Analisis Teknik *Social Engineering* Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur

Eristya Maya Safitri[1], Zelda Ameilindra[2], Rina Yulianti[3]

[1,2,3] Sistem Informasi, Universitas Pembangunan Nasional Jawa Timur
[1]maya.si@upnjatim.ac.id
[2]zeldaameilindra@gmail.com
[3]rinayulianti498@gmail.com

***Abstrak*— Di era sekarang ini, informasi merupakan salah satu aset yang berharga bagi sebuah perusahaan, oleh karena sebuah perusahaan akan berusaha untuk melindungi informasi yang mereka miliki. Namun, dinding keamanan sistem informasi yang terkuat sekalipun dapat runtuh jika orang di dalamnya membuat kesalahan yang mengakibatkan adanya celah pada dinding keamanan tersebut. Kesalahan seperti ini biasanya di eksploitasi oleh *attacker* dengan menggunakan social *engineering*. *Social engineering* merupakan suatu metode peretasan (*hacking*) dimana seorang *attacker* melakukan aksinya dengan memanipulasi dan merekayasa sebuah data berupa website, aplikasi atau *software*, file dan lain-lain yang dikirim menggunakan email juga media komunikasi berupa SMS dan telepon. Hal ini bertujuan agar korban tertarik, tertipu dan tidak mencurigai sehingga seorang *attacker* dapat melakukan segala jenis aksinya. Karena itulah pada *paper* ini akan dibahas tentang tipe penyerangan *social engineering* dengan cara menganalisa serta mengumpulkan literatur. Sehingga dapat memberi informasi dan upaya penghindaran kepada orang lain tentang *social engineering* dan ancamannya.**

Kata Kunci*— *Ancaman, Keamanan Sistem Informasi, Social Engineering

I. PENDAHULUAN

Serangan terhadap keamanan sistem informasi (*security attack*) dewasa ini seringkali terjadi. Kejahatan komputer (*cyber crime)* pada dunia maya seringkali dilakukan oleh sekelompok orang yang ingin menembus suatu keamanan sebuah sistem. Aktivitas ini bertujuan untuk mencari, mendapatkan, mengubah, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar-benar dibutuhkan.

Tidak semua pekerjaaan *hacking* (menjebol sistem) murni dilakukan dari balik layar atau hanya fokus mengeksploitasi mesin, karena semakin berkembangnya zaman keamanan komputer juga semakin sulit ditembus. Teknik ini banyak dipakai untuk penyebaran *malware* atau mendapatkan informasi yang diperlukan *hacker,* seperti identitas seseorang.

Social engineering merupakan istilah yang digunakan untuk berbagai tindak kejahatan yang dilakukan dengan memanfaatkan interaksi dengan manusia. Teknik ini menggunakan manipulasi psikologis untuk menipu korban agar mereka melakukan kesalahan keamanan dan memberikan informasi sensitif. *Social engineering* sering digunakan oleh para *hacker* untuk mendapat informasi penting karena mereka memahami bahwa manusia atau *user* menjadi rantai terlemah pada sistem keamanan jaringan. Meskipun *programmer* telah membangun sistem keamanan yang baik, namun jika dioperasikan oleh *user* yang tidak kompeten, sistem tetap bisa dengan mudah diserang oleh *hacker*.

Tujuan dari *paper* studi literatur ini adalah untuk mengetahui pengertian, tahapan, jenis-jenis serta ancaman dari *social engineering* berdasarkan literatur yang penulis kumpulkan.

II. METODE PENELITIAN

Pengerjaan *paper* ini menggunakan teknik studi literatur. Teknik studi literatur merupakan pengumpulan dan analisa literatur terkait teknik *social engineering* yang merupakan salah satu ancaman dalam kemanan sistem informasi. Pengumpulan studi literatur menggunakan Google sebagai mesin pencari utama dan dua *database* jurnal *online* yaitu Science Direct dan ResearchGate. Untuk mencukupi kebutuhan data yang diperlukan, pengumpulan literatur tidak mempertimbangkan faktor kredibilitas jurnal dan konferensi. Namun, pada implementasinya jurnal akan diseleksi menjadi jurnal utama dan jurnal pendukung. Jurnal dan konferensi diseleksi sesuai dengan relevansi topik yang diangkat sesuai tujuan *paper* ini. Berikut secara detail rincian dalam proses pencarian data yang relevan untuk mendukung penyusunan *paper* :

a. Menggunakan kombinasi antara mesin pencarian akademik dengan *database* akademik. Google dipilih sebagai mesin pencari utama jurnal-jurnal yang berhubungan dengan topik dalam *paper* ini. *Keyword* yang digunakan dalam proses pencarian ini terangkum dalam Tabel 1. Dengan mengkombinasikan *keyword* tersebut, memutar balik, menambah dan mengurangi kata, penelitian sebelumnya yang mendukung pembahasan topik *paper* dapat ditemukan. Proses yang sama dilakukan pada dua *database* akademik utama yaitu Science Direct dan ResearchGate, untuk meningkatkan cakupan data pada *paper* ini.

Tabel 1. Kata Kunci Pencarian Literatur

Keyword ke-1	Keyword ke-2	Keyword ke-3
"Social engineering"	"Attack" "Cyber security"	"Information system" "Therats"

b. Sumber penelitian yang digunakan pada *paper* ini meliputi jurnal-jurnal dan konferensi prosiding. *Paper* ini berfokus utama pada konteks *literature review* terkait teknik *social engineering*. Pengembangan *paper* dengan topik tersebut membutuhkan pembahasan dan teori-teori terkait pengertian, kategori, jenis-jenis, dan teknik pencegahan. Penelitian diluar konteks tersebut tidak dipergunakan dalam pengerjaan *paper* ini.
c. Literatur yang telah di*review*, dikategorikan menjadi dua bahasan. Bahasan pertama adalah analisis teknik *social engineering* yang telah dibahas peneliti sebelumnya. Bahasan yang kedua adalah teknik pencegahan dan analisisnya.

III. HASIL DAN PEMBAHASAN

A. Ancaman Social Engineering Terhadap Sistem

Sasaran utama dari *social engineering* adalah sama dengan *hacking* pada umumnya, yaitu untuk memperoleh akses yang tidak sah ke sistem atau informasi dalam rangka melakukan *fraud* (penipuan atau kecurangan), penyusupan ke dalam jaringan, aktivitas mata-mata perindustrian, pencurian identitas, atau hanya untuk menghadirkan gangguan pada sistem atau jaringan. Sasaran-sasaran yang khas adalah perusahaan telfon, perusahaan dengan nama besar, institusi keuangan, agen pemerintah, instansi militer, dan rumah sakit.

Alasan mengapa menggunakan *social engineering* untuk memperoleh akses sangat sederhana yaitu begitu cara ini dikuasai, *social engineering* dapat dipakai di sistem manapun terlepas dari *platform* atau kualitas *hardware* dan *software* yang ada. *Social engineering* sudah ada sejak manusia ada. Ia memangsa mata rantai terlemah pada sistem keamanan, yaitu manusia. *Social engineering* memiliki berbagai bentuk, namun semuanya berdasar pada prinsip menyamar sebagai *non-hacker* yang membutuhkan atau berhak atas informasi untuk memperoleh akses ke sistem.

Serangan *social engineering* menempati dua tingkatan, yaitu tingkatan fisik dan psikologis. Pertama-tama, kita akan konsentrasi pada lingkungan fisik yang rawan terhadap serangan-serangan *social engineering*, yaitu tempat kerja, telepon, tempat sampah dan internet. Di tempat kerja, *hacker* dapat dengan mudah masuk ke kantor dengan berpura-pura sebagai pekerja *maintenance* atau konsultan yang memiliki akses ke organisasi. Kemudian sang penyusup berkeliling kantor sampai dia menemukan kata sandi yang tercecer dan keluar dari gedung dengan informasi yang cukup untuk mengeksploitasi jaringan organisasi dari tempat kerjanya sendiri. Cara lain untuk memperoleh informasi autentifikasi adalah meminta salah seorang pegawai untuk mengetikkan kata sandi dan menghafalkannya.

B. Kategori Serangan Social Engineering

Serangan *social engineering* dapat dikategorikan menjadi dua yaitu :

1. ***Hunting***

Pendekatan ini berusaha untuk melakukan serangan *social engineering* melalui interaksi seminimal mungkin dengan target. Setelah tujuan yang ditentukan tercapai dan pelanggaran terhadap keamanan dilakukan, komunikasi akan segera diakhiri. Ini adalah metodologi yang paling sering digunakan untuk mendukung serangan *cyber* dan sebagai aturan atau modus yang melibatkan satu pertemuan.

2. ***Farming,***

Farming tidak sering dipraktikkan, namun teknik ini dapat digunakan untuk tujuan yang situasional. Penyerang bertujuan untuk membangun hubungan dengan korban untuk mengekstraksi informasi pada periode waktu yang lebih lama. Sepanjang proses, interaksi dapat berubah, target dapat mempelajari kebenaran dan *social engineering* dapat berusaha untuk memeras target [4] [5].

C. Tahapan Serangan *Social Engineering*

Berikut merupakan tahapan-tahapan *social engineering* secara umum :

a. *Research* (Pengumpulan informasi),

Website perusahaan dapat menjadi salah satu sumber informasi utama untuk menjalankan serangan *social engineering*. Informasi seperti nomor kontak perusahaan, lokasi dan alamat cabang, alamat *e-mail*, bagan struktur organisasi, laporan keuangan dan lain-lain, tidak hanya bersangkut-paut dengan calon pelanggan, namun juga memberi kesempatan pada penyerang *social engineering* untuk merencanakan serangan. Seseorang dapat dengan mudah mengumpulkan informasi seperti faktur, korespondensi, manual, *e-mail*, dan lain-lain, yang dapat membantu si penyerang memperoleh informasi penting. Tujuan si penyerang dalam tahap ini adalah untuk mempelajari sebanyak mungkin informasi agar ia dapat menyamar sebagai pegawai, kontraktor, atau vendor.

b. *Hook* (Pemilihan sasaran),

Dalam tahap ini, si penyerang mengidentifikasi mata rantai terlemah untuk ditembus. Target yang paling umum adalah *help desk* dan resepsionis, karena mereka dilatih untuk memberikan bantuan. Organisasi yang yang mempekerjakan pihak luar sebagai *help desk* bahkan lebih rentan lagi. Korban paling umum berikutnya adalah asisten administrasi karena ia mengetahui banyak informasi penting yang beredar di antara anggota tim manajemen. Mereka juga menangani *mail account* dan jadwal supervisor mereka.

c. *Play* (Serangan),

Tahap serangan ini dapat dilakukan dengan berbagai cara dan metode. Serangan ini bertujuan untuk mencapai tujuan social engineering, yang dapat mengekstraksi informasi atau memanipulasi target untuk mengkompromikan sistem.

d. *Exit,*

Terakhir, *social engineering* menyelesaikan interaksi dengan korban, dengan tanpa menimbulkan kecurigaan. Setelah tahap terakhir ini, penyerang biasanya sangat sulit dilacak [2] [6].

D. Jenis-Jenis *Social Engineering*

Berikut adalah jenis serangan *social engineering* yang sering dilakukan oleh *hacker:*

a. Pendekatan Secara Sosial

1. ***Tailgating,***

Tailgating adalah tindakan mengikuti target yang tidak dikenal, yang mempunyai akses yang sah melalui keamanan ke ruang terbatas.

2. ***Impersonating***(meniru),

Penyerang mengambil identitas palsu untuk mendapatkan kredibilitas sebagai dasar untuk melakukan tindakan. Peniruan ini mirip dengan *tailgating*, penyerang bertujuan untuk mendapatkan akses fisik ke area yang aman, dengan mendapatkan izin dari orang yang memiliki akses yang sah dengan tindakan peniruan. Inti dari serangan ini adalah pembuatan skenario yang masuk akal untuk dilakukan kepada korban yang ditargetkan. Metode ini membutuhkan cerita yang kredibel untuk mencegah timbulnya kecurigaan, dan dengan demikian melakukan penelitian pada target tersebut terlebih dahulu mutlak diperlukan.

3. **Melalui telepon,**

Jenis serangan *social engineering* yang paling lazim dilakukan melalui telepon. Seorang *hacker* akan menelpon dan menirukan seseorang yang memiliki otoritas dan secara bertahap mengumpulkan informasi dari si penerima panggilan telepon. *Help desk* adalah contoh yang mudah terkena serangan jenis ini. *Hacker* mampu untuk berpura-pura menelepon dari dalam organisasi dengan cara menggunakan trik-trik pada interkom atau operator interkom, jadi penggunaan *caller-ID* tidak selalu menjamin keamanan. Contoh trik interkom misalnya: "Selamat siang, saya adalah petugas reparasi jaringan telepon. Saya sedang memperbaiki jaringan telepon Anda dan saya membutuhkan Anda untuk menekan beberapa tombol" (sumber : Computer Security Institute). *Help desk* sangatlah rentan terhadap serangan semacam ini karena mereka ditugaskan untuk memberikan *help* (pertolongan). Ini adalah suatu fakta yang dapat dimanfaatkan oleh orang-orang yang berusaha mendapatkan informasi-informasi penting. Pegawai-pegawai *help desk* di-*training* untuk bersikap ramah dan bersedia memberi-kan informasi; ini adalah "tambang emas" untuk serangan *social engineering*. Pegawai-pegawai *help desk employees* dididik sangat minim dalam bidang keamanan dan dibayar dengan gaji yang sangat kecil, sehingga mereka cenderung langsung menjawab pertanyaan dan melanjutkan ke panggilan telepon berikutnya. Hal ini dapat membuat lubang keamanan yang cukup besar.

4. ***Eavesdropping*** (menguping),

Dalam sebuah perusahaan, karyawan dapat dengan mudah mendiskusikan hal-hal rahasia. Hanya karena berada di tempat yang tepat pada waktu yang tepat, pelaku *social engineering* dapat melakukannya dengan mengeksploitasi pelanggaran keamanan seperti ini. Meskipun demikian, penyerang juga dapat secara proaktif mendengarkan saluran komunikasi seperti *e-mail* dan saluran telepon.

5. ***Shoulder surfing,***

Mengacu pada tindakan pengamatan langsung dengan target untuk mendapatkan informasi, biasanya digunakan untuk mengekstraksi data otentikasi

6. ***Dhumpster diving,***

Dumpster diving, yaitu mengacak-acak tong sampah, adalah cara lain yang populer dalam *social engineering*. Sejumlah besar informasi penting dapat dikumpulkan melalui tong-tong sampah perusahaan. "The LAN Times" merinci hal-hal berikut sebagai kemungkinan kebocoran keamanan yang ada di tong sampah: buku telepon perusahaan, bagan organisasi, memo, petunjuk kebijakan perusahaan, jadwal pertemuan, kegiatan-kegiatan, manual sistem, *printout* dari data-data penting atau nama login beserta kata sandi, *printout* dari *source code,* disket, *tape,* kertas surat perusahaan, form memo, serta perangkat keras usang.

7. ***Reverse social engineering****,*

Cara yang paling mutakhir untuk memperoleh informasi dikenal sebagai *reverse social engineering*. Ini adalah saat dimana sang *hacker* menciptakan seorang tokoh yang tampak seperti seseorang yang memiliki otoritas sehingga pegawai akan menanyakan informasi kepadanya, bukan sebaliknya. Apabila diteliti dahulu sebelumnya, direncanakan dan dilaksanakan dengan baik, serangan *reverse social engineering* dapat memberi *hacker* kesempatan yang jauh lebih baik untuk memperoleh data dari pegawai-pegawai. Namun, cara ini memerlukan persiapan, penelitian, dan *pre-hacking* yang cukup banyak untuk dilakukan. Menurut Rick Nelson dalam papernya "*Methods of Hacking : Social Engineering*", tiga bagian dalam serangan *reverse social engineering* adalah sabotase, penawaran, dan bantuan. Sang *hacker* mensabotase sebuah jaringan, membuat masalah muncul. *Hacker* tersebut kemudian menawarkan dirinya sebagai orang yang selayaknya mampu membereskan masalah tersebut. Lalu kemudian, saat ia datang untuk membereskan masalah jaringan, ia meminta beberapa informasi dari pegawai-pegawai dan ia mendapatkan informasi yang ia inginkan. Para pegawai tidak pernah tahu bahwa ia adalah seorang *hacker,* karena masalah pada jaringan mereka terselesaikan dan semua orang senang.

b. Pendekatan Secara Sosio Teknik

1. ***Phising,***

   Serangan *phishing* berupaya mengekstraksi informasi yang dapat diidentifikasi pribadi melalui cara digital, seperti *fake* email yang tampaknya berasal dari sumber yang sah serta situs web palsu. Lebih lanjut penipuan canggih seperti ini cenderung memperhitungkan kerentanan psikologis yaitu dengan memanipulasi korban. *Phishing* menargetkan banyak orang sebagai korban. Situs jejaring sosial juga dapat digunakan oleh penjahat *cyber* untuk menambang data tentang calon korban, mengekstraksi informasi untuk membuat pesan khusus yang tampaknya dikirim oleh teman dekat.

2. ***Baiting,***

   Penyerang dapat menggunakan serangan fisik ini dengan menginfeksi media penyimpanan dengan *malware*

3. ***Whatering hole,***

   Ini adalah salah satu *social engineering* paling canggih, karena membutuhkan teknis yang substansial akan pengetahuan. Setelah meneliti, penyerang mengidentifikasi satu atau lebih situs web yang sah dan secara teratur dikunjungi oleh target. Mencari kerentanan, menginfeksi situs web yang paling menguntungkan untuk serangan dan penipuan [5].

E. *Social Engineering* yang Paling Banyak Dilakukan

Palo Alto Research Center (PARC) telah menyiapkan sejumlah percobaan untuk mengamati potensi pada 2012 terhadap perilaku ancaman orang dalam di lingkungan online yang tertutup. Mereka melihat *game online* multi-pemain besar-besaran, World of Warcraft. *Game* ini memungkinkan pengguna untuk membangun karakter, bergabung dengan organisasi besar yang disebut *guild*, dan melanjutkan misi dan penugasan. Para pemain yang berburu naga dan orc akhirnya berkolaborasi dengan rekan setim, melamar posisi dan mendapatkan imbalan dengan cara yang hampir sama dengan tim kerja yang menangani proyek-proyek besar. Permainan dengan demikian berfungsi sebagai proksi yang cocok untuk lingkungan kerja dunia nyata. Para peneliti menemukan bahwa mereka dapat memprediksi yang akan berhenti dalam enam bulan sebelumnya dengan tingkat akurasi 89%.

Setelah memperluas penelitian ke dunia nyata, mereka menemukan beberapa petunjuk penting yang dapat memprediksi perilaku ancaman orang dalam yang potensial. Gesekan gejala yang paling muncul adalah lebih sedikit email, lebih sedikit pesan setelah jam kerja, lebih sedikit lampiran, dan lebih sedikit kata secara bersamaan. Kelihatannya bahwa karyawan berpotensi melakukan tindak kejahatan dalam organisasi. Menurut para peneliti, model ini dapat ditingkatkan untuk diterapkan ke hampir semua domain tempat interaksi sosial online dapat diamati dan diukur, termasuk dalam *social engineering*. Sehingga bisa disimpulkan, *social engineering* dalam dunia online atau internet lebih sering digunakan para penyerang untuk menipu korbannya [7].

F. Pencegahan *Social Engineering*

Berikut ini merupakan cara-cara yang digunakan untuk mencegah terjadinya *social engineering* :

a. **Pelatihan *Security Awareness,***

Pelatihan *security awareness* direkomendasikan secara konsisten kepada semua karyawan. Pelatihan dapat membantu karyawan memahami mengapa suatu budaya keamanan adalah penting, menyoroti pentingnya pemantauan informasi yang tersedia. Menurut Naomi Fine, seorang pakar dalam bidang rahasia perusahaan dan presiden serta *Chief Executive Officer* dari Pro-Tec Data (www.protecdata.com), 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. Seluruh pegawai harus dilatih bagaimana untuk menjaga data rahasia tetap aman.

b. **Kebijakan *Security,***

*C*ara memerangi *social engineering* membutuhkan tindakan pada kedua aspek, yaitu aspek fisik dan aspek psikologis. Pelatihan pegawai sangatlah penting. Kesalahan yang dilakukan oleh banyak perusahaan adalah mengantisipasi serangan hanya dari sisi fisik. Itu membuat mereka sangat rentan terhadap kemungkinan serangan dari sisi sosial-psikologis. Jadi untuk memulainya, manajemen harus memahami pentingnya mengembangkan dan mengimplementasikan prosedur dan kebijakan *security* yang baik. Secara teoritis, keamanan fisik yang baik tampak seperti hal yang mudah, namun untuk benar- benar mencegah agar rahasia perusahaan tidak sampai bocor, dibutuhkan perhatian tambahan. Siapapun yang memasuki gedung harus diperiksakan kartu iden-titasnya, tanpa terkecuali. Beberapa dokumen khusus perlu untuk dikunci dalam laci atau tempat penyimpanan aman (dan kuncinya tidak dibiarkan tergeletak begitu saja di tempat-tempat yang mudah dijangkau). Dokumen- dokumen lainnya perlu di *shredding* agar tidak bisa dibaca oleh pihak-pihak yang mungkin melakukan *dumpster diving.* Begitu pula media-media magnetik harus dihapus isinya agar datanya tidak bisa dipulihkan kembali (Berg, 1995).

c. **Pembatasan jaringan,**

Suatu organisasi bisa mempertimbangkan memblokir akses ke situs web tertentu pada sistem perusahaan, misalnya situs jejaring sosial. Hal ini karena sering terdapat URL phishing / vishing serangan.

d. **Review website perusahaan,**

Informasi tentang situs web perusahaan dapat menjadi harta karun bagi penyerang. Sehingga harus ditinjau untuk menilai keseimbangan antara kebutuhan akan informasi yang hadir, dan apakah itu menimbulkan risiko atau tidak.

e. ***Social Engineering Penetration Test,***

Penipuan yang umun dilakukan adalah menyusup ke jaringan interkom perusahaan. *Hacker* dapat dengan mudah melepon operator interkom dan meminta untuk melakukan panggilan telepon keluar perusahaan, kemudian melakukan panggilan dengan tagihan yang akan dibayarkan oleh perusahaan. Hal ini dapat dicegah dengan menerapkan kebijakan yang mengontrol percakapan SLJJ dan SLI, dan dengan melacak panggilan-panggilan yang patut diwaspadai. Dan apabila ada yang menelepon dan mengaku sebagai teknisi telepon yang memerlukan kata sandi untuk akses, agar tidak ditanggapi. Menurut "Verizon Communications", teknisi telepon dapat melakukan tes tanpa bantuan dari pelanggan, maka dari itu apabila ada telepon yang mengaku sebagai teknisi telepon dan meminta *password* atau autentifikasi lainnya, patut dicurigai. Seluruh pegawai harus waspada dengan hal ini agar tidak menjadi korban dari cara seperti itu [8].

G. Respon Terhadap Social Engineering

Berikut ini merinci beberapa taktik penyusupan yang umum dilakukan beserta strategi untuk mencegahnya :

- Daerah Rawan Telepon (*Help Desk*), teknik hacker biasanya dengan cara menirukan seseorang dan persuasi. Strategi pencegahannya adalah dengan melatih pegawai / *help desk* untuk tidak memberi kata sandi atau informasi rahasia lainnya melalui telepon. Semua pegawai diberikan PIN khusus untuk membantu konfirmasi petugas *help desk*
- Daerah Rawan Pintu Masuk Gedung Kantor, teknik hacker biasanya dengan cara mengakses dari jalan yang tidak sah. Strategi pencegahannya adalah dengan memberikan prosedur keamanan ketat, pelatihan pegawai, dan keberadaan petugas.
- Daerah Rawan Kantor, teknik hacker biasanya dengan cara mengintip, berjalan-jalan di ruangan mencari kantor yang terbuka, mencuri dokumen-dokumen penting. Strategi pencegahannya adalah dengan tidak mengetik *password* saat ada orang lain (atau bila terpaksa, ketik dengan cepat), semua tamu yang datang ditemani, tandai dokumen-dokumen yang penting dan kunci mereka di tempat yang aman
- Daerah Rawan Ruang/Meja untuk Meninggalkan Pesan, teknik hacker biasanya dengan cara penyisipan memo palsu. Strategi pencegahannya adalah kunci dan awasi ruangan
- Daerah Rawan Ruang Mesin, teknik hacker biasanya dengan cara mencoba memperoleh akses, mencuri peralatan, atau memasang penyadap untuk mencuri data penting. Strategi pencegahannya adalah dengan memastikan ruang-ruang mesin telah dikunci dan diawasi setiap saat, serta rincian daftar peralatan harus terus diperbaharui.
- Daerah Rawan Telepon Dan Interkom Perusahaan, teknik hacker biasanya dengan cara mencuri akses telepon keluar perusahaan. Strategi pencegahannya adalah dengan mengontrol telepon SLJJ dan SLI, melacak telepon-telepon mencurigakan, menolak transfer sambungan telepon
- Daerah Rawan Tong Sampah, teknik hacker biasanya dengan cara mengacak-acak tong sampah. Strategi pencegahannya adalah dengan menyimpan sampah di tempat yang aman dan teramati, mencacah dokumen-dokumen berisi data-data penting, menghapus media-media magnetik.
- Daerah Rawan Internet-Internet, teknik hacker biasanya dengan cara menggunakan *Software-software* yang dapat mencuri *password.* Strategi pencegahannya adalah dengan Kewaspadaan kontinu pada perubahan sistem dan jaringan, pelatihan dalam penggunaaan

IV. KESIMPULAN

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. Dalam dunia nyata, teknik *social engineering* yang paling sering digunakan adalah eksploitasi internet, seperti *fake-email, phising*, dan lain sebagainya.

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. Selain mensosialisasikan kebijakan, sangat penting mendidik pegawai agar waspada terhadap metode *social engineering* berikut resiko yang terjadi andaikan serangan tersebut berhasil. Karena salah satu titik lemah rantai keamana adalah manusia, pendidikan menjadi faktor yang sangat penting.

UCAPAN TERIMA KASIH

Judul untuk ucapan terima kasih dan referensi tidak diberi nomor. Terima kasih disampaikan kepada Tim JIFTI yang telah meluangkan waktu untuk membuat template ini.

REFERENSI

P. J. S. Nabie Y Contech, "Cybersecurity: Risk Vulnerabilities and Countermeasures to Prevent Social Engineering Attacks," *International Journal of Advanced Computer Research,* vol. 6, pp. 23-31, 2016.

"Hacking the human operating system: The role of social engineering within cybersecurity," in *Technical report, Intel Security*, 2015.

S. Heikkinen, "Social Engineering in The World of Emerging Communication Technologies," *Proceedings of Wireless World Research Forum,* pp. 1-10, 2006.

“Hacking the human of operating system : The Role of social engineering within cybersecurity," *Technical Report, Intel Security,* 2015.

B. H. M. T. Breda F, "Social Engineering and Cyber Security," *Conference Paper,*2017.

R. S. Patel, "Kali Linux Social Engineering," *Packt Publishing Ltd,* 2013.

D. Tayouri, "The human factor in the social media security - combining education and technology to reduce social engineering risks and damages, " *Procedia Manufacturing,* vol. 3, no. 2015, pp. 1096-1100, 2015.

R. L. B. G. A. R. A. B. Matthew Edwards, "Panning for Gold: Automatically analysing online social engineering attack surfaces," *ScienceDirect,* no. Computer & Security, pp. 18-34, 2017.