EFEKTIVITAS KEAMANAN INFORMASI DALAM MENGHADAPI ANCAMAN *SOCIAL ENGINEERING*

EFFECTIVENESS OF INFORMATION SECURITY THREATS FACING SOCIAL ENGINEERING

Suherman[1], Pujo Widodo[2], Dadang Gunawan[3]
Prodi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan
(suherman2112@gmail.com)

Abstrak – Indonesia adalah sebuah negara yang sedang berkembang. Perekonomian Indonesia sedang meningkat dan didukung dengan kemajuan teknologi dan informasi. Dunia perbankan di Indonesia sudah cukup bagus, sehingga kejahatan cyber akan semakin besar Social engineering merupakan suatu metode dalam kejahatan cyber.Ancaman kejahatan cyber saat ini sangat mempengaruhi kerentanan keamanan informasi, khususnya di dunia perbankan. Bentuk nyata adalah dengan adanya pembobolan kartu kredit ,pencurian data oleh karyawan dalam perusahaan dan lain sebagainya. E.B Taylor menyatakan bahwa kerentanan yang dapat ditembus oleh social engineering melalui kebiasaan, ilmu pengetahuan penekanan dan kepercayaan. Perusahaan merespon akan bahaya kejahatan cyber crime yaitu ancaman social engineering, akibat yang ditimbulkannya adalah kehancuran akan keamanan informasi Pelaksanaan efektivitas dapat berjalan dengan baik apabila bagian bagian yang terlibat dalam proses pelaksanaannya dapat memerankan peranannya dengan baik. Adapun tesis ini bertujuan adalah untuk menganalisis efektifitas dan penerapan prosedur operasional dan kebiasaan yang dilakukan karyawan untuk keamanan informasi dalam menghdapi bahaya sosial engineering. Penelitian ini menggunakan metode kualitatif dengan teknik pengumpulan data yaitu, wawancara, observasi, studi pustaka, dan studi dokumen. Hasil dari penelitian ini adalah bahwa melalui penerapan Standar Operasional Prosedur yang benar, rasa memiliki, penggunaan surat dalam melakukan suatu permintaan dan mengirim email keseluruh karyawan tentang keamanan informasi secara berkala. Sehingga Perusahaan dapat terhindar dari ancaman social engineering .Maka efektivitas keamanan informasi dalam menghadapi bahaya social engineering dapat terwujud. Keamanan informasi perbankan dapat terjaga baik secara nasional maupun internasional.
Kata kunci: *Keamanan Informasi, Social Engineering, Standard Operasional Prosedur, Efektivitas*

Abstract– *Indonesia is a developing country. Indonesia's economy is increasing . this is because the support of Information and tecnology development. The Bank world in Indonesia is good enough. This might make crime is getting bigger. Social Engineering is a cyber crime. The threat of cyber crime influences the weakness of information security, especially in Bank world. The real cyber crime are the piercing of Credit Card, data robbing by the employee inside the company. E.B Taylor said that the succeptibility can be penetrated by social engineering through habbit, the science of information security, trust and pressure. Artha Graha Int'l Bank is very good in responding dan facing one of the cyber crime methods which is social engineering threat. The effectivity can run well if parts involved in the process can run their parts well. This thesis has purposes to analise the effectivity and the application operational procedure and employee's habbit for the information security in facing the danger of social engineering. This research use qualitative method with gathering data technique by*

[1]Penulis adalah mahasiswa Pasca Sarjana Program Study Peperangan Asimetris Cohort-4 TA 2016 Fakultas Strategi Petahanan Universitas Pertahanan.
[2]Dosen FSP, Universitas Pertahanan, pujowidodo78@gmail.com.
[3]Wakil Rektor III, Universitas Pertahanan, dadang.gunawan@idu.ac.id.

interview, observations, library research and document study. The result of the research is that by applying the right standardized operational procedure, self belonging, the use of demand letter and the use of emails to all employees about the informational security continually. So that Artha Graha Bank can avoid social engineering threat. The effectivityof information security in facing social engineering can be done. The Bank security can be well kept nationally and internationally.
***Keywords**: Information Security, social engineering, standardized opeartional Procedure, effectivity*

Pendahuluan

Pembukaan Undang-Undang Dasar 1945 merupakan pokok atau kaedah yang fundamental, mempunyai kedudukan yang tepat dan melekat Perusahaan Negara Republik Indonesia. Hal ini karena setiap alinea yang terdapat dalam Pembukaan UUD tercantum tujuan dan prinsip dasar yang hendak dicapai oleh bangsa negara Indonesia. Salah satu tujuan bangsa yang terkandung dalam pembukaan UUD adalah tujuan keamanan nasional, yaitu untuk melindungi segenap bangsa Indonesia, seluruh tumpah darah Indonesia[4].

Tercantum juga dalam pasal 30 UUD 1945 mengenai usaha pertahanan dan keamanan yang dilakukan oleh Negara dijalankan dengan menggunakan sistem pertahanan dan keamanan rakyat secara keseluruhan oleh TNI dan POLRI sebagai kekuatan yang utama, dan rakyat sebagai kekuatan pendukung. Keamanan nasional ini tidak berhenti hanya pada keamanan negara, namun juga keamanan seperti keamanan masyarakat dan keamanan individu atau insani (human security)[5]. Buzan menyebutkan bahwa keamanan individu mencakup keamanan dalam bidang pangan, kesehatan, lingkungan, pribadi, komunitas dan politik[6].

Seiring dengan perkembangan zaman dan teknologi, bentuk ancaman dalam menghadapi keamanan nasional akan berubah. Kini ancaman dapat pula terjadi di dunia virtual. Cyber crime atau kejahatan di dunia siber. Beberapa kasus cyber crime diantaranya adalah kejahatan yang dilakukan oleh kelompok teroris memelalui media internet. Beberapa situs yang dianggap radikal yang disebarkan melalui propaganda radikalisme melalui media internet terbukti mengganggu keamanan nasional[7].

[4] Subekti, V. S. (2015). Dinamika Konsolidasi Demokrasi: Dari Ide Pembaharuan Sistem Politik hingga ke Praktik Pemerintahan Demokratis . Jakarta: Yayasan Pustaka Obor Indonesia.

[5] Muradi. (2013). Penataan Kebijakan Keamanan Nasional. Bandung: Penerbit Dian Cipta.

[6] Buzan, B. (2000). Human Security: What It Means, and What It Entails. Kuala Lumpur: the 14st Asia Pasific Roundtable on Confidence uliding and Conflict Resolution.

[7] Siagian, B. D. (2016). Analisis Wacana Radikalisme pada Situs Online di Indonesia dalam Perspektif Keamanan Nasional(Tesis). Bogor: Program StudiPeperanganAsimetrisUniversitasPertahanan.

Kasus lain dari kejahatan cyber adalah kejahatan dalam bentuk Social Engineering. Seperti yang dilakukan oleh Edward Snowden, seorang pegawai NSA, yang mencuri data dan membocorkannya,dengan menggunakan penyadapan yang dilakukan oleh NSA. Kasus Social Engineering terjadi pertama kali diluar negeri dilakukan oleh Kevin Mitnick. Kevin Mitnick adalah seorang pria amerika serikat yang di tahan di tahun 1995. Mitnick tercatat sebagai salah seorang hacker yang dalam mencari mangsanya hampir tidak menggunakan komputer dalam mengeksploitasi kelemahan targetnya. dimana sebagian besar melakukan teknik Social Engineering[8].

Kevin Mitnick telah menyatakan bahwa Social Engineering adalah Bagian yang sederhana dalam pendekatannya. Bila rata-rata orang ingin melukisan bagaimana rupa hacker. Mitnick menyatakan dalam bukunya The Art of Deception. Adalah para pelaku Social Engineering merupakan hacker dengan keterampilan teknis tetapi ia memiliki keterampilan sosialisasi yang benar dan memanfaatkannya dalam memanipulasi orang, sehingga cara ini memungkinkan hacker untuk berbicara seperti biasa untuk mendapatkan data yang dinginkan dalam secara tidak logis.

Adapun kasus perbankan dalam negeri yang dilakukan oleh Steven Haryanto, membuat duplikasi situs asli tapi palsu di Bank BCA melalui internet BCA, dan berharap agar nasabah masuk dalam situsnya terlihat nomor identitasnya dan nomor identiffikasi nasabah. Dan ternyata terdapat 130 nasabah yang terperangkap oleh jebakannya. Sebagai contoh alamat palsu tersebut adalah : kilkbca.com, klikbac.com

Kemudahan dalam memperoleh informasi tersebut merupakan faktor kerentanan yang disebebkan oleh kelalaian manusia. Akibat dari kelalaian tersebut banyak perusahaan atau instansi yang dirugikan. Kerugian itu adalah hilangnya data informasi rahasia atau pencurian data yang memang harus di jaga. Purba Kuncara menyatakan bahwa rantai terlemah dalam sistem jaringan komputer adalah manusia.

Pada kegiatan kerja sehari-hari budaya kerja karyaawan masih tergolong kurang dalam disiplin kerjan, pengetahuan tentang pentingnya keamanan informasi, mudah percaya

[8]Azis,(2015); cybercrime-dan-social-engineering, http://fahmirahmatazis.co.id/2015/09/cybercrime-dan-social-engineering.

kepada teman kerja dengan memberikan informasi dan masih adanya penekanan yang dilakukan oleh pejabat yang lebih tinggi jabatannya dan ini sangat rentan sekali dalam menjaga kerahasiaan informasi yang dapat digunakan oleh pelaku social engineering. Perilaku yang kurang baik ini dapat dimanfaatkan oleh pelaku social engineering. Misalnya user menggunakan password yang mudah untuk dibobol, selanjutnya user tersebut tidak ingat untuk melakukan proses logout ketika meninggalkan ruang kerja. Hal tersebut akan memperbesar peluang pelaku Social Engineering untuk melakukan hal-hal yang illegal seperti mencuri informasi yang tidak seharusnya diketahui olehnya. Dalam artikel Indrajit[9] menjelaskan bahwa sesuai dengan prinsip keamanan informasi data yang harus diperhatikan adalah melalui aspek-aspek sebagai berikut :

a. Kerahasiaan (Confidentiality), bahwa menjamin kerahasiaan akan data dan atau informasi, menyatakan bahwa informasi hanya dapat diakses oleh pihak yang berhak atau pihak yang berwenang dalam menjamin kerahasiaan data yang akan dikirim, diterima dan disimpan.

b. Keutuhan (Integrity), bahwa melindungi keakuratan dan kelengkapan informasi, dapat menjamin bahwa data tidak dapat diubah tanpa ijin dari pihak yang berwenang, dalam menjaga keakurasian dan keutuhan informasi tersebut.

c. Ketersediaan (Availability), bahwa informasi akan tersedia pada saat dibutuhkan. (idsirti.or.id).

Dalam buku Primitive Culture, EB Taylor[10] mendeskripsikan mengenai beberapa hal yang mempengaruhi terjadinya Social Engineering antara lain adalah kebiasaan atau budaya, pengetahuan (knowledge), kepercayaan (trust), dan ketakutan atau penekanan. Dari empat prinsip dasar inilah korban ditampilkan dan mendukung pada keinginan dari seseorang yang berniat jahat dengan memanfaatkan kelemahan sosial pada manusia umumnya. Berdasarkan uraian fakta-fakta diatas, Social Engineering merupakan salah satu metode di dalam peperangan asimetris. Hal ini dapat dibuktikan dengan adanya subjek yang lemah yaitu individu atau kelompok dan yang kuat yaitu sebuah perusahaan besar yang memiliki informasi

[9] Indrajit,(2015), Social Engineering Masih Menjadi Ancaman

[10] Primitive Culture, EB Taylor https://en.wikipedia.org/wiki/Edward_Burnett_Tylor

rahasia. Social Engineering juga merupakan salah satu cara dalam melakukan kejahatan cyber, karena hal ini berkaitan dengan penerobosan pintu-pintu keamanan melalui sistem komputasi.

Ancaman kejahatan cyber saat ini sangat mempengaruhi kerentanan keamanan informasi. Berhubungan dengan keamanan infomasi, salah satu sektor yang kerap kali menjadi sasaran pencurian informasi yang bersifat rahasia ialah sektor perbankan. Maka dari itu, Peneliti berpendapat bahwa hal ini dapat berakibat fatal apabila tidak di respon secara baik dan cepat. Dalam hal ini peneliti ingin meneliti sejauh mana Perusahaan dalam merespon dan menghadapi salah satu metode kejahatan cyber yaitu ancaman *Social Engineering*. Dengan demikian, Peneliti hendak melakukan penelitian dengan judul Efektivitas Keamanan Informasi Dalam Menghadapi Ancaman *Sosial Engineering*.

Metodologi

Dalam penelitian ini akan digunakan metode kualitatif. Penelitian ini akan dilakukan dengan menggunakan wawancara dengan beberapa narasumber yaitu para pakar telematika, khususnya di bidang keamanan informasi, para pejabat perusahaan dan karyawan.[11]

Hasil dan Pembahasan

Keamanan Informasi Perusahaan Berdasarkan Teori Whiteman dan Mattord

Sebelum berbicara mengenai keefektivitasan keamanan informasi dalam menghadapi ancaman Social Engineering, peneliti hendak menyelaraskan hasil analisis data dengan salah satu teori yang berisikan komponen-komponen dalam keamanan informasi. Berikut ini ialah teori yang dikemukakan oleh Whitman dan Mattord[12], yang dapat melihat tingkat efektivitas keamanan informasi pada perusahaan yang didasarkan pada komponen-komponen sebagai berikut:

a. Personal Security, menyangkut keamanan karyawan dalam konteks upaya pengamanan informasi.

Perusahaan dalam hal ini telah melakukan upaya dalam menghindarkan karyawannya dari modus-modus Social Engineering melalui berbagai cara, termasuk juga dengan dibentuknya

[11] Sugiyono (2016), Metode Penelitian Kuantitatif, Kualitatif dan R & D, Bandung, Penerbit ALFABETA, CV Berbagai Sumber Daya Bagi Pertumbuhan Berkelanjutan, Jakarta

[12] Whitman, Michael E, dan Mattord, Herbert J (2012), Principles of Information Security (4th ed). Boston, MA, USA Course Technologi.

Standard Operasional Prosedur hingga pengiriman himbauan mengenai keamanan informasi melalui e-mail blast. Pelatihan-pelatihan mengenai kesadaran akan pentingnya menjaga keamanan informasi pun dilakukan perusahaan, baik pada saat proses penyeleksian calon karyawan hingga pada masa kerjanya berlangsung.

b. Operation Security, yang menitikberatkan kepada strategi dalam mengamankan kemampuan organisasi dalam upayanya untuk menjaga keamanan informasi.

Manajemen perusahaan selalu melakukan peningkatan kemampuan organisasinya dalam menjaga keamanan informasi, salah satunya dengan cara peninjauan kembali Standar Operasional Prosedur yang telah diolah oleh manajemen perusahaan mengingat bahwa Standar Operasional Prosedur tersebut tidak sempurna, melainkan selalu ada celah-celah yang berpotensi menyebabkan kebocoran informasi. Maka manajemen perusahaan selalu melakukan peninjauan ulang dalam menghadapi Standar Operasional Prosedur dengan tetap menyelaraskan aturan-aturan utama yang tercantum pada peraturan yang telah ditetapkan.

c. Communication Security, memiliki tujuan untuk mengamankan media komunikasi, teknologi komunikasi, serta kemampuan untuk memanfaatkan alat komunikasi terkait menjaga keamanan informasi.

Perusahaan telah menerapkan komponen ini dengan melakukan kebijakan berkenaan dengan sharing informasi yang harus selalu dilaksanakan secara tertulis dalam proses perizinannya. Segala upaya dalam mengakses informasi melalui jaringan telekomunikasi baik yang berbasis kabel maupun nirkabel tidak diperbolehkan. Penggunaan teknologi seperti pengiriman data melalui public e-mail ataupun pesan singkat pun tidak diperkenankan. Ketentuan ini berlaku tidak hanya untuk karyawan, tetapi juga untuk para pejabat-pejabat di perusahaan yang memiliki posisi yang lebih tinggi daripada karyawan biasa.

d. Network Security, yang menitikberatkan kepada pengamanan peralatan jaringan data perusahaan, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam upaya menjaga keamanan informasi.

Berkaitan dengan keamanan jaringan, Divisi Teknologi perusahaan telah menerapkan sistem HTTPS dalam

penggunaan Internet, dengan demikian HTTPS akan menjamin bahwa situs yang dikunjungi ialah situs resmi milik perusahaan. Selain itu, dalam upaya pengamanan informasi, dalam melakukan transfer data, perusahaan juga telah melakukan metode SFTP. SFTP akan melakukan enkripsi pada saat dilakukannya pemindahan data, sehingga data tersebut terkunci pada kode enkripsi yang hanya mampu dipecahkan oleh orang yang memiliki otoritas,

Berdasarkan uraian dari pembahasan diatas, dapat Peneliti simpulkan bahwa teori tersebut memiliki persamaan dengan persyaratan dari ISO/IEC 27001. Perbedaannya hanya mengenai spesifikasi dari syarat-syarat keamanan informasi. Pada teori Whitman dan Mattord, hanya dideskripsikan sebanyak 4 komponen dalam keamanan informasi, yang mana pada syarat ISO/IEC 27001 memecah ke-4 komponen tersebut menjadi lebih spesifik. Dengan demikian, tidak ditemukan suatu celah pada manajemen perusahaan terkait dengan komponen atau syarat-syarat yang belum terpenuhi berdasarkan teori dan persyaratan standar internasional tersebut.

Berdasarkan teori efektivitas yang dikemukakan oleh Duncan, suatu efektivitas akan terjadi dengan baik apabila karyawan beserta pimpinannya bisa saling terbuka dalam menginterpretasikan pesan dari pimpinan kepada karyawannya, serta keduanya dapat menjalin hubungan dengan baik. Ketika hubungan keduanya telah berjalan dengan baik serta terjadi keterbukaan yang berkesinambungan, maka pekerjaan pun akan berjalan dengan baik.

Dari hasil analisis data yang telah dilakukan, Peneliti beranggapan bahwa sejauh ini, efektivitas perusahaan dalam menjaga keamanan informasi dinilai sudah cukup efektif. Hal itu dapat dilihat dari upaya manajemen teknologi perusahaan dalam mempersulit user untuk dapat menembus pengamanan yang berlapis. Pertama, pada situs perusahaan, manajemennya telah menggunakan sistem HTTPS, dimana berfungsi untuk memastikan kepada peramban dan pengguna bahwa keduanya sedang berada di perusahaan yang sesungguhnya.

Jika bertolak ke belakang, pernah terjadi suatu kejadian Social Engineering yang dialami oleh perusahaan lain karena situsnya belum menggunakan sistem HTTPS, melainkan masih menggunakan HTTP. Akhirnya, terdapat oknum yang membuat situs yang serupa dengan

perbedaan yang sangat tidak mencolok. Perbedaan tersebut terletak dari tata letak huruf nama situs. Kejadian tersebut memakan korban yang tidak sedikit, sehingga oknum tidak hanya dapat mengakses informasi-informasi rahasia milik perusahaan melainkan dapat melakukan pencurian data.

Kedua, metode pemindahan data secara komputerisasi pun telah beralih dari FTP menjadi SFTP. Melalui protokol SFTP, maka pada saat informasi rahasia dipindahkan dari satu tempat ke tempat lainnya, data tersebut akan terenkripsi sehingga tidak dapat diakses tanpa kode atau password yang dimiliki oleh orang-orang yang memiliki otoritas. Enkripsi data ini lah yang membuat informasi rahasia tersebut tetap aman dari para pelaku rekayasa sosial. Ketiga, perusahaan berupaya dalam menjaga keamanan informasinya melalui kebijakan-kebijakan yang dikeluarkan oleh manajemen perusahaan dalam bentuk Standar Operasional Prosedur, juklak, pedoman, memo hingga e-mail blast yang ditujukan untuk seluruh karyawannya.

Dalam teori efektivitas, terdapat tiga indikator yang bisa dijadikan sebagai alat ukur efektivitas suatu pekerjaan. Pertama di lihat dari indikator pencapaian tujuan. Berdasarkan indikator ini, Peneliti menemukan bahwa perusahaan telah melakukan siklus Plan-Do-Check-Act (PDCA) yang merupakan aturan main dari SNI ISO/IEC 27001 tentang SMKI. Perusahaan melakukan pengamanan informasi melalui tahap-tahap perencanaan, pelaksanaan, penilaian serta penindakan. Perusahaan melakukan tahap perencanaan dengan cara mengumpulkan masing-masing kepala divisi dan kepala Bagian untuk merumuskan suatu pedoman, Standar Operasional Prosedur, maupun surat edaran terkait dengan keamanan informasi secara sempit, dan terkait dengan penyelarasan visi dan misi dari perusahaan itu sendiri secara luas.

Tahap pelaksanaan dilakukan dengan cara melakukan pengamanan informasi perbankan yang diemban oleh Bagian Keamanan Teknologi Informasi dari Divisi Teknologi. Divisi Teknologi mengemban tanggung jawab untuk mengamankan informasi data dari kejahatan cyber, khususnya Social Engineering. Pada tahap penilaian, akan dilakukan suatu perbandingan antara kebijakan-kebijakan tertulis dengan aksi di lapangan. Proses penilaian ini akan dilakukan oleh Bagian Audit yang melakukan pemastian kualitas.

Di lihat dari indikator adaptasi, yaitu mengenai penyesuaian perilaku karyawan dalam menghadapi sosialisasi serta awareness keamanan informasi. Pada dasarnya, disinilah letak kendala yang ditemukan oleh Peneliti, dimana masih terdapat beberapa pelanggaran dalam menghadapi clean desk policy. Berdasarkan analisis data yang sudah Peneliti lakukan, aspek adaptasi ini sangat berkaitan erat dengan perilaku karyawan dalam menghadapi keamanan informasi. Berdasarkan pernyataan yang berasal dari National Institute of Standards and Technology (NIST) Special Publication (SP) 800-50 mendeskripsikan bahwa manusia adalah kunci dari keamanan informasi. Dengan demikian diperlukan adanya perhatian khusus bagaimana manusia untuk membangun kesadaran mengenai urgensi keamanan informasi.

Peneliti simpulkan bahwa untuk menjaga keamanan informasi dalam menghadapi ancaman Social Engineering, perusahaan dinilai telah cukup efektif, terutama pada indikator pencapaian tujuan serta integrasi. Manajemen perusahaan telah membuat berbagai kebijakan yang cukup variatif dalam menghadapi para karyawannya sehingga upaya pengamanan tidak hanya dilakukan secara satu arah, melainkan dua arah. Sosialisasi melalui Pusdiklat perusahaan merupakan salah satu contoh utama dari upaya pengamanan informasi secara dua arah.

Dari keseluruhan pembahasan yang telah diuraikan, dapat diambil benang merahnya bahwa terkait dengan keamanan informasi, tergantung pada 3 aspek CIA. Pemenuhan dalam menghadapi ketiga aspek tersebut dapat di breakdown melalui beberapa alat ukur, yaitu melalui standar internasional ISO/IEC 27001, Teori Keamanan Informasi Whitman & Mattord, serta Teori Efektivitas Duncan. Berdasarkan ketiga alat ukur tersebut, perusahaan telah memenuhi seluruh komponen-komponennya sehingga ketiga aspek dasar dari Confidentialy,Integrity Availebility sudah terpenuhi. Walaupun demikian, suatu sistem tidak ada yang sempurna, sehingga walaupun komponen-komponen tersebut sudah terpenuhi, pasti akan terdapat sedikit celah yang kemungkinan besar berasal dari faktor manusia mengingat bahwa manusia lah faktor yang terkuat sekaligus yang terlemah terkait keamanan informasi ini.

Hakikat Manusia Sebagai Korban *Social Engineering*

Sebelum berbicara mengenai ancaman Social Engineering, ada baiknya jika kita memahami terlebih dahulu mengenai hakikat manusia sebagai makhluk sosial. Berdasarkan teori budaya, manusia pada dasarnya merupakan makhluk budaya yang memiliki akal, budi dan daya untuk mendapatkan suatu gagasan dan karya cipta yang berupa seni, moral, hukum, dan kepercayaan yang dilakukan secara terus menerus yang pada akhirnya membentuk suatu kebiasaan yang kemudian diakumulasikan dan disampaikan secara sosial atau kemasyarakatan.

Manusia sebagai pencipta kebudayaan memiliki kemampuan daya yaitu akal, intelegensia, dan intuisi, perasaan dan emosi, kemauan, fantasi dan perilaku. EB Taylor mendeskripsikan beberapa faktor dari manusia yang dapat mempermudah para pelaku Social Engineering untuk melakukan aksinya:

a. Kebiasaan atau Budaya

Dalam konteks Social Engineering, sudah menjadi kebiasaan bagi manusia, khususnya di Indonesia untuk memiliki rasa saling tolong menolong dalam menghadapi sesama. Budaya gotong royong pun telah mendarah daging bagi masyarakat Indonesia. Seringkali seseorang tidak segan untuk memberikan pertolongan kepada orang lain yang baru dikenalnya. Hal ini yang menurut Peneliti, terkadang dapat dijadikan celah bagi pelaku Social Engineering untuk mendapatkan sesuatu yang diinginkannya.

b. Pengetahuan

Tingkat wawasan ilmu pengetahuan seseorang tentu berbeda satu sama lainnya. Terkadang, sesorang pegawai tidak mengetahui tingkat kerahasiaan suatu informasi, atau tidak mengetahui modus-modus dari pelaku Social Engineering, sehingga ia akan mudah terjebak oleh pelaku. Rendahnya tingkat pengetahuan tersebut juga memberikan peluang yang besar bagi pelaku untuk mendapatkan apa yang diinginkannya.

c. Kepercayaan

Faktor kepercayaan merupakan faktor yang memberikan resiko besar dalam menghadapiseseorang untuk masuk ke dalam perangkap Social Engineering. Seseorang terkadang akan memberikan suatu informasi rahasia kepada orang lain atas dasar kepercayaan bahwa orang tersebut tidak akan menyalahgunakan atau pun menyebarkan informasi yang bersifat rahasia. Atas dasar kepercayaan pula, seseorang akan bersikap lengah dan

tidak waspada dengan lingkungan sekitarnya. Hal ini juga memberikan celah bagi pelaku Social Engineering untuk menjalankan modus-modusnya.

d. Ketakutan atau Penekanan (Fear)

Semua manusia memiliki rasa takut dalam menghadapiancaman atau tekanan dalam menghadapiberbagai hal. Rasa takut ini lah yang bisa dimanfaatkan oleh pelaku Social Engineering. Melalui cara-cara yang menakuti seperti ancaman ataupun gertakan, maka manusia akan mudah untuk membocorkan informasi yang diketahuinya demi melindungi dirinya dari rasa takut tersebut.

Berdasarkan keempat faktor diatas, dapat disimpulkan bahwa manusia sebagai makhluk yang memiliki akal, inteligensia dan intuisi, perasaan dan emosi, fantasi dan perilaku, dapat menjadi objek yang sangat rentan dalam menghadapiSocial Engineering. Keempat faktor tersebutlah yang memberikan peluang kepada para pelaku Social Engineering, sehingga seseorang akan menjadi lengah dan tidak sadar bahwa ia telah memasuki jebakan dari pelaku Social Engineering.

Menurut Amanda Andreas, terdapat tiga hal yang dijadikan sebagai komponen utama dari keamanan informasi. Komponen yang pertama ialah manusia. Manusia merupakan sebuah sistem yang dikuasai oleh manusia itu sendiri. Tetapi, dalam sebuah jaringan, keamanan manusia merupakan Bagian yang paling lemah dalam sistem. Dalam konteks keamanan informasi, manusia lah faktor yang paling krusial yang harus diperhatikan. Komponen kedua ialah proses yang merupakan sekumpulan sistem keamanan yang dibuat berdasarkan dokumen resmi perusahaan seperti standar operasional prosedur, surat edaran, maupun petunjuk pelaksana atau kebijakan-kebijakan perusahaan lainnya. Kebijakan ini lah yang merupakan salah satu pondasi bagi terjaganya keamanan informasi.

Sasaran utama dari Social Engineering adalah dengan memperoleh akses yang illegal ke sistem dan/atau informasi untuk melakukan suatu penipuan ataupun kecurangan melalui sarana manusia. Selain itu, penyusupan ke dalam jaringan, pencurian identitas dan juga pencurian infomasi data rahasia, juga merupakan sederetan target dari pelaku Social Engineering.

Menurut Supradono (2009), keamanan informasi tidak hanya bisa disandarkan pada teknologi keamanan informasi saja, tetapi harus ada pemahaman yang dilakukan oleh

organisasi atau perusahaan agar dapat menangani masalah secara tepat dalam memenuhi kebutuhan keamanan informasi. Dengan demikan, dibutuhkan pengelolaan yang komprehensif mengenai keamanan informasi, keamanan informasi harus memperhatikan tiga aspek, yaitu Confidentially, Integrity, dan Availability (CIA).[13]

Dalam pemenuhan aspek CIA, perusahaan telah menerapkan dua bentuk konkrit mengenai pemenuhan aspek ini, yaitu mengenai penerapan dalam bentuk non-operasional atau administratif yang berisi berbagai kebijakan tertulis yang berupa pedoman, prosedur, surat edaran maupun memo. Bentuk kedua yaitu melalui penerapan dalam bentuk operasional dengan mengadakan program sharing ilmu pengetahuan serta sosialiasasi, himbauan dengan melalui e-mail blast.

Salah satu dari implementasi kebijakan tersebut adalah dengan diterapkannya "clean desk policy" yang mengatur karyawan agar tidak meninggalkan catatan-catatan penting di meja kerja, tidak memasang password pada komputernya, tidak mematikan komputer saat hendak ditinggal untuk suatu keperluan tertentu, dan harus selalu mengunci setiap laci yang ada di meja kerja masing-masing karyawan. Kebiasaan karyawan dalam membiarkan catatan-catatan kecil yang di temple pada layar monitor, serta membiarkan dokumen-dokumen berserakan di atas meja masih belum bisa ditinggalkan sehingga dapat meningkatkan faktor kerentanan dalam menghadapi keamanan informasi dan memperbesar peluang user untuk melakukan rekayasa sosial dalam menghadapi karyawan tersebut.

Situasi Keamanan Informasi Perusahaan dalam menghadapi Metode Social Enginnering

Terakhir, Peneliti akan melakukan pembandingan antara upaya-upaya yang dilakukan oleh perusahaan dalam menjaga keamanan informasi melalui sudut pandang ancaman Social Engineering dengan cara-cara yang dapat dilakukan oleh pelaku Social Engineering untuk mendapatkan informasi secara illegal. Metode Social Engineering menurut Mawarna[14] ada empat yaitu yang pertama ialah Social Engineering by

[13] Kennetth C. Laudon, Jane p. Laudon . Sistem Informasi Manajemen 1, Jakarta , Penerbit Salemba Empat

[14] Marwana (2012), Teknik Social Engineering Dan Pencegahannya.

Phone. Metode ini menggunakan sarana telepon sebagai sarana utamanya dalam melakukan aksi Social Engineering. Biasanya pelaku akan berpura-pura untuk menelepon dari dalam perusahaan dengan menggunakan interkom untuk mendapatkan suatu informasi. Hal ini tidak akan terjadi di perusahaan, telah menerapkan kebijakan mengenai sharing informasi yang hanya melalui surat dan berdasarkan kewenangan dari pihak yang memiliki otoritas. Sehingga, kemungkinan bagi pelaku Social Engineering dalam mendapatkan informasi melalui saluran telepon sangat kecil.

Metode yang kedua ialah Dumpster Diving. Dumpster Diving dilakukan dengan cara 'mengacak-acak tong sampah'. Tong sampah disini ialah dalam artian bahwa pelaku bisa mendapatkan informasi melalui buku telepon perusahaan, bagan organisasi yang sudah tidak terpakai, memo yang dibuang secara sembarangan, petunjuk kebijakan perusaahan, jadwal pertemuan, nama login dan password, hingga segala informasi yang tertulis pada post-it note di layar komputer serta hardware yang sudah usang. Dalam mencegah pelaku untuk melakukan metode ini, maka perusahaan menerapkan kebijakan "clean desk policy" dimana seluruh karyawan diwajibkan untuk memusnahkan segala catatan-catatan yang sudah tidak berguna, dilarang untuk menempelkan post-it note yang berisikan password ataupun nomor rekening nasabah hingga penguncian meja kantor untuk menghindari tindakan pencurian dokumen-dokumen penting.

Metode yang ketiga ialah Social Engineering Online. Peneliti berpendapat bahwa metode ini bukan merupakan metode yang tepat untuk menyerang karyawan. Menurut Peneliti, metode ini akan lebih menguntungkan jika dilakukan kepada karyawan perusahaan. Namun, tidak menutup kemungkinan juga bahwa karyawan perusahaan bisa terjebak pada metode ini karena tidak adanya kesadaran mengenai pentingnya membedakan password masing-masing akun atau perangkat keras demi menjaga keamanan informasi. Urgensi mengenai pentingnya perbedaan password dan mengganti password secara berkala pun sudah dilakukan oleh perusahaan melalui himbauan e-mail blast kepada seluruh jajaran karyawan.

Metode yang keempat ialah Social Engineering dari sudut pandang psikologis. Metode ini menggunakan teknik persuasif, seperti menyamar seperti orang yang memiliki kewenangan

atas suatu informasi. Selain itu, cara ini juga memanfaatkan kondisi pertemanan dalam memperoleh sebuah informasi. Pertemanan yang dimaksud adalah menjalin hubungan yang seolah-olah baik dengan seseorang.

Maka untuk menghadapi metode seperti itu, perusahaan telah melakukan berbagai pelatihan-pelatihan untuk meningkatkan profesionalitas dan kinerja para karyawannya. Di dalam dunia pekerjaan, manajemen perusahaan terutama dari divisi sumber daya manusia selalu menekankan mengenai profesionalitas, dimana di dalam lingkungan pekerjaan hanya ada istilah rekan kerja. Maksud dari pernyataan tersebut ialah, rekan kerja memiliki makna pertemanan hanya dalam ruang lingkup pekerjaan yang mengutamakan profesionalitas.

Metode yang terakhir ialah Reverse Social Engineering, serupa dengan metode Social Engineering dari sudut pandang psikologis, yang membedakan ialah metode ini memiliki 3 alur yang identik, yaitu:

a. Sabotase, sebelum melancarkan aksinya, pelaku harus melakukan sabotase dalam menghadapijaringan yang berhubungan dengan pengamanan suatu informasi.
b. Penawaran, pelaku akan berpura-pura sebagai teknisi yang mampu untuk menyelesaikan akibat dari sabotase tersebut kepada perusahaan.
c. Bantuan, pelaku akan meminta bantuan kepada karyawan untuk menanyakan sesuatu yang berkaitan dengan sabotase tersebut sampai ia mendapatkan informasi yang diinginkan.

Berdasarkan 3 alur tersebut, Peneliti berpendapat bahwa untuk melakukan alur tersebut dibutuhkan kemampuan yang jauh diatas normal, dan hanya bisa dilakukan oleh orang-orang yang professional. Untuk melakukan sabotase, pelaku harus mempelajari seluk beluk jaringan sistem informasi perusahaan, yang mungkin informasi itu baru bisa didapatkan melalui karyawan maupun mantan karyawan. Pada kasus demikian, sense of belonging dari karyawan serta treatement perusahaan dalam menghadapi karyawan diuji. Berdasarkan pernyataan Kepala Divisi sumber daya manusia, suatu kebocoran informasi tidak akan terjadi apabila terdapat sense of belonging dari karyawan dalam menghadapi perusahaan yang tentu saja diciptakan melalui treatement yang diberikan oleh perusahaan kepada karyawan.

Berdasarkan uraian di atas, Peneliti menyimpulkan bahwa pernyataan mengenai manusia merupakan faktor yang terlemah sekaligus terkuat menjadi semakin tidak terbantahkan. Manusia merupakan faktor yang paling penting dalam menjaga keamanan informasi. Maka dari itu, perusahaan harus menerapkan standar operasional prosedur serta memberikan pelatihan-pelatihan kepada karyawannya untuk menumbuhkan kesadaran akan keamanan informasi. Dengan adanya kesadaran akan keamanan informasi, ditambah dengan sense of belonging dalam menghadapi perusahaan, Peneliti berpendapat bahwa karyawan tersebut akan menjadi karyawan yang professional dan loyal kepada perusahaannya. Melalui profesionalitas dalam bekerja, serta sense of belonging yang kuat akan semakin memperkecil ancaman Social Engineering.

Kesimpulan

Melalui teori efektivitas, teori keamanan informasi dan syarat dari ISO/IEC 27001, Peneliti menilai bahwa Perusahaan telah memenuhi seluruh komponen dari teori-teori dan syarat tersebut. Hal itu tercermin mulai dari pelaksanaan Standar Operasional Prosedur hingga pengadaan pelatihan-pelatihan juga menunjukkan keefektivitasan upaya pengamanan informasi perbankan.

Walaupun demikian, pada observasi yang telah dilakukan, masih terdapat pelanggaran, terutama berkaitan dengan clean desk policy dimana masih ditemukannya post-it notes pada layar komputer. Hal ini menunjukkan bahwa karyawan masih ada yang belum menyadari mengenai pentingnya menjaga keamanan informasi. Maka, Peneliti meyimpulkan bahwa tingkat efektivitas keamanan informasi perusahaan dilihat dari upaya manajemen sudah dinilai cukup efektif. Sedangkan efektivitas pada tingkat karyawan dalam pengaplikasian pengamanan informasi dinilai masih dalam penyempurnaan yang lebih baik lagi.

Pada teori EB Taylor mendeskripsikan mengenai beberapa hal yang mempengaruhi terjadinya Social Engineering antara lain adalah kebiasaan atau budaya, pengetahuan (knowledge), kepercayaan (trust), dan ketakutan atau penekanan tidak bisa diterapkan oleh kejahatan social engineering karena teknologi sistem keamanan yang cukup baik yaitu dengan menerapkan clean desk policy , permintaan data dengan menggunakan surat dan email blast

mengenai peringatan tenttang keamanan informasi..

Manusia merupakan faktor yang paling penting sekaligus yang paling lemah dalam konteks keamanan informasi perbankan. Manusia merupakan faktor yang paling kuat karena manusialah yang bertugas untuk melakukan kegiatan perusahaan serta melakukan pengamanan informasi. Manusia sebagai faktor yang paling lemah, di lihat dari aspek psikologis, dimana manusia akan sangat rentan untuk menjadi korban dari serangan Social Engineering yang akan mengakibatkan kebocoran informasi yang seharusnya dijaga.

Dalam hal ini, seluruh jajaran Kepala Divisi, mulai dari Kepala Divisi Teknologi hingga Sumber Daya Manusia, memiliki arah pemikiran yang sama yaitu mengenai pemberdayaan manusia dalam mengamankan informasi perbankan sehingga tidak akan menjadi korban dari Social Engineering. Hal ini telah terbukti dengan rutinnya diadakan pelatihan-pelatihan mengenai information security awareness, hingga pengiriman e-mail blast yang berisikan himbauan mengenai tata cara melakukan pengamanan informasi secara sederhana.

Daftar Pustaka

Buku

Buzan, B. (2000). Human Security: What It Means, and What It Entails. Kuala Lumpur: the 14st Asia Pasific Roundtable on Confidence uliding and Conflict Resolution.

Golose, P. R. (2015). Invasi Terorisme ke Cyberspace. Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian.

Muradi. (2013). Penataan Kebijakan Keamanan Nasional. Bandung: Penerbit Dian Cipta.

Christopher Hadnagy (2010). Social Engineering. The Art of Homan Hacking. Indianapolis, Indiana. Wiley Publishing, inc

Departemen Pertahanan Republik Indonesia (2008) Buku Putih Pertahanan Republik Indonesia 2008

Departemen Pertahanan Republik Indonesia (2015) Buku Putih Pertahanan Republik Indonesia 2015

Mary Kaldor (2007). Human Security : Reflections on Globalization and Intervention. Cambridge, UK Copyright

Idrus Muhammad (2009). Metode Ilmu Penelitian Ilmu Sosial : Pendekatan Kualitatif dan Kuantitatif. Yogjakarta, Penerbit Erlangga

Sugiyono (2016), Metode Penelitian Kuantitatif, Kualitatif dan R & D, Bandung, Penerbit ALFABETA, CV Berbagai Sumber Daya Bagi Pertumbuhan Berkelanjutan, Jakarta

Kennetth C. Laudon, Jane p. Laudon . Sistem Informasi Manajemen 1, Jakarta , Penerbit Salemba Empat

Jurnal

Granger, Sarah., Social Engineering Fundamentals, Part I: Hacker Tactics. Symantec

Lucky Adhie, 2010, Identity Thet dengan menggunakan Social Engineering Studi Kasus: Kartu Kredit di indonesia.

Peltier, T.R., 2001, Information Security Risk Analysis, Auerbach Publications.

Papadaki, Maria, Furnell, Steven dan Dodge, Ronald C., Social Engineering – Exploiting the Weakest Links. s.l. : European Network and Information Security Agency, 2008

Rhodes, Colleen., Safeguarding Against Social Engineering. East Carolina : s.n., 2006.

Siagian, B. D. (2016). Analisis Wacana Radikalisme pada Situs Online di Indonesia dalam Perspektif Keamanan Nasional(Tesis). Bogor: Program StudiPeperanganAsimetrisUniversitasPertahanan.

Solichul Huda , 2007 Pengamanan Sistem Komputer dari Model Social Engineering dengan mengaktifkan program Security Awareness,

Subekti, V. S. (2015). Dinamika Konsolidasi Demokrasi: Dari Ide Pembaharuan Sistem Politik hingga ke Praktik Pemerintahan Demokratis . Jakarta: Yayasan Pustaka Obor Indonesia.

Whitman, Michael E, dan Mattord, Herbert J (2012), Principles of Information Security (4th ed). Boston, MA, USA Course Technologi

Marwana (2012), Teknik Social Engineering Dan Pencegahannya.

Website

Azis,(2015); cybercrime-dan-social-engineering. diakses 30 September, 2016, http://fahmirahmatazis.co.id/2015/09/cybercrime-dan-social-engineering.

Bagus Artiadi Soewardi, Cyber Defence diakses 5 januari 2017. http//www.kemhan.go.id/pothan

Dr. Joel Brenner (2009), National Counterinteligence Executive diakses 5 januari 2017. https://cryptome.org/dni-cbs-24.pdf

Etikakelompok7,(2013) Keamanan Jaringan dan Komputer diakses 30 https://keamananjaringandankomputer/2013/03/22/website-palsu-klik-bca/

Houchins Thomas (2002); Security's Biggest Threats: Social Engineering Your Employees, diakses 5 januari 2017.

https://www.giac.org/paper/gsec/2149/securitys-biggest-threats-social-engineering-employees/

Indrajit,(2015), Social Engineering Masih Menjadi Ancaman, diakses 30 September 2016 http://www.ciso.co.id/2015/03/social-engineering-masih-menjadi-ancaman/).

Institute, Insurance Information., Identity Theft. Consumer Fraud and Identity Theft. Insurance Information Institute, 2009. Diakses : 23 september 2016.] http://www.iii.org/media/facts/statsbyissue/idtheft/.

Indra, D. dan M. Chandrataruna (2009) pencuri data adalah karyawan Huawei (http://teknologi.vivanews.com/news/read/41027. pencuri data adalah karyawan huawei. Diakses 3 oktober 2016.

Nudin,2005 Teori Organisasi 30 September, 2016 http://file.upi.edu SekilasTentang Cyber Crime, Cyber Security ,diakses 30 September, 2016, http://inet.detik.com/read/2015/08/31/sekilas-tentang-cyber-crime-cyber-security-dan-cyber-war

S. Juliandri Simanungkalit 2009, Perancangan Manajemen, 30 September, 2016 http://lib.ui.ac.id/file?file=digital/Perancangan20manajemen-Literatur.pdf.