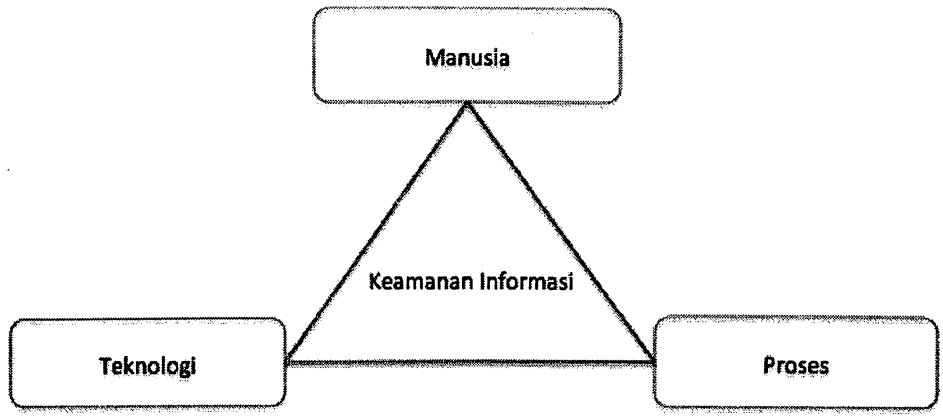
Metode Penelitian

Metodologi yang digunakan dalam penelitian ini adalah analisis kualitatif. Pertama-tama mencari data-data pendukung seperti sumber literatur dan contoh kasus yang pernah terjadi. Dari data tersebut kemudian akan di analisa sehingga akan didapat pemaparan mengenai teknik penyerangan *Social Engineering*, cara-cara yang umumnya dilakukan, serta ancaman-ancaman yang dapat ditimbulkan. Ancaman-ancaman yang dapat ditimbulkan juga akan diperkuat dengan data-data berupa contoh kasus yang pernah terjadi sebelumnya, dimana contoh kasus ini dapat dijadikan sebagai ukuran akan ancaman yang dapat ditimbulkan oleh *Social Engineering* ini. Hasil akhir dari penelitian ini selain dapat memaparkan tentang *Social Engineering* juga akan memberikan beberapa rekomendasi yang dapat digunakan untuk menghadapi tipe penyerangan seperti ini. (Gambar 1)



Gambar 1. Metodologi Analisis *Social Engineering*

Salah satu pemikiran yang salah, terutama masih dimiliki oleh sebagian besar dari masyarakat Infonesia adalah dengan beranggapan bahwa *hacker* adalah seseorang yang menggunakan komputer untuk menjebol suatu sistem keamanan dengan tujuan mencuri, mengubah, atau merusak sistem tersebut. Secara umum untuk dapat melewati suatu sistem keamanan seorang *hacker* biasanya akan mengeksploitasi kelemahan-kelemahan dari suatu sistem keamanan, karenanya akan sangat penting bagi seorang yang mengurus keamanan jaringan di suatu perusahaan untuk selalu menutup kelemahan-kelemahan yang ada di sistem mereka, cara seperti ini adalah salah satu contoh yang dilakukan untuk menjaga keamanan informasi dari segi teknologi. Namun, suatu sistem keamanan tidak hanya terdiri dari teknologi saja. Seperti yang digambarkan pada gambar 2, manusia merupakan bagian dalam sebuah kemanan informasi.



Gambar 2. Komponen utama Keamanan Informasi

Menurut Amanda Andress, ada tiga hal yang menjadi komponen utama dari keamanan informasi, yaitu manusia, proses, dan teknologi.[5]

Proses:

Suatu sistem keamanan dibangun dengan menggunakan dokumen resmi perusahaan yang berupa standar, prosedur, maupun kebijakan. Kebijakan yang dimiliki oleh perusahaan inilah yang akan menjadi landasan utama dalam keamanan informasi, dimana kebijakan tentang keamanan informasi sebaiknya harus ditandatangani oleh pimpinan puncak dari suatu perusahaan. Dengan adanya penandatanganan dari pimpinan puncak akan menandakan bahwa pimpinan sudah menyetujui adanya kebijakan tersebut dan menjadikannya sebagai prioritas utama dari perusahaan yang harus diikuti oleh semua karyawan perusahaan tersebut. Karena itulah dalam keamanan informasi, suatu kebijakan menjadi urutan pertama yang harus diprioritaskan.

Manusia:

Sebuah sistem dijalankan oleh manusia sebagai penggunanya. Akan tetapi seperti yang dikemukakan oleh Prof. Richardus Eko Indrajit, dalam sebuah jaringan keamanan manusia menjadi bagian terlemah dalam sistem tersebut. Oleh karena itulah dalam keamanan informasi, manusia menjadi prioritas kedua yang harus diperhatikan. Ditambah lagi dalam aspek inilah yang akan menjadi sasaran utama dari *Social Engineer Hacker.*

Teknologi:

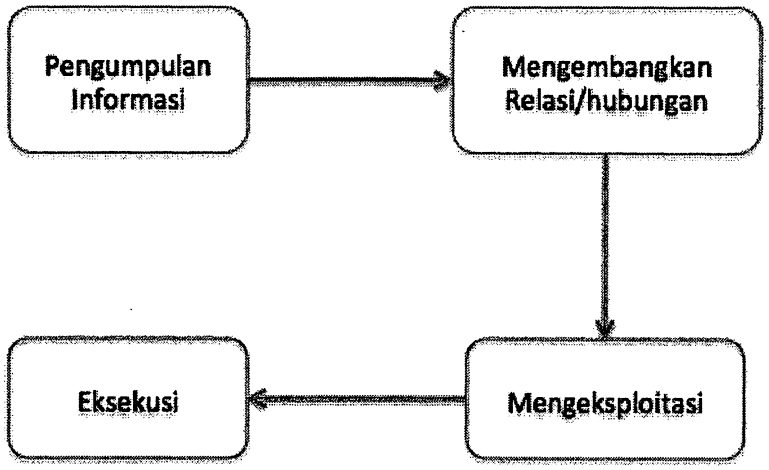
Meskipun saat berbicara mengenai sebuah keamanan jaringan selalu menyinggung tentang teknologi, akan tetapi aspek ini menjadi urutan ke tiga yang harus diprioritaskan. Aspek teknologi yang dapat digunakan

untuk keamanan jaringan dapat berupa pemasangan/penyettingan *firewall* untuk mengatur keluar masuknya transmisi di dalam jaringan, *anti-virus, anti-spam, Intrusion Detection System* untuk mendeteksi keanehan di dalam jaringan, maupun *Intrusion Prevention System* sebagai pencegahan jika ada terjadi penyerangan.

Ketiga aspek tersebut menjadi sebuah kesatuan yang sangat penting dalam membangun keamanan informasi di dalam sebuah jaringan yang dimiliki oleh persuhaan, dimana aspek satu dengan yang lainnya saling mendukung. Jika melihat tiga komponen utama tersebut, teknologi menjadi prioritas ketiga. Masalah dalam bidang keamanan informasi akan terus muncul dan akan sangat sulit jika kita hanya mengandalkan dari aspek teknologi semata untuk menutup masalah yang muncul tersebut. Karena itu peran dari manusia sebagai pengguna sangat dibutuhkan untuk memperkuat sebuah sistim keamanan, dimana semua tindakan yang dilakukan manusia sebagai pengguna di dalam sebuah perusahaan haruslah diatur dalam sebuah dokumen resmi perusahaan yang jelas, yaitu dapat berupa perangkat peraturan, prosedur ataupun kebijakan perusahaan. Seperti yang dikemukakan oleh Prof. Richardus Eko Indrajit, dalam ketiga aspek tersebut manusia menjadi bagian yang terlemah dalam sebuah jaringan keamanan.[2] Manusia sebagai pengguna juga menjadi target utama bagi *Social Engineering Hacker,* yaitu *hacker* yang menggunakan teknik *social engineering* untuk menembus suatu sistem keamanan.

Social Engineer adalah *hacker* yang menggunakan otaknya daripada otot komputernya. *Hackers* menelpon pusat data dan berpura-pura menjadi pelanggan yang kehilangan user dan passwordnya. Bentuk lain dari *Social Engineering* tidak begitu mudah dikenali. *Hackers* selalu dikenal untuk membuat website palsu yang menanyakan kata sandi yang dimiliki si pengguna, dikutip dari Karren J Bannen.[6] Begitu juga yang dikemukakan oleh Harl, *"Social Engineering is the art and science of getting people to comply with your wishes"*,[7] atau dalam bahasa Indonesianya, *Social Engineering* adalah seni dan sains dalam menjadikan orang untuk mematuhi keinginanmu. *Social Engineering* menjadikan staff/manusia sebagai targetnya.

Mereka mendatangi staff tersebut untuk mendapatkan informasi yang mereka butuhkan. Biasanya *Social Engineering Hacker* seperti yang dikemukakan sebelumnya dari Karren J Banne, akan berpura-pura menjadi pelanggan untuk mendapatkan informasi yang mereka inginkan seperti password yang dimiliki pelanggan sebenarnya. Mereka juga dapat berpura-pura sebagai orang dalam organisasi tersebut, hal ini bisa diperburuk dengan tidak adanya control yang jelas akan staff yang keluar dan masuk. Dalam penyerangan *Social Engineering* terdapat pola umum yang biasa mereka gunakan. Menurut Gartner (Gambar 3), ada 4 tahap yang menjadi pola umum yang biasa dilakukan oleh *Social Engineering Hacker.*[8]



Gambar 3. Pola Umum Penyerangan *Social Engineering* [8]

Pengumpulan Informasi:
Banyak tehnik yang bisa digunakan oleh penyerang untuk mendapatkan informasi mengenai sasarannya. Bisa berupa struktur organisasi, list nama orang dalam, tanggal ulang tahun, dan cara lainnya yang dapat digunakan nantinya untuk mengembangkan relasi/hubungan dengan targetnya.

Mengembangkan Relasi/hubungan:

Setelah mendapatkan informasi yang cukup maka selanjutnya adalah berusaha mendekati salah seorang staff yang telah menjadi sasaran. Pada tahap ini semua informasi yang telah diperoleh di awal akan digunakan untuk mendapatkan kepercayaan sasaran tersebut. Misalnya saat bertemu dengan orang yang menjadi sasaran, si *hacker* tersebut mengaku sebagai saudara dari atasan orang yang menjadi sasaran tersebut dengan menyebutkan nama panggilan dan alamat atasan tersebut. Karena merasa informasi yang disebutkan oleh *hacker* tersebut benar, orang yang menjadi sasaran tersebut mulai mempercayai *hacker* tersebut.

Mengeksploitasi:
Setelah mendapatkan kepercayaan dari orang yang dijadikan sebagai sasarannya, langkah selanjutnya yang akan dilakukan oleh *hacker* tersebut adalah berusaha mengeksploitasi informasi-informasi penting yang dapat digunakan oleh *hacker* tersebut untuk masuk ke dalam system perusahaan. Informasi-informasi yang biasa digali oleh *hacker* bisa berupa *username, password*, arsitektur jaringan perusahaan, dan sebagainya.

Eksekusi:
Setelah berhasil mendapatkan informasi-informasi yang diinginkan pada saat inilah tahapan dari pola penyerangan *Social Engineering* berakhir dan dilanjutkan dengan mengakses sistem yang menjadi sasaran awal dari *hacker* dengan menggunakan informasi-informasi yang dia miliki. Setelah berhasil masuk ke dalam sistem *hacker* tersebut dapat dengan mudah mencuri, merubah, bahkan merusak sistem dan data di dalamnya tanpa terhalangi oleh sistem keamanan.

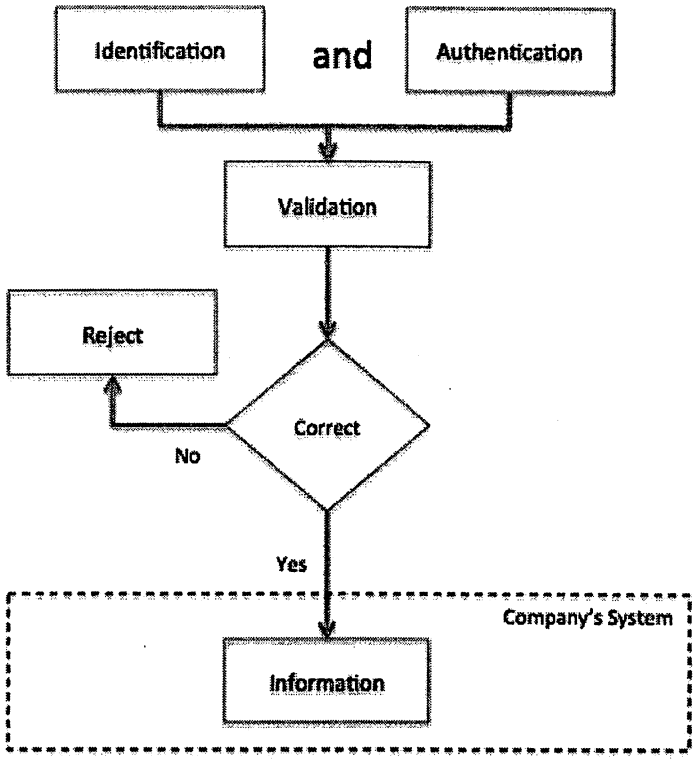
Contoh Kasus

Sebagai contoh kasus yang pernah terjadi di Indonesia, yaitu kasus pencurian data milik pejabat XL yang dilakukan oleh karyawan Huawei pada tanggal 13 Maret 2009.[9] Pada saat itu perusahaan telekomunikasi, XL sedang mengadakan rapat dengan pihak perusahaan Huawei, perusahaan perangkat jaringan milik China. Kemudian, salah satu karyawan Huawei tersebut menyelinap keluar ruangan rapat lalu menyusup ke ruang *General Manager Network Planning XL* Opbet Suwadji yang terletak di lantai 15. Oknum tersebut sempat mengkopi file-file di folder *My Document* computer milik Opbet, ke dalam *Flash Disk* miliknya, namun sempat terpergok oleh seorang karyawan XL. Jika pada saat itu pelaku berhasil membawa kabur data-data yang berhasil dia kopi dan dimana diantara data-data tersebut tersebut terdapat informasi yang sensitif bagi perusahaan, maka perusahaan XL akan mengalami kerugian yang sangat besar karena informasi sensitif perusahaan telah bocor keluar. Satu kasus lagi yang sangat dikenal di dunia ialah kasus "Kevin Mitnick", seorang pria asal Amerika Serikat yang ditahan pada tahun 1995.[10] Kevin Mitnick adalah orang yang tercatat sebagai salah seorang *hacker* yang dalam mendapatkan sasaran-sasarannya hampir dengan tanpa menggunakan komputer untuk mengeksploitasi kelemahan sasarannya, dimana sebagian besar dilakukannya dengan menggunakan teknik *social engineering.*

Ia terbukti telah masuk ke beberapa sistem komputer perusahaan dan mencuri *software-software* milik Motorola, Novell, Fujitsu, Sun Microsystems, dan perusahaan lainnya. Sebagai salah satu tindakan kriminalnya, Kevin Mitnick juga mengaku bahwa ia telah mencuri E-mail dan berpura-pura menjadi salah seorang karyawan perusahaan korbannya, seperti Nokia dimana ia telah mengambil *software* yang sedang dikembangkan oleh perusahaan tersebut.

Ancaman yang dapat ditimbulkan

Dari dua contoh kasus tersebut bisa dilihat bahwa *Social Engineering* menjadi sebuah ancaman yang sangat nyata bagi perusahaan maupun organisasi manapun. Letak ancaman dari *Social Engineering* dapat dilihat pada Gambar 4.sebagai berikut.



Gambar 4. Gambaran sederhana sebuah sistem keamanan

Dari Gambar 4 sederhana dapat dilihat bahwa sebuah sistem keamanan yang memiliki fungsi untuk melindungi informasi yang ada di dalam sebuah sistem perusahaan. Untuk dapat mengakses informasi yang dilindungi ini, terlebih dahulu harus melewati tahap validasi. Pada tahap validasi dibutuhkan sebuah identifikasi yang (biasanya berupa *username*) yang menunjukkan identitas dari orang yang akan mengakses informasi tersebut dan otentikasi (biasanya berupa *password*) yang menjadi alat bukti bahwa memang orang itulah yang memiliki hak untuk mengakses informasi tersebut. Dalam teknik *social engineering* seorang *hacker* akan berusaha untuk membuat agar staff/orang yang memiliki hak akses akan informasi tersebut untuk memberikan *username* dan *password* mereka, dimana seringkali mereka tidak menyadari kalau mereka telah menjadi korban. Saat *hacker* telah mendapatkan *username* dan *password* maka ia dapat dengan mudah untuk masuk ke dalam sistem perusahaan, karena sistem keamanan perusahaan mengenal *hacker* tersebut sebagai seorang pengguna yang memiliki hak akses resmi. Jika hal seperti ini terjadi maka semua sistem keamanan yang telah dipasang di perusahaan tersebut menjadi tidak berguna, karena prinsip dasar dari sebuah sistem keamanan adalah untuk menjaga agar orang yang tidak mempunyai hak tidak dapat masuk, sedangkan setelah *hacker* tersebut memiliki *username* dan

password ia telah menjadi seorang pengguna yang memiliki hak akses resmi. Namun, agar seorang *hacker* dapat melewati sistem keamanan tidak terbatas dengan hanya berusaha mendapatkan *username* dan *password*, ada banyak hal lain yang dapat dijadikan oleh *hacker* sebagai informasi penting untuk dapat melewati sistem keamanan, dimana untuk memperoleh informasi penting ini didapatkan oleh mereka dengan menggunakan *social engineering*.

KESIMPULAN

Seorang *hacker* dalam mendapatkan sasarannya tidak terbatas hanya dengan menggunakan komputer untuk mengeksploitasi kelemahan-kelemahan sasarannya. Mereka juga dapat menjadikan manusia sebagai sasarannya untuk mendapatkan informasi-informasi penting yang dapat digunakan untuk menerobos suatu sistem keamanan. Cara yang dipakai seperti itu ialah *social engineering*, yang bertujuan untuk membuat agar staff/manusia yang menjadi sasarannya memberikan informasi-informasi yang dia inginkan. Jika *hacker* tersebut telah memiliki informasi-informasi penting yang dibutuhkan olehnya untuk menerobos sistem keamanan, maka sistem keamanan yang telah dipasang akan menjadi tidak berguna. Untuk menanggulangi masalah seperti ini adalah dengan cara meningkatkan kesadaran dari staff/pengguna mengenai *social engineering* dan ancamannya. Selain itu perusahaan juga harus memiliki dokumen resmi yang jelas berupa standar, prosedur, atau kebijakan mengenai keamanan informasi, sehingga staff/pengguna dapat mengikuti, mematuhi, dan selalu menjadikan dokumen resmi tersebut sebagai acuan atas segala tindakan yang dilakukan di perusahaan tersebut.

Rekomendasi

Untuk menanggulangi teknik *social engineering* ada hal penting yang dapat dilakukan:

Yang pertama adalah meningkatkan kesadaran pengguna akan pentingnya sebuah informasi. Pengguna juga harus sadar bahwa dalam menjaga keamanan informasi, pengguna dari informasi itu sendiri memiliki peranan yang sangat penting, dimana kekuatan dari sebuah keamanan informasi sangat berpengaruh dari keterlibatan pengguna. Langkah kedua yaitu memberikan pemahan mengenai *social engineering* dan ancamannya. Hal ini bisa dilakukan dengan cara memperkenalkan kepada pengguna mengenai *social engineering* dan acaman yang dapat ditimbulkannya. Karena jika melihat kembali kasus Kevin Mitnick, masalah *social engineering* ini bukan masalah baru, melainkan masalah lama yang seringkali diabaikan oleh banyak orang, dan sekali lagi pengguna memiliki peranan yang sangat penting agar dapat menghindari ancaman *Social Engineering*.

Setelah sebuah perusahaan dapat mempersiapkan sumber daya manusianya yang kuat langkah ketiga ialah membuat dokumen resmi yang jelas mengenai standar, prosedur, dan kebijakan perusahaan akan keamanan informasi, dimana dokumen resmi ini harus ditandatangani oleh pimpinan puncak suatu perusahaan untuk menandakan bahwa masalah keamanan informasi menjadi perhatian utama perusahaan. Pembuatan dokumen resmi inii juga harus mengacu kepada standar keamanan informasi yang berlaku, yaitu mengacu kepada standar ISO seri 27000 tentang keamanan Informasi. Dengan mengikuti standar yang telah diakui di dunia keamanan informasi diharapkan pembuatan dokumen resmi perusahaan dapat memenuhi kebutuhan keamanan informasi. Staff/pengguna juga harus diarahkan agar dapat mengikuti dan mematuhi standar, prosedur, atau kebijakan perusahaan yang telah dibuat. Mereka juga harus dapat diarahkan jika terjadi hal apapun yang dapat menyebabkan bocornya informasi perusahaan untuk segera melaporkannya kepada atasan. Karena salah satu penyebab kenapa terjadinya penyerangan dengan menggunakan *social engineering* sulit dideteksi ialah karena staff/pengguna takut disalahkan jika mereka melaporkannya ke atasan, padahal hal ini jugalah yang sering menjadikan *social engineering* menjadi sebuah ancaman karena sulitnya terdeteksi tadi. Langkah terakhir ialah dengan menyiapkan perencanaan menegemen resiko. Walaupun dengan melakukan semua langkah yang ada diharapkan dapat menangkal serangan *Social Engineering* namun perusahaan harus tetap bersiap untuk kemungkinan terburuk, yaitu terjadinya insiden. Dengan adanya persiapan menegemen resiko diharapkan walau insiden terjadi, perushaan dapat memperkecil kerugian yang ditanggung sekecil mungkin. Adanya managemen resiko juga dapat membantu perusahaan agar tetap dapat menjalankan kegiatan perusahaan sehari-hari walaupun ada insiden yang sedang terjadi.

Daftar Pustaka

Allen, M. (2007). Social Engineering: A Means to Violate a Computer System. http://www.sans.org/reading_room/whitepapers/engineering/, diakses 14 Juli 2011).

Andres, A. (2007). *Surviving Security: How to Integrate People, Process, and Technology*. London: Taylor and Francis

Bannan, K. J. (2001) Social Engineering. *Internet World*, 1 Januari 2001.

[3]How to Protect Insiders from Social Engineering Threats. (2006). (http://technet.microsoft.com/en-us/library/cc875841.aspx, diakses 14 Juli 2011).

Indrajit, R. E. Seluk Beluk Teknik Social Engineering. (http://idsirtii.or.id/cyber-6/, diakses 12 Juli 2011).

How to Protect Insiders from Social Engineering Threats. (2006). (http://technet.microsoft.com/en-us/library/cc875841.aspx, diakses 14 Juli 2011).

Protect Against Social Engineering. (www.cisco.com/web/about/security/intelligence/mysdn-social-engineering.html/, diakses 14 Juli 2011).

Harl. (1997). People Hacking: The Psychology of Social Engineering. *Prosiding Kongres Access All Areas III.* 7 Mei 1997.

Gartner. 2005. Management Update: How Business Can Defend Against Social Engineering Attacks.

Indra, D. dan M. Chandrataruna. (2009). Pencuri Data adalah Karyawan Huawei. (http://teknologi.vivanews.com/news/read/41027-pencuri_data_adalah_karyawan_huawei/, diakses 15 Juli 2011)

Kevin Mitnick Sentenced to Nearly Four Years in Prison; Computer Hacker Ordered to Pay Restitution To Victim Companies Whose Systems Were Compromised. 1999 (http://www.cybercrime.gov/mitnick.htm/, diakses 15 Juli 2011)