Antisipasi Dampak *Social Engineering* Pada Bisnis Perbankan

Dani Indra Junaedi
Program Studi Teknik Informatika
STMIK Sumedang, Jl. Angkrek Situ No. 19, Sumedang, 45323 Indonesia
email : daniindra2405@yahoo.co.id

ABSTRACT
Perkembangan teknologi informasi membuat institusi perbankan mengubah strategi bisnis dengan menempatkan teknologi sebagai unsur utama dalam proses inovasi produk dan jasa. Kecanggihan teknologi yang diterapkan oleh institusi perbankan telah diakui mampu menangkal potensi kejahatan perbankan yang dilakukan oleh *hacker*. Menyadari semakin canggihnya perlindungan sistem perbankan, *hacker* tidak hanya beroperasi di balik komputer untuk menyerang targetnya, mereka juga menghampiri targetnya secara langsung untuk mendapatkan informasi berharga yang mereka butuhkan sehingga dapat mengakses sistem yang terlindungi oleh benteng keamanan dan membuat penanganan keamanan apapun menjadi tidak berguna, cara seperti inilah yang biasa disebut sebagai *Social Engineering*. Dalam *social engineering*, si pelaku memanfaatkan sifat alamiah dari manusia. Hal ini diartikan bahwa betapa sifat alami manusia dapat diketahui dan dipelajari juga dimanfaatkan untuk tujuan tertentu. Kejahatan *social engineering* sangat membahayakan bisnis perbankan karena berpotensi menimbulkan kerugian finansial, reputasi dan hukum bagi bank dan nasabahnya melalui serangan fisik dan serangan psikologis. Untuk mengurangi resiko tersebut, bank perlu untuk melatih dan mendidik staf mereka mengenai ancaman keamanan dan bagaimana caranya mengenali dan mengantisipasi serangan *Social Engineering*. Untuk mencegah dampak *social engineering* pada bisnis perbankan diperlukan langkah antisipatif melalui mencegah kebocoran password, keamanan akses informasi, verifikasi kontak, mengikuti prosedur, pelaporan tindakan mencurigakan, menjaga emosi, pelatihan berkelanjutan dan memberikan edukasi kepada nasabah

***Kata Kunci** : Perbankan, Hacker, Social Engineering, Keamanan Informasi, Nasabah*

1. Introduction

Perkembangan teknologi telekomunikasi dan informatika dipicu oleh ketatnya kompetisi yang selalu melahirkan berbagai inovasi dan lompatan teknologi telematika. Hal ini tentu saja sangat mempengaruhi pola dan strategi bisnis, tidak terkecuali industri perbankan. Keragaman layanan, kemudahan, kecepatan dan harga jasa yang sangat murah menjadi tuntutan yang sangat umum dari nasabah.

Kemajuan suatu sistem perbankan harus didukung oleh teknologi informasi. Semakin berkembang dan kompleksnya fasilitas yang diterapkan perbankan untuk memudahkan pelayanan akan sejalan dengan adopsi teknologi yang dimiliki oleh suatu bank yang bertujuan untuk memudahkan operasional juga untuk memudahkan pelayanan terhadap nasabah.

Perkembangan teknologi informasi membuat institusi perbankan mengubah strategi bisnis dengan menempatkan teknologi sebagai unsur utama dalam proses inovasi produk dan jasa. Seperti halnya pelayanan *e-banking* melalui ATM, *phone banking* dan *Internet Banking* yang merupakan bentuk dari pelayanan bank yang mengubah pelayanan transaksi manual menjadi pelayanan transaksi yang berbasis teknologi. Faktor kepercayaan dan efisiensi serta kualitas layanan menjadi alasan bagi institusi perbankan untuk selalu menata ulang bisnisnya dengan mencermati ketersediaan inovasi teknologi serta dampaknya bagi kelangsungan dan pertumbuhan bisnis.

Untuk memastikan kelancaran dan keamanan sistem operasional, institusi perbankan menerapkan sistem kemanan yang seimbang dengan kecanggihan teknologi yang diterapkan. Cara yang digunakan untuk mencegah potensi gangguan dan serangan terhadap keamanan sistem komputer adalah dengan menerapkan program dan sistem komputer yang rumit namun memberikan jaminan keamanan. Pembaharuan sistem komputer dan enkripsi data tingkat tinggi adalah solusi umum untuk permasalahan yang mungkin terjadi. Tidak hanya potensi resiko yang berkenaan dengan teknologi tapi resiko-resiko lain juga sudah diperhitungkan.

Risiko dalam konteks perbankan adalah suatu kejadian potensial, baik yang dapat diperkirakan (*anticipated*) maupun yang tidak dapat diperkirakan (*unanticipated*) yang berdampak negatif ke pendapatan maupun modal Bank. Segala bentuk potensi resiko sudah diperhitungkan oleh institusi perbankan.

Bank Indonesia selaku bank sentral telah mengatur dalam SE BI No.13/23/DPNP tanggal 25 Oktober 2013 telah mengatur mengenai Manajemen Risiko yaitu kecukupan prosedur dan metode yang digunakan dalam melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko yang timbul dari kegiatan usaha bank sehingga tetap dapat terkendali (*manageable*) pada batasan / limit yang masih dapat diterima (*risk appetite bank*) serta menguntungkan. Ada delapan resiko yang harus diperhitungkan institusi perbankan yaitu RISIKO KREDIT, RISIKO PASAR, RISIKO LIKUIDITAS, RISIKO OPERASIONAL, RISIKO HUKUM, RISIKO STRATEGIK, RISIKO REPUTASI dan RISIKO KEPATUHAN. Dengan antisipasi resiko yang intensif tentunya bank memberikan jaminan keamanan kepada semua pihak yang terkait termasuk nasabah dan *stakeholder*.

2. Research Method

2.1. Perbankan dan *Cybercrime*

Kecanggihan teknologi yang diterapkan oleh institusi perbankan telah diakui mampu menangkal potensi kejahatan perbankan yang dilakukan oleh *hacker*. Tidak dipungkiri, perbankan adalah target potensial para pelaku kejahatan termasuk *cybercrime*. Selalu terjadi kompetisi intelegensi antara perbankan dan pelaku kejahatan, perbankan mengantisipasi potensi resiko dan penjahat mencari celah kelemahan yang bisa ditembus. Jika aktivitas kejahatan terjadi maka perbankan akan melakukan perbaikan sistem supaya tidak terjadi lagi, begitu seterusnya.

Cybercrime didefinisikan sebagai kejahatan dengan obyek komputer (*hacking, phishing, spam*) atau menggunakan komputer sebagai alat untuk melakukan kejahatan (pornografi anak, prostitusi *online*, kejahatan dengan motif kebencian). Penjahat *cyber* dapat menggunakan teknologi komputer untuk mengakses informasi pribadi, rahasia dagang bisnis, atau menggunakan internet untuk tujuan eksploitatif atau berbahaya. Penjahat juga dapat menggunakan komputer untuk komunikasi dan dokumen atau penyimpanan data. Penjahat yang melakukan kegiatan ilegal yang sering disebut sebagai *hacker*.

Terdapat beberapa jenis *Cybercrime*, yaitu:

1. Penggandaan Kartu . Misalnya: Skimming ATM, Pencurian nomor Kartu kredit.
2. Nama Domain Misalnya : calo / *cybersquat*, plesetan / *typosquating* nama domain, nama pesaing.
3. Pembajakan / menggunakan komputer orang lain tanpa izin (*Hijacking*).
4. Akses data tanpa izin (*Hacking*), bisa dengan virus atau cara lain.
5. Membocorkan data (*Data Leakage*), terutama data rahasia negara / perusahaan.
6. Pembajakan software (*Software piracy*) terhadap hak cipta yang dilindungi HAKI.
7. Hoax: pembuatan dan penyebaran berita palsu, dll.

Menyadari semakin canggihnya perlindungan sistem perbankan, *hacker* tidak hanya beroperasi di balik komputer untuk menyerang targetnya, mereka juga menghampiri targetnya secara langsung untuk mendapatkan informasi berharga yang mereka butuhkan sehingga dapat mengakses sistem yang terlindungi oleh benteng 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, *Social Engineering Hacker* dapat menjadikan kecerobohan, kemalasan, kesopanan, bahkan antusiasme dari seorang staff di sebuah organisasi sebagai targetnya. korban tidak menyadari kalau mereka telah ditipu.

2.2. *Social Engineering* Sebagai Salah Satu Bentuk Cybercrime

Manusia sering dianggap sebagai komponen terlemah dalam suatu sistem jaringan komputer. Walaupun suatu sistem telah dilindungi dengan piranti keras dan piranti lunak canggih untuk menangkal serangan seperti dipasangnya *firewall*, anti virus, IDS/IPS, dan lain sebagainya, tetapi jika manusia yang mengoperasikannya lengah, maka keseluruhan peralatan itu menjadi tidak berarti. Pelaku kriminal dunia maya sangat paham akan hal ini sehingga mereka menggunakan cara *social engineering* untuk mendapatkan informasi penting yang disimpan secara rahasia oleh manusia untuk tujuan tertentu.

Menurut [1] 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.

Dalam *social engineering*, si pelaku memanfaatkan sifat alamiah dari manusia. Hal ini diartikan bahwa betapa sifat alami manusia dapat diketahui dan dipelajari juga dimanfaatkan untuk tujuan tertentu. Banyak metode yang digunakan pelaku kejahatan dalam melancarkan usahanya agar bisa mendapatkan apa yang diinginkan. Biasanya dilakukan dengan cara memanfaatkan sisi psikologis seperti memuji, bersikap ramah, melakukan suatu hal yang berlebihan agar lebih dekat dengan targetnya seperti memberi sesuatu yang bisa membuat korban menjadi merasa senang dan bahagia, ataupun dengan cara membujuk. Banyak cara pelaku bisa mempermainkan emosi target sehingga tanpa sadar akan memberikan informasi rahasia. Dalam *social engineering* terdapat beberapa pola umum yang biasa dilakukan oleh para *hacker*, antara lain:

1. Mengumpulkan informasi, Informasi bisa berupa struktur organisasi dan daftar nama didalamnya, tanggal ulang tahun, dan sebagainya untuk mengembangkan relasi dengan targetnya.
2. Mengembangkan relasi/hubungan, Setelah mendapatkan informasi yang cukup, selanjutnya adalah berusaha mendekati salah satu pegawai yang sudah dijadikan sasaran.Informasi yang telah diperoleh digunakan untuk mendapatkan kepercayaan dari sasaran tersebut.
3. Mengeksploitasi, Setelah mendapatkan kepercayaan dari orang yang dijadikan sasaran, langkah selanjutnya adalah mengeksploitasi informasi-informasi yang telah didapat untuk masuk ke dalam sistem perusahaan.
4. Eksekusi, Setelah berhasil masuk ke dalam sistem, *hacker* tersebut dapat dengan mudah mencuri, merubah, bahkan merusak sistem dan data tanpa terhalangi sistem keamanan.

2.3. Ancaman *Social Engineering* Terhadap Sistem

Sasaran utama dari *social engineering* [2] adalah untuk memperoleh akses illegal ke dalam suatu sistem atau informasi perbankan dalam rangka melakukan :

1. *Fraud* (penipuan atau kecurangan),
2. Penyusupan ke dalam jaringan,

3. Aktivitas mata-mata,
4. Pencurian identitas,
5. Atau hanya untuk menghadirkan gangguan pada sistem atau jaringan.

Penggunaan internet yang semakin luas memiliki andil dalam serangan. Pada umumnya, pelaku lebih menyukai menyerang organisasi yang besar seperti perbankan. Kompleksitas keamanan perbankan menjadi tantangan tersendiri untuk para *hacker*s, belum lagi kompleksitas dampak yang ditimbulkan jika berhasil ditembus. Cara *social engineering* lebih mudah untuk mendapatkan akses daripada menggunakan teknik-teknik hacking yang biasa digunakan. Jika mereka sudah bisa mendapatkan akses terhadap sasaran, *hacker* dapat dengan mudah masuk ke kantor bank dengan berpura-pura sebagai pekerja maintenance atau konsultan yang memiliki akses. Kemudian sang penyusup berkeliling kantor sampai dia menemukan kata sandi yang tercecer dan keluar dari gedung dengan informasi yang cukup untuk mengeksploitasi jaringan organisasi selanjutnya mereka bisa melakukan apa saja sesuai dengan tujuannya. 4 (empat) kelompok/ individu di perbankan yang kerap menjadi korban tindakan *social engineering*, yaitu:

1. *Receptionist* dan/atau *Help Desk* sebuah kantor bank, karena merupakan pintu masuk ke dalam bank yang biasanya memiliki pengetahuan yang standar mengenai perusahaan dan pegawai yang ada di bank tersebut. Kewajiban untuk selalu ramah dan memberikan pelayanan terbaik bisa menjadi celah bagi pelaku *social engineering*.
2. *IT Support* yang melayani pimpinan dan manajemen bank, mereka biasanya memegang akses penting ke data dan informasi rahasia, berharga, dan strategis;
3. *Administrator* sistem dan pengguna komputer, karena mereka memiliki otoritas untuk mengelola password dan account semua pengguna teknologi informasi
4. Mitra kerja atau vendor, karena mereka adalah pihak yang menyediakan berbagai teknologi beserta fitur yang dipergunakan oleh manajemen dan karyawan bank;
5. Karyawan baru yang masih belum begitu paham mengenai prosedur standar keamanan informasi di bank.

Pelaku *Social engineering* tidak membutuhkan keahlian *hacking* dan teknologi canggih untuk melakukan aksinya, pelaku mengambil keuntungan dari kurangnya kesadaran tiap individu untuk menjaga keamanan informasi [3]. Karena sifatnya yang sangat manusiawi dan memanfaatkan interaksi sosial, teknik-teknik memperoleh informasi rahasia berkembang secara sangat variatif. Beberapa contoh adalah sebagai berikut:

1. Ketika seseorang memasukkan password di ATM atau di PC, yang bersangkutan "mengintip" dari belakang, sehingga karakter passwordnya dapat terlihat;
2. Mengaduk-ngaduk tong sampah tempat pembuangan kertas atau dokumen kerja perusahaan untuk mendapatkan sejumlah informasi penting atau rahasia lainnya yang terbuang oleh pegawai;
3. Menyamar menjadi "*office boy*" untuk dapat masuk bekerja ke dalam kantor manajemen atau pimpinan puncak perusahaan guna mencari informasi rahasia;
4. Ikut masuk ke dalam ruangan melalui pintu keamanan dengan cara "menguntit" pegawai atau mereka yang memiliki akses legal;
5. Mengatakan secara meyakinkan bahwa yang bersangkutan lupa membawa *ID-Card* yang berfungsi sebagai kunci akses sehingga diberikan bantuan oleh satpam;
6. Membantu membawakan dokumen atau tas atau *notebook* dari pimpinan dan manajemen dimana pada saat lalai yang bersangkutan dapat memperoleh sejumlah informasi berharga;
7. Melalui *chatting* di dunia maya, si penjahat mengajak ngobrol calon korban sambil pelan-pelan berusaha menguak sejumlah informasi berharga darinya;

8. Dengan menggunakan situs *social networking* dengan melakukan komunikasi yang mengarah pada proses penggalian informasi rahasia;

3. Result and Analysis

Sebagai lembaga intermediary yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya dalam bentuk pinjaman, perbankan mengandalkan kepercayaan sebagai modal utama dalam menjalankan bisnisnya. Faktor utama masyarakat menyimpan uang di bank adalah karena percaya bahwa bank akan menjaga uangnya dengan aman selain berbagai fitur pelayanan yang ditawarkan. Bank tahu betul akan hal ini sehingga berbagai cara akan dilakukan untuk menjaga kepercayaan tersebut. Hal-hal yang berpotensi merusak kepercayaan selalu diantisipasi dengan berbagai proteksi mulai dari sistem, fisik hingga SDM yang terlibat di dalamnya.

Jika melihat keamanan sistem yang diterapkan oleh institusi perbankan sepertinya akan sulit bagi *hacker* manapun untuk bisa menembusnya tapi tidak dengan cara *social engineering* yang justru memanfaatkan kelengahan manusia yang juga termasuk di dalam rangkaian keamanan sistem tersebut.

Ada beberapa metode *Social Engineering* yang biasa dilakukan *hacker* untuk bisa mengganggu keamanan sistem perbankan

1. *Pretexting*
   Pelaku melakukan pendekatan dengan korban dan berusaha menggali informasi atau membujuk korban untuk melakukan suatu tindakan, seperti memberitahukan password atau melakukan instalasi program berbahaya.
2. *Phising*
   Pelaku mengirimkan email yang seolah-olah berasal dari sumber terpercaya dan berusaha mempengaruhi korban untuk mengirimkan informasi sensitif seperti password, membuka file atau melakukan instalasi aplikasi berbahaya.
3. *Shoulder surfing*
   Pelaku menggunakan teknik pengamatan langsung contohnya dengan mengintip password, PIN, dan no rekening yang diinput oleh korban.
4. *Dumpster Diving*
   Pelaku mencari informasi dari sampah seperti laporan, resi, dan dokumen yang berisi informasi penting dan juga dari post-it yang ditempelkan di meja kerja yang terkadang menyimpan informasi seperti password.
5. *Tailgating*
   Pelaku yang tidak mempunyai akses masuk ke dalam area terbatas dengan mengikuti pekerja yang mempunyai akses.

Area kantor bank adalah area yang sensitif. Akses nasabah hanya sebatas *banking hall*, selebihnya adalah area yang harus steril dari orang-orang luar. Sesama pegawai pun mempunyai ruang privasi tersendiri, tidak setiap pegawai bisa bebas memasuki ruang-ruang tertentu. Misalnya ruang berkas yang hanya bias diakses oleh petugas arsip, ruang teller yang tidak boleh dimasuki oleh pegawai lain selain teller. Resiko kehilangan dokumen, berkas pinjaman ataupun uang akan sangat besar jika ada orang selain pegawai yang berkepentingan masuk ke ruang-ruang tertentu apalagi ruang server yang menjadi "jantung" operasional kantor bank. Jika server terganggu atau terinfeksi aplikasi berbahaya maka operasional bank akan lumpuh.

Setiap komputer dalam sistem operasi kantor bank memiliki nama sesuai dengan penggunanya. User ditentukan secara legal lengkap dengan surat keputusan dan segala kewenangannya. Tidak diperbolehkan pegawai lain menggunakan atau mengakses komputer yang bukan miliknya.

Kebocoran password adalah hal yang sangat ditabukan dalam operasional perbankan. Konsekuensi dari kebocoran password adalah pemutusan hubungan kerja (PHK) bagi si pemilik password. Setiap pegawai bank memiliki kewenangan masing–masing dalam operasional dan setiap pekerjaan tidak sepenuhnya memiliki kewenangan individual dalam memberikan keputusan. Selalu ada prinsip MCS (Maker, Checker, Signer). Maker adalah pembuat pekerjaan, dia bekerja sesuai dengan uraian jabatan yang dimilikinya. Ketika pekerjaannya selesai maka dia akan mengirimkannya kepada atasan yang akan memeriksa kebenaran dari hasil kerjanya, inilah yang disebut dengan Checker. Setelah diyakini kebenarannya maka diteruskan kepada atasan yang lebih tinggi atau pimpinan untuk diberikan persetujuan (Signer). Rangkaian pekerjaan ini bisa dilakukan by sistem melalui mekanisme approval oleh pejabat MCS. Hampir di setiap kantor bank menganut sistem MCS dalam setiap pekerjaan untuk menjamin kebenaran dan keamanan transaksi. Secara sistem, transaksi baru bisa terjadi jika ketiga tahapan ini sudah dilakukan berarti ada tiga password yang digunakan untuk terjadinya suatu transaksi. Kebocoran password di salah satu proses akan menyebabkan kesalahan transaksi dan kerugian di pihak bank atau nasabah. Jika hal ini terjadi, tidak hanya kerugian finansial yang didapat tapi juga reputasi suatu bank akan hancur, kehilangan kepercayaan nasabah, kehilangan privasi dan terancam hukuman pidana.

Adapun Informasi penting yang dapat dimanfaatkan dari *social engineering*

1. Username dan password
2. Data pegawai
3. Data Nasabah
4. Strategi Bisnis
5. Laporan Perusahaan
6. Kebijakan internal
7. Dokumen Rahasia

3.1. Pencegahan Sosial Enginering pada Bisnis Perbankan

Social engineering berfokus pada mata rantai terlemah dalam rantai kemanan informasi-manusia. Kenyataannya, hampir semua solusi informasi sangat bergantung pada manusia. Kelemahan ini bersifat universal, dan terbebas dari hardware, software, platform, jaringan, dan usia peralatan. *Social engineering* telah mencapai tingkatan tertinggi kematangan sebagai strategi dalam membobol keamanan informasi. Keamanan ini digunakan perusahaan untuk melindungi apa yang dianggap asset-aset paling penting perusahaan, termasuk informasi. Mekanisme keamanan yang terbaik pun dapat ditembus dengan *social engineering*. Untuk mengurangi resiko tersebut, bank perlu untuk melatih dan mendidik staf mereka mengenai ancaman keamanan dan bagaimana caranya mengenali serangan.

Untuk dapat menggagalkan suatu serangan, akan lebih mudah jika kita mengenali serangan tersebut. beberapa pertanda serangan *social engineering* yang dapat dikenali antara lain menolak memberi kontak, terburu-buru, mencatut nama, intimidasi, hal-hal kecil seperti salah pengejaan nama atau pertanyaan agak aneh, dan meminta informasi terlarang.

Saat dimana seorang pegawai merasakan adanya suatu keganjilan, dia memerlukan prosedur untuk melaporkan insiden yang terjadi. Sangat penting untuk adanya seseorang yang bertanggung jawab untuk melacak insiden-insiden ini. Selain itu pula, pegawai tersebut perlu memberitahu rekan-rekan kerjanya di posisi yang sama bahwa mereka pun mendapat ancaman serangan serupa.

Untuk lebih mengenali *social engineering*, setiap Bank dapat membantu menjamin keamanan dengan cara mengadakan program-program pelatihan kewaspadaan akan keamanan. Kewaspadaan kontinu di seluruh kantor bank adalah kunci dari perlindungan berkelanjutan.

Serangan *social engineering* terdiri dari aspek fisik dan aspek psikologis. Aspek fisik mencakup lokasi serangan seperti tempat kerja, telepon, mengacak-acak tong sampah, internet dan sebagainya.

Sedangkan aspek psikologis mencakup segala sesuatu yang berkenaan dengan cara serangan itu terjadi seperti persuasi, menirukan orang, mencari muka, mencari kesamaan dan keramah-tamahan. Cara memerangi *social engineering* membutuhkan tindakan pada kedua aspek tersebut. Manajemen harus memahami pentingnya mengembangkan dan mengimplementasikan prosedur dan kebijakan security yang baik. Pelatihan pegawai sangatlah penting Manajemen wajib untuk mengerti bahwa seluruh uang yang mereka habiskan untuk patch perangkat lunak, perangkat keras untuk kemanan, audit akan sia-sia tanpa persiapan yang cukup untuk menangkal *social engineering* dan reverse *social engineering* (Rick Nelson :"Methods of Hacking: *Social Engineering*,").

Pencegahan Terhadap Serangan Fisik dilakukan dengan cara :

1. Pemeriksaan kartu identitas bagi siapapun yang memasuki gedung
2. Beberapa dokumen khusus perlu untuk dikunci dalam laci atau tempat penyimpanan aman
3. Dokumen-dokumen lainnya perlu di shredding agar tidak bisa dibaca oleh pihak-pihak yang mungkin melakukan dumpster diving.
4. Media-media magnetik harus dihapus isinya agar datanya tidak bisa dipulihkan kembali .
5. Bila perlu, tong-tong sampah harus dikunci dan diawasi.
6. Semua perangkat yang terhubung dalam jaringan (termasuk sistem remote) perlu diproteksi dengan kata sandi.

Serangan psikologis dilakukan dengan cara merubah emosi seseorang sesuai dengan keinginan pelaku *social engineering* dengan cara melakukan persuasi, menirukan orang, mencari muka, mencari kesamaan dan keramah-tamahan.

Operasional perbankan bisa berjalan dengan baik karena kedisiplinan pegawainya pada Standard Operating Procedure (SOP) yang telah ditetapkan. Bekerja diluar kewenangannya berpotensi fraud. Tujuan dari serangan psikologis adalah membuat pegawai bank bekerja keluar dari SOP-nya, melakukan sesuatu diluar kewenangannya sesuai dengan keinginan pelaku *social engineering*. Misalnya petugas analis kredit yang melakukan manipulasi data di lapangan, membuat hasil analisa dengan usulan kredit yang lebih besar dari kondisi sebenarnya karena terbujuk oleh nasabahnya. Kondisi ini menyebabkan over kredit yang beresiko menyebabkan kredit macet.

Kemudian pernah terjadi di salah satu bank ketika seorang manajer operasional memerintahkan teller untuk mencairkan giro senilai Rp 1.500.000.000,- tanpa prosedur yang benar. Dana giro belum tersedia, tapi karena pelaku berhasil meyakinkan manajer bank dan diperkuat nota faximile yang dikirimkan oleh sindikat pelaku, maka dana tersebut dicairkan tanpa proses validasi karena manajer bisa diyakinkan bahwa dana tersebut akan tersedia beberapa jam kemudian. Ternyata dana tersebut tidak pernah ada, akhirnya manajer bank tersebut harus mengganti kerugian bank dan diproses hukum.

Kasus lain juga pernah terjadi ketika seorang customer service di sebuah bank kedatangan teman lama yang berkunjung ke kantornya dan bermaksud membuka rekening deposito. Si customer service kemudian mengeluarkan bilyet deposito dari ruang manajer yang saat itu kebetulan sedang tidak berada di tempat. Manajer memang menitipkan kunci lemari tempat penyimpanan surat berharga kepadanya. Disaat customer service lengah, pelaku kemudian pamit berpura pura mau mengambil uang di mobil padahal langsung kabur dengan membawa beberapa lembar bilyet deposito. Belakangan diketahui kalau ternyata bilyet tersebut digunakan untuk kejahatan.

Mengantisipasi serangan psikologis pelaku *social engineering* tidak mudah karena sifat dan karakter manusia tidak sama. Selain itu kondisi dan orientasi manusia bisa berubah dari waktu ke waktu. Kondisi psikologis seseorang bisa terbentuk oleh lingkungan atau bisa muncul karena suatu rangsangan. Keterbatasan-keterbatasan inilah yang dimanfaatkan oleh pelaku. Cara mengantisipasinya adalah dengan melatih pegawai agar selalu waspada, pengaturan jam istirahat yang tepat dan pembuatan komitmen untuk tetap bekerja sesuai SOP.

3.2. Pencegahan *Social Engineering*

3.2.1. Teknis Pencegahan

1. Password
   a. Menjaga kerahasiaan password.
      Jika seseorang menghubungi dan menanyakan password, bisa dipastikan merupakan penipuan. Selain itu jangan menyimpan informasi seperti password dengan menuliskannya dikertas dan menempelkannya di meja kerja. Jangan pernah membagi password melalui telepon pada siapapun baik yang dikenal atau tidak
   b. Password timer
      Seringkali pegawai lupa melakukan proses logout dari aplikasi komputer ketika meninggalkan pekerjaan untuk suatu keperluan. Hal ini perlu diantisipasi dengan mengatur waktu aplikasi jika tidak aktif untuk logout secara otomatis sehingga kemungkinan orang lain untuk masuk ke dalam aplikasi sangat kecil karena memerlukan password untuk login kembali.
   c. Karakter Password
      Dalam penggunaan password, di usahakan jangan ada sangkut paut nya dengan identitas diri kita. Karena hal tersebut sangatlah sensitif. Buatlah password yang unik dan tidak mudah di tebak oleh siapapun. kombinasi karakter di password sangat di anjurkan. dan hindari password yang menginputkan tanggal lahir, nama panggilan, dan bersifat sensitif lainnya. Usahakan pula mengganti password baru dalam beberapa jangka waktu ke depan demi keamanan
2. Keamanan Informasi
   a. Jangan melakukan sharing informasi yang menyangkut pekerjaan di media social
      Data perusahaan seperti data nasabah, data pekerja, dan laporan merupakan dokumen rahasia perusahaan jangan pernah melakukan sharing hal-hal tersebut di media sosial.
   b. Selalu berhati-hati dan waspada dalam berinteraksi dalam dunia maya. Khususnya dalam ber sosial media. Diusahakan informasi pribadi jangan di umbar seperti tanggal lahir dan lokasi pendidikan kita atau alamat karena bersifat sensitif. Informasi tersebut bisa dimanfaatkan oleh orang tidak bertanggung jawab dan menjadi peluang bagi pelaku kejahatan.
   c. Hindarilah membicarakan/mendiskusikan infromasi mengenai perusahaan pada pihak yang tidak perlu mengetahuinya, tempat umum seperti restoran dan angkutan umum dan melalui email public / instant messenger / media sosial
   d. Batasi informasi yang diberikan ke pihak luar, mulai dari konsultan, vendor, supplier, dan juga pekerja magang / kerja praktik
   e. Selalu menjaga barang-barang yang berisi informasi-informasi penting khususnya handphone. Berilah security pada handphone tersebut baik secara sistem ataupun per aplikasi yang berisi informasi sensitif. Karena kita tidak tahu bila handphone itu tidak bersama kita atau hilang.
3. Verifikasi Ulang Kontak
   Jangan mudah percaya ketika dihubungi oleh yang mengaku dari bank, operator telepon atau organisasi yang melakukan validasi data pribadi dan kita tidak yakin dengan penelepon. Sebaiknya menanyakan nama orang tersebut dan nomor teleponnya, kemudian bandingkan

nomor telepon tersebut dengan nomor telepon yang berasal dari sumber terpercaya atau yang tercantum pada website resmi perusahaan tersebut.

4. Ikuti prosedur dan ketentuan Security yang sudah ditentukan oleh Bank, laporkan aktifitas yang mencurigakan ke Bagian Terkait
5. Jaga Emosi
   Selalu menjaga kestabilan emosi dalam hal pembicaraan dengan orang lain walaupun itu orang terdekat sekalipun. Karena emosi kita dapat menjadi pancingan pelaku dalam melakukan aksinya.
6. Pelatihan Berkelanjutan
   Pentingnya untuk melatih pegawai tidak hanya mencakup help desk, namun mencakup seluruh pegawai. Para pegawai harus dilatih dalam hal bagaimana mengidentifikasi informasi yang seharusnya dianggap rahasia, dan memiliki pemahaman penuh akan tanggung jawab mereka untuk melindungi rahasia tersebut. Demi berhasilnya usaha ini, organisasi-organisasi harus menjadikan keamanan komputer sebagai bagian dari tiap pekerjaan, terlepas dari apakah para pegawai menggunakan komputer atau tidak. Semua orang di dalam organisasi wajib untuk mengerti mengapa sangat penting agar informasi rahasia diperlakukan seperti itu, dengan demikian mereka merasa bertanggung jawab atas keamanan jaringan organisasi.

3.2.2. Upaya Pencegahan Social Enginering terhadap Nasabah Bank

Tidak hanya internal perbankan yang berpotensi terkena dampak *social engineering*. Nasabah perbankan juga memiliki potensi terkena dampak yang sama. Potensi kerugian perbankan mencakup finansial, reputasi dan tuntutan hukum. Hal ini tidak jauh berbeda dengan yang akan dialami nasabah jika menjadi korban social engieering.

Contoh kasus :

1. Seorang nasabah mengadukan kehilangan sejumlah uang di tabungannya setelah dia kehilangan dompet yang didalamnya berisi kartu ATM. Setelah diselidiki ternyata telah terjadi pengambilan di beberapa ATM yang dilakukan oleh pelaku. Kenapa bisa ? padahal hanya kartu ATM nya saja. Ternyata si nasabah menuliskan pin ATM di secarik kertas yang juga ada di dompet tersebut
2. Seorang nasabah seperti terhipnotis dipandu untuk mentransfer sejumlah uang ke rekening orang lain melalui handphone setelah menghubungi nomor tertentu yang memberi berita bahwa si nasabah mendapatkan hadiah
3. password internet banking bocor ke orang lain sehingga ketika handphone jatuh ke orang tersebut, semua dana di tabungannya berpindah ke rekening lain.
4. kartu identitas jatuh ke tangan orang lain sehingga disalahgunakan untuk membuka rekening dan dijadikan rekening penampungan dana transfer hasil penipuan

Masih banyak lagi contoh kasus yang sudah terjadi menimpa nasabah bank yang diakibatkan *social engineering*. Salah satu cara sederhana namun diyakini cukup ampuh menangkal kejahatan *social engineering* adalah dengan cara memberikan edukasi kepada nasabah. Selain itu, dengan edukasi akan mampu meningkatkan awareness. Nasabah akan lebih berhati-hati ketika ingin melakukan transaksi, atau ketika meng-input data-data pribadinya. Di samping itu ketika melihat ketidaknormalan dalam sebuah layanan transaksi, nasabah akan cepat melakukan konfirmasi.

Kejahatan berbasis teknologi mengincar sektor perbankan, baik sistem banknya sendiri atau langsung ke individu nasabahnya. Pihak bank pun sudah sangat paham kerentanan ini, sehingga akan lebih baik jika optimal dalam mengedukasi nasabahnya. Edukasi harus dilakukan dengan jelas dan

mudah dipahami dan sebisa mungkin harus detail sehingga pengguna bisa memahami kerentanan atau kemungkinan resiko yang akan terjadi.

Pihak bank bisa memberi informasi tentang jenis-jenis kerentanan yang ada semisal penggandaan kartu, contoh-contoh kasus metode *social engineering*, atau imbauan untuk meng-update antivirus. Selain itu akan lebih baik lagi kalau bank juga meyertakan tips agar terhindar dari potensi kejahatan fraud dalam edukasinya. Selain menambah pengetahuan, cara-cara ini juga diyakini bisa membuat nasabah lebih percaya diri dalam melakukan transaksi, dan semakin loyal dengan bank tempatnya menyimpan dana. Cara edukasi yang bisa dilakukan oleh pihak bank adalah sebagai berikut :

1. Membagikan Brosur atau Buku saku yang berisi tentang gambaran, perilaku dan bahaya *social engineering* supaya nasabah bisa mengenal dan mengantisipasi supaya terhindar dari dampaknya.
2. Memasang pengumuman/peringatan di atm atau lokasi lokasi tertentu supaya nasabah lebih berhati hati terhadap ancaman *social engineering*
3. berkoordinasi dengan petugas keamanan di lokasi ATM, jika ada perilaku mencurigakan dari terduga pelaku *social engineering* akan cepat diantisipasi
4. Membuat iklan layanan masyarakat di televisi tentang potensi bahaya *social engineering*.
5. Menayangkan video tentang bahaya *social engineering* di banking hall atau ruang tunggu nasabah.
6. menyebarkan SMS kepada setiap nasabah mengenai bahaya *social engineering*

4. Conclusion

Perkembangan teknologi informasi membuat institusi perbankan mengubah strategi bisnis dengan menempatkan teknologi sebagai unsur utama dalam proses inovasi produk dan jasa.

Untuk memastikan kelancaran dan keamanan sistem operasional, institusi perbankan menerapkan sistem kemanan yang seimbang dengan kecanggihan teknologi yang diterapkan. Jika melihat keamanan sistem yang diterapkan oleh institusi perbankan sepertinya akan sulit bagi *hacker* untuk bisa menembusnya. *Hacker* kemudian menggunakan cara *social engineering*.

Social engineering berfokus pada mata rantai terlemah dalam rantai kemanan informasi-manusia. Kenyataannya, hampir semua solusi informasi sangat bergantung pada manusia. Kelemahan ini bersifat universal, dan terbebas dari hardware, software, platform, jaringan, dan usia peralatan. *social engineering* telah mencapai tingkatan tertinggi kematangan sebagai strategi dalam membobol keamanan informasi. Mekanisme keamanan yang terbaik pun dapat ditembus dengan *social engineering*.

Untuk mengurangi resiko tersebut, bank perlu untuk melatih dan mendidik staf mereka mengenai ancaman keamanan dan bagaimana caranya mengenali dan mengantisipasi serangan *Social Engineering*. Nasabah bank juga memiliki potensi terkena dampak *social engineering* yang sama untuk mengantisipasinya, bank perlu melakukan edukasi terhadap nasabahnya.

References

[1] Indrajit, R. E. Seluk Beluk Teknik *Social Engineering*. (http://idsirtii.or.id/cyber-6/ diakses 04 Mei 2017).

[2] Rick Nelson, "Methods of Hacking: *Social Engineering*," the Institute for Sistems Research, University of Maryland. (http://www.academia.edu /4903480/Methods_of Hacking-*social Engineering*), diakses 10 Mei 2017)

[3] How to Protect Insiders from *Social Engineering* Threats. (2006). (http://msdn.microsoft.com/en-us/library/cc875841.aspx, diakses 06 Mei 2017)