IT Risk Management

Pertanyaan:

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!

2. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

3. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi?
4. Jelaskan sumber penyebab ancaman terhadap IT ! Lengkapi penjelasan tersebut menggunakan contoh

5. Dalam Manajemen Resiko IT digunakan framework sebagai guide dalam pelaksanaannya. Jelaskan persamaan dan perbedaan dari framework-framework IT Risk Management yang ada? (at least membandingkan 2 framework, more is better)

---- Selamat bekerja ----

Nama : Hamzah Ramadhan

NIM : 182420124

Kelas : MTI Reguler B

UAS IT Risk Management

Pertanyaan:

1. Metode apa yang digunakan oleh seorang social engineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!

2. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis di mana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami risiko apa yang mungkin muncul di lingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

3. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi?
4. Jelaskan sumber penyebab ancaman terhadap IT ! Lengkapi penjelasan tersebut menggunakan contoh

5. Dalam Manajemen Resiko IT digunakan framework sebagai guide dalam pelaksanaannya. Jelaskan persamaan dan perbedaan dari framework-framework IT Risk Management yang ada? (at least membandingkan 2 framework, more is better)

---- Selamat bekerja ----

Jawaban :

1. Seorang social engineering hacker menggunakan trik pendekatan sosial dan psikologi korbannya dalam melakukan aksi untuk memperoleh userid dan password dari pengguna akun sosial media atau akun e-banking dengan tujuan menguntungkan dirinya sendiri.
   Contohnya :
   Hari adalah seorang social engineering hacker. Dia sudah lama memendam rasa suka kepada teman wanitanya bernama Andini. Namun Hari bukan tipe orang yang berani berbicara langsung kepada wanita. Hari adalah anak yang pemalu. Dan dia lebih banyak aktif di dunia maya daripada di dunia nyata. Maka Hari memutuskan untuk memperoleh userid dan password dari akun instagram dan facebook Andini untuk mengetahui biodata lengkap Andini, serta kesukaannya.
   Hari membuat sebuah halaman situs film korea yang berisi film-film yang bisa diunduh. Namun dengan persyaratan harus login akun facebook dan instagram yang dimiliki oleh usernya. Kemudian halaman situs tersebut dibagikan link nya kepada temannya untuk diteruskan nanti ke Andini.
   Hal yang kemudian terjadi adalah, apabila Andini menerima link halaman situs tersebut dan tertarik untuk melakukan download, maka secara otomatis Andini telah menyerahkan userid

dan password facebook dan instagramnya di halaman situs tersebut. Karena halaman tersebut memiliki pop up untuk log in ke akun facebook dan instagram. Dimana pop up itu ditautkan untuk menyimpan informasi yang diberikan oleh user berupa userid dan password. Teknik tersebut biasa disebut Baiting.

2. Sebuah organisasi setidaknya memiliki kemampuan untuk mengelola dan menerapkan manajemen risiko TI yang menjadi aset penting bagi organisasi atau perusahaan tersebut. Strategi yang dibutuhkan adalah menerapkan kerangka-kerangka terpadu dalam mengelola risiko TI sehingga dapat mengambil keputusan secara rasional dan menjauhkan organisasi dari kerugian yang lebih besar.
   Kerangka-kerangka untuk memanajemen risiko adalah :
   1. Identifikasi risiko
      Hal ini berkaitan dengan pengetahuan anggota lain mengenai aset yang dimiliki oleh organisasi disertai dengan peluang risiko apa yang akan terjadi dengan aset tersebut.
   2. Analisa dan Prioritas risiko
      Setelah kita mengetahui berbagai aset yang dimiliki, kita harus melakukan seleksi terhadap aset yang penting dan rentan terhadap risiko yang berat. Hendaknya aset tersebut diberikan sebuah proteksi khusus agar terhindar daripada risiko yang dibayangkan.
   3. Perencanaan dan Implementasi penanggulangan
      Semua anggota harus diberikan kesadaran biaya dan pentingnya pencegahan dan perencanaan dari risiko yang akan terjadi terhadap aset TIK yang dimiliki oleh organisasi atau perusahaan. Dengan begitu, maka semua akan peduli dan menaruh perhatian lebih terhadap segala macam ancaman yang datang. Selain itu diperlukan juga langkah pencegahan apabila risiko yang timbul tidak bisa diantisipasi seperti menyimpan cadangan data, server dan lain sebagainya.
   4. Pantau dan laporkan
      Kepedulian yang mulai timbul dari masing-masing anggota organisasi atau perusahaan nanti akan melahirkan kesadaran untuk memantau setiap ancaman dan bahaya yang mungkin timbul dan menjadi salah satu sebab risiko terjadi. Dan setiap temuan tadi baiknya dilaporkan kepada pihak manajemen agar bisa memberikan keputusan dalam menghindari risiko yang lebih besar.
   5. Kontrol
      Pihak manajemen berperan juga dalam hal kontrol setiap laporan yang diberikan oleh anggota dan tidak lupa mengontrol kinerja anggota yang sekiranya berpeluang untuk menghadirkan risiko bagi aset.
   6. Petik pelajaran
      Ketika semua hal telah dilaksanakan dengan baik, mulai dari perencanaan, pencegahan, pemantauan, hingga tindak lanjut berupa kontrol dan aksi yang dilakukan di lapangan, namun ternyata masih juga terjadi risiko tersebut, hal yang kemudian dilakukan adalah bagaimana dalam situasi tersebut, pihak manajemen beserta seluruh jajaran hingga anggota memetik pelajaran yang berharga untuk dijadikan evaluasi agar tidak terjadi lagi bencana yang serupa. Minimal kita bisa melakukan perbaikan segera ketika bencana tersebut terjadi.

3. Teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi karena teknologi yang usang memiliki celah yang mudah untuk diserang. Setiap tahun, serangan siber makin bervariasi dan berkembang seiring zaman. Semakin canggih perangkat teknologi yang ada, maka semakin canggih pula cara serangan siber terhadap perangkat yang ada. Maka setiap tahun, selalu ada inovasi dari teknologi dari tingkat keamanan untuk diperbarui. Semakin lama usia teknologi yang digunakan, maka tingkat keamanan yang dimiliki juga semakin lemah. Sementara itu para peretas yang berada di luar sana selalu mengikuti perkembangan teknologi yang ada. Maka jika teknologi yang usang masih digunakan, hal

tersebut akan memudahkan para peretas dalam menjalankan serangannya ke sistem maupun data yang ada.

4. Sumber penyebab ancaman IT terbagi menjadi 2 :
   1. Ancaman aktif adalah ancaman yang berasal dari serangan para peretas yang ingin menyerang perangkat komputer dengan tujuan untuk melakukan pencurian data pribadi maupun organisasi
      Ancaman aktif bisa berupa
      a. Unauthorized Access to Computer System and Service : peretas masuk ke dalam sistem jaringan komputer yang ada tanpa memiliki izin yang legal.
      b. Data Forgery : melakukan pemalsuan data-data pada dokumen elektronik yang ada untuk disalahgunakan.
      c. Cyber Espionage : melakukan kegiatan mata-mata di dalam sebuah sistem dengan cara menyusup ke dalam sistem tersebut tanpa izin yang sah.
      d. Cyber Sabotage and Extortion : melakukan gangguan dengan memasukkan virus komputer atau logic bom untuk merusak sistem sehingga komputer atau jaringan tidak bisa digunakan.
   2. Ancaman pasif adalah ancaman yang berasal dari kesalahan pengguna dalam menggunakan perangkat IT maupun sistem informasinya dan berupa ancaman bencana alam yang datang.
      Ancaman pasif bisa berupa
      a. Bencana Alam : banjir, kebakaran, gempa bumi, petir, angin badai.
      b. Kesalahan pengguna : tersiram air, korsleting listrik, terjatuh

5. Framework yang biasa digunakan dalam manajemen risiko IT adalah :

COBIT

COBIT yang merupakan singkatan dari *Control Objectives for Information and Related Technology*, dimiliki dan didukung oleh ISACA. Pertamakali di luncurkan pada tahun 1996 sebagai COBIT. Versi yang terbaru saat ini adalah COBIT 2019 namun hingga saat ini COBIT 5 masih digunakan secara luas sebagai framework TI untuk Tata Kelola TI. Di mana COBIT 5 merupakan gabungan dari framework COBIT 4.1, VAL IT 2.0, dan Risk IT.

COBIT merupakan framework TI yang digunakan untuk membantu kita dalam mengoptimalkan *value* atau nilai suatu organisasi enterprise melalui TI dengan cara menjaga keseimbangan antara realisasi keuntungan, optimalisasi risiko, dan pemanfaatan sumber daya. Kerangka kerja TI ini mengover baik bisnis maupun unit TI dalam keseluruhan organisasi. Memberikan model maturity atau model kematangan proses dan metriknya untuk mengukur apakah organisasi TI telah mencapai tujuannya. Sebagai tambahan, COBIT juga menjaga keseimbangan antara kebutuhan stakeholder baik internal maupun eksternal.

ISO/IEC 27001 merupakan standarisasi untuk ISMS (Information Security Management System) yang isinya merupakan pedoman petunjuk dan prosedur praktis pengelolaan Sistem Manajemen Keamanan Informasi. ISO27001 lebih memfokuskan diri pada aspek manajemen pelaksanaan. Dimana output dokumennya merinci hingga detail aktivitas keamanan yang mesti dilakukan. Namun demikian proses implementasi maupun aktivitas audit keamanan sistem informasi sebenarnya bersifat fleksibel tergantung pada tipe dan kebutuhan organisasi serta fokus dan *concern* mereka pada proses bisnis dan proses TI-nya seturut dengan tujuan dan strategis perusahaan.

It Risk Management & Disaster Recovery

Dosen Pengampu : Dedy Syamsuar , S.Kom., M.I.T., Ph.D

Nama : Masroni Dedi Kiswanto
NIM : 182420139
Kelas : MTI Reguler B

PROGRAM PASCASARJANA

MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

Tahun 2019

IT Risk Management

Pertanyaan:

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!

2. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

3. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi?
4. Jelaskan sumber penyebab ancaman terhadap IT ! Lengkapi penjelasan tersebut menggunakan contoh

5. Dalam Manajemen Resiko IT digunakan framework sebagai guide dalam pelaksanaannya. Jelaskan persamaan dan perbedaan dari framework-framework IT Risk Management yang ada? (at least membandingkan 2 framework, more is better)

---- Selamat bekerja ----

Jawaban.

---

1. Malware atau Keylogger

Biasanya Social Engineering hacker menyisipkan Link yang berisikan malware di beberapa website jika user asal buka link tersebut atau install aplikasi sembarangan yang ada di internet maka hacker akan dengan mudah mendapatkan segala sesuatu yang bersifat privasi dari pengguna tersebut. Karena dalam link atau aplikasi yang disisipkan pada beberapa situs tersebut bisa jadi mengnadung malware yang telah disisipi keylogger. Jika sudah terinfeksi malware tersebut maka setiap user ID, Email, hingga password yang diketik oleh user akan direkam dan dikirimkan oleh trojan yang ada didalamnya.

Contoh keylogger berbentuk software adalah Invisible Keylogger, KGB Keylogger, dan Stealth Keylogger. Software ini bisa di install ke computer korban dan secara otomatis software ini akan menyembunyikan dirinya sehingga tidak diketahui oleh korbannya. Korban tidak akan bisa melihat program ini sedang berjalan, karena semua software keylogger menawarkan Hide modus (Modus Sembunyi) yang tidak akan menampilkan

icon, nama program pada task manager dan lainnya. Banyak juga Trojan yang digunakan para hacker yang berfungsi sebagai keylogger seperti Back Orifice, Netbus, Sub Seven,dll.

---

2. Strategi Untuk Memanagement resiko IT yaitu

1. Risk Identification merupakan proses dalam menentukan apa, bagaimana, dan mengapa suatu kondisi atau kejadian dapat terjadi. Misalnya mengidentifikasi masalah IT yang kemungkinan timbul seperti kemungkinan tersebarnya data yang bersifar rahasia ataupun kehilangan data, dengan mengetahui kemungkinan tersebut maka upaya yang dilakukan yaitu bagaimana seluruh staff harus bisa menjaga data yang bersifat rahasia dan juga memberikan keamanan pada data center suatu organisasi berupa firewall dan lain sebagainya. Selain itu untuk mengantisipasi terjadinya kehilangan data perlu juga dilakukan backup data hal ini dilakukan sebagai langkah antisipasi jika sewaktu waktu data hilang/bermasalah, penting juga untuk melakukan pengamanan fisik pada suatu data center yang mengelola IT tersebut. Sehingga upaya Risk Indentifikation sebagai salah satu IT risk Management dapat berjalanan dengan baik .
2. Risk Assesment
   risk assessment untuk menentukan tingkat ancaman yang potensial dan resiko yang berhubungan dengan suatu sistem IT seluruh *System Development Life Cycle* (SDLC). Output hasil dari proses ini membantu kearah mengidentifikasi kendali yang sesuai untuk mengurangi atau menghapuskan resiko sepanjang/ketika proses peringanan resiko. Untuk menentukan kemungkinan suatu peristiwa/kejadian di masa mendatang yang kurang baik, ancaman pada suatu sistem IT harus dianalisis bersama dengan *vulnerability* yang potensial dan pengendalian pada tempatnya untuk sistem IT.
3. *Risk mitigation*
   adalah satu langkah yang melibatkan usaha-usaha untuk memprioritaskan, mengevaluasi dan menjalankan kontrol atau pengendalian yang dapat mengurangi resiko yang tepat yang direkomendasikan dari proses *risk assessment*.

---

3. mengacu kepada ancaman IT yang dihadapi dari penggunaan teknologi yang sudah usang. Penggunaan teknologi yang sudah usang akan memiliki tingkat keamanan teknologi yang semakin rendah hal ini ter jadi karena dalam dunia IT selalu ada pembaharuan. Contohnya seperti anti virus, jika anti virus tidak di update maka anti virus tersebut tidak akan mendeteksi virus jenis baru yang disusupkan kedalam aplikasi, website, ataupun ke jaringan internet. Sehingga pembaruan terhadap teknologi baik dari software ataupun Hardware harus selalu dilakukan demi keamanan IT pada suatu organisasi.

4. **Backdoor** merupakan algoritma atau sistem enkripsi yang bermanfaat untuk mem-bypass proses otentifikasi atau kontrol keamanan. Sebagai contoh, sebuah backdoor dapat dimasukkan ke dalam kode di dalam sebuah situs belanja online (e-commerce) untuk mengizinkan pengembang tersebut memperoleh informasi mengenai transaksi yang terjadi antara pembeli dan penjual, termasuk di antaranya adalah kartu kredit.

Denial-of-service attacks **(DOS)** merupakan serangan terhadap sistem komputer dengan tujuan supaya sumberdaya jaringan komputer kepunyaan korban laksana server, website, atau software sehingga tidak bisa bekerja.Penyerang dapat menyerang dengan teknik memasukkan password korban berkali-kali sampai-sampai akun korban terkunci atau dengan teknik lain memberi beban pada sistem jaringan komputer hingga overload sampai-sampai sistem komputer korban mustahil bekerja. Kalau serangannya dari satu IP address dapat diatas dengan teknik memblock IP tsb tapi bila serangannya bertipe DDoS (Distributed Denial of Service) maka serangan hadir dari sekian banyak titik dalam jumlah besar sampai-sampai sulit guna diatasi, Serangan ini biasa hadir dari komputer zombie atau botnet yang dikuasai oleh penyerang

Evasdropping merupakan tindakan diam-diam memperhatikan percakapan individu (menguping), seringkali antara host di dalam jaringan yang sama. Misalnya, program laksana Karnivore dan NarusInSight telah dipakai oleh FBI dan NSA guna menguping sistem penyedia layanan internet. Bahkan mesin yang beroperasi sebagai sistem tertutup (yaitu, tanpa kontak ke dunia luar) bisa disadap melewati pemantauan transmisi elektro-magnetik samar yang didapatkan oleh perlengkapan

Direct Access Attacks merupakan mereka yang punya akses langsung secara jasmani terhadap komputer dapat secara langsung mencopy data. Malah lebih dari tersebut mereka dapat membahayakan ketenteraman dengan tindakan laksana : memodifikasi OS, menginstall aplikasi jahat (worms, keylogger, covert listening devices, dsb). Walau sudah memakai sistem ketenteraman komputer, tetap saja dapat di tembus dengan teknik membooting komputer lantas menjalankannya memakai OS yang terinstall di USB atau CD Room

Multivector, Polymorphic Attacks serangan multi-vektor atau polimorfik. Polymorphic attacks merupakan ancaman maya hadir dengan menggabungkan sejumlah jenis serangan dan tidak jarang kali berubah format untuk menghindari perlengkapan kontrol ketenteraman saat mereka menyebar ke dalam sistem. Ancaman ini sudah diklasifikasikan sebagai serangan cyber generasi kelima.

Spoofing merupakan tindakan menyamar sebagai entitas atau user yang valid melewati pemalsuan data (seperti alamat IP atau nama pemakai), guna mendapatkan akses ke informasi atau sumber daya yang tidak dipunyai oleh pihak yang tidak berwenang. Ada sejumlah jenis spoofing, termasuk:

- Email spoofing, di mana penyerang memalsukan alamat ekspedisi (Dari, atau sumber) dari suatu email.
  Alamat IP spoofing, di mana penyerang mengolah alamat IP sumber dalam paket jaringan guna menyembunyikan identitas mereka atau meniru sistem komputasi lain.

- MAC spoofing, di mana seorang penyerang memodifikasi alamat Media Access Control (MAC) dari antarmuka jaringan mereka guna tampil sebagai pemakai yang sah di jaringan.
- Spoofing biometrik, di mana penyerang menghasilkan sampel biometrik palsu untuk diperlihatkan sebagai pemakai lain

Privilage escalation merupakan situasi di mana penyerang dengan level akses terbatas bisa -tanpa otorisasi- menambah hak istimewa atau tingkat akses mereka. Sebagai contoh, pemakai komputer standar barangkali dapat mengelabui sistem supaya memberi mereka akses ke data yang dibatasi; atau bahkan guna "menjadi root" dan mempunyai akses sarat yang tidak terbatas ke sebuah sistem

---

5. PERBEDAAN :

• COBIT dan ITIL adalah standard yang cakupan areanya adalah menengah ke bawah

• COBIT dan ITIL cocok jika dijadikan sebagai IT framework IT Risk management

• ISO 38500 cocok jika digunakan sebagai framework IT Risk Management.

• Kerangka kerja COBIT memasukkan hal-hal berikut ini : (1) Maturity Models , (2) Critical Success Factors (CSFs), (3) Key Goal Indicators (KGIs), dan (4) Key Performance Indicators (KPIs).

• Kerangka kerja yang digunakan untuk mengelola infrastruktur teknologi dan informasi dalam suatu organisasi, dan bagaimana memberikan pelayanan yang terbaik bagi para pengguna teknologi informasi.

• Kerangka kerja digunakan bagi pemerintahan untuk membantu mereka pada tingkat tertinggi dari organisasi untuk memahami dan memenuhi kewajiban hukum, peraturan, dan etika mereka dalam hal penggunaan organisasi mereka 'IT.

PERSAMAAN :

Dijadikan sebagai framework IT risk Managemen

memberikan pedoman pada perusahaan bahwa keputusan-keputusan strategic IT tidak hanya berada pada CIO saja tetapi juga pada direksi.

COBIT

- COBIT adalah framework matang, pertama kali dirilis pada tahun 1996 oleh Information System Audit and Control Association (ISACA)
- Sekarang CoBIT dipublikasikan dengan nama ITGI (the IT Governance Institute)
- COBIT adalah framework untuk informasi manajemn resiko IT, atau lebih formal, sebuah "kerangka kerja dan toolset pendukung yang memungkinkan manajer untuk menjembatani kesenjangan antara kebutuhan pengendalian permasalahan teknis dan risiko bisnis"(ref: ISACA)

Kelebihan Cobit:

1. Rahasia
2. Proteksi terhadap informasi yang sensitif dari akses yang tidak bertanggung jawab.

3. Integritas

4. Berhubungan dengan penyediaan informasi yang sesuai untuk manajemen.

5. Secara umum dapat dikatakan bahwa COBIT merupakan sebuah model tata kelola TI yang memberikan sebuah arahan yang lengkap mulai dari sistem mutu, perencanaan, manajemen proyek, keamanan, pengembangan dan pengelolaan layanan. Arahan dari COBIT kemudian didetailkan kembali oleh beberapa model framework sesuai dengan perkembangan keilmuan.

Kekurangan COBIT

1. COBIT hanya memberikan panduan kendali dan tidak memberikan panduan implementasi operasional.

2. COBIT hanya berfokus pada kendali dan pengukuran.

ITIL

- ITIL adalah sebuah framework yang mulai dikembangkan sejak tahun 1980 oleh pemerintahan Inggris, untuk kebutuhan mereka sendiri
- Dalam beberapa tahun terakhir ini telah diadopsi secara luas, dan internasional
- Dapat dikatakan kerangka manajemen yang paling banyak digunakan IT
- ITIL mencakup struktur organisasi dan persyaratan keterampilan untuk organisasi IT dengan menghadirkan seperangkat prosedur manajemen
- Ini dimaksudkan untuk menjadi pemasok independen dan berlaku untuk semua aspek infrastruktur TI.

Kelebihan ITIL :

1. Memberi deskripsi rinci sejumlah praktik penting TI dan menyediakan daftar komprehensif tugas dan prosedur yang didalamnya setiap organisasi dapat menyesuaikan dengan kebutuhannya sendiri

2. ITIL bukan merupakan standard yang memberikan prescription tetapi lebih kepada merekomendasikan, oleh karena itu implementasi antara satu organisasi dengan organisasi lain dapat dipastikan terdapat perbedaan. Dengan demikian kita tidak bisa membandingkan / melakukan benchmark secara pasti;

Kelemahan ITIL :

1. Kelemahan ITIL antara lain: buku-buku ITIL sulit terjangkau bagi pengguna non komersial, ITIL bersifat holistic yang mencakup semua kerangka kerja untuk tatakelola TI, pelaksanaan pedoman dalam buku ITIL memerlukan pelatihan khusus dan biaya pelatihan atau sertifikasi ITIL terlalu tinggi.

Melihat dari beberapa kelebihan dan kekurangan dari masing – masing Framework IT Risk Manajemen diatas menurut saya Cobit paling tepat digunakan sebagai Framework IT risk managemen hal ini karena menurut saya cobit cobit menyediakan informasi yang sesuai untuk manajemen resiko IT

IT Risk Management
Nama : Mezi Puspayani
Nim : 182420120

Pertanyaan Dan Jawaban :

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!
   JAWAB : Biasanya seorang social enggineering hacker untuk memperoleh user id dan password dari pengguna tertentu dengan cara melakukan penipuan dengan metode Phising Attack yaitu tehnik untuk mendapatkan informasi sensitif(Data pribadi atau akun) dari korban dengan cara menulis email yang seolah-olah berasal dari website resmi. Contohnya hacker akan menulis email yang menganjurkan korban untuk meng update data akun dan mengganti password akun dengan dalih akun korban disalah gunakan orang. Korban akan diminta klik link menuju website yang benar-benar mempunyai kemiripan 100% seperti aslinya dimana website tersebut sebenarnya palsu yang dibuat oleh hacker itu sendiri.

2. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatar belakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

   Jawab :
   Strategi strategi yang dapat dilakukan untuk melakukan management resiko:
   1. **Membuat Perencanaan manajement resiko yang solid**. Contohnya seperti membuat daftar resiko, Penilaian tiap risiko berdasarkan kecendrungan terjadi dan dampaknya, Penilaian terhadap pengendalian saat ini, dan Rencana tindakan
   2. **Menentukan bagaimana cara menangani resiko.** Contohnya mengidentifikasi seluruh risiko utama dalam bisnis kita, memprioritaskannya berdasarkan kecendrungan dan dampak, dan menilai efektifitas kendali sekarang ini.
   3. **Memonitoring.** Contohnya Memonitor bisnis secara reguler untuk mengidentifikasi dan menangani risiko baru.

3. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi?
   Jawab : Karena teknologi yang sudah kita gunakan tersebut masih memiliki/ menyimpan data-data yang telah kita buat walaupun terlihat tidak berfungsi lagi akan tetapi masih bisa direcovery kembali dengan cara mengabil chif yang masih tersimpan didalamnya maka dari itu kita harus menghancurkan barang tersebut agar kedepannya nanti tidak menjadi ancaman.

4. Jelaskan sumber penyebab ancaman terhadap IT ! Lengkapi penjelasan tersebut menggunakan contoh.
   Jawab : Sumber ancaman terhadap IT contohnya hardisk yang telah rusak dimana kita sering menyepelekan hal ini padahal itu juga termasuk sumber ancaman karena biasanya

kita menyimpan data-data yang penting didalamnya. Apabila hardisk tersebut kita buang begitu saja tanpa dihancurkan terlebih dahulu maka akan disalah gunakan oleh orang yang salah dan data kita akan diambil oleh orang tidak bertanggungjawab maka itu bisa jadi ancaman untuk kita ataupun perusahaan tempat kita bekerja.

5. Dalam Manajemen Resiko IT digunakan framework sebagai guide dalam pelaksanaannya. Jelaskan persamaan dan perbedaan dari framework-framework IT Risk Management yang ada? (at least membandingkan 2 framework, more is better).

   Jawab :

   1. COBIT (*Control Objectives for information and related Teclonology*) adalalah membantu manajemen senior dalam memahami dan mengelola risiko-risiko yang berhubungan dengan IT. COBIT menyediakan kerangka IT governance dan petunjuk control objective yang detail untuk manajemen, pemilik proses bisnis, user dan auditor. *Planning & Organisation. Acquisition & Implementation* yaitu Domain ini menitikberatkan pada proses pemilihan, pengadaaan dan penerapan teknologi informasi yang digunakan. *Delivery & Support* yaitu Domain ini menitikberatkan pada proses pelayanan TI dan dukungan teknisnya. Dan *Monitoring* yaitu domain ini menitikberatkan pada proses pengawasan pengelolaan TI pada organisasi.

   2. PMBOK (*Guide Integration Project Risk*) yaitu TahapanProject Management Plan Scope Management Perancangan, Risk Management Plan Risk Time Management 1 Planning Cost Identify Risk, Risk Identification 2 Quality Qualitative Risk Analysis, Risk Analysis Human Resources 3 Quantitative, Risk Responses Communication Risk Analysis 4 Planning Risk Plan Risk Responses, Risk Monitoring and 5 Control Procurement Monitor & Control Risk Source : PMBOK Guide 4th Edition.

NAMA :MUHAMMAD SYAHRIL

NIM : 182420106

KELAS: MTI REGULER-B

IT Risk Management

Pertanyaan:

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!

2. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

3. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi?
4. Jelaskan sumber penyebab ancaman terhadap IT ! Lengkapi penjelasan tersebut menggunakan contoh

5. Dalam Manajemen Resiko IT digunakan framework sebagai guide dalam pelaksanaannya. Jelaskan persamaan dan perbedaan dari framework-framework IT Risk Management yang ada? (at least membandingkan 2 framework, more is better)

---- Selamat bekerja ----

1. Phishing menjadi jenis serangan paling umum dalam social engineering. Hacker akan menggunakan email yang berisi pesan palsu dan link berbahaya untuk memancing korban agar memberikan informasi penting agar korban percaya.Contohnya hacker akan menulis pesan semirip mungkin dengan perusahaan resmi. Pesan juga akan ditulis dengan bahasa yang mampu menimbulkan rasa urgensi sehingga korban akan membuka link berbahaya dan memberikan data sensitif seperti user id, password, atau data penting lainnya. Jika Anda menemukan email yang mencurigakan sebaiknya hindari untuk membuka attachment atau link di dalamnya karena hacker juga bisa mengirim malware melalui email tersebut

2. A. Melakukan perencanaan: dengan melakukan perencanaan kita dapat memutuskan bagaimana manajemen resiko yang baik dan sesuai dengan proyek yang dilakukan contohnya sebelum memulai suatu proyek perusahaan harus terlebih dahulu membuat daftar resiko,penilaian tiap resiko berdasarkan kecendrungan terjadi dan dampaknya,penilaian terhadap pengendalian saat ini,dan rencana tindakan yang akan dilakukan

B. melakukan identifikasi:mencari dampak resiko berdasarkan kecendrungan dan dampak yang akan terjadi.

C. melakukan evaluasi:setelah masalah teridentifikasi kemudian masalah di evaluasi berdasarkan probabilitas kejadian resiko yang akan terjadi dan potensi kerugian yang terkait dengannya.

D. Melakukan mitigasi: etelah risiko diidentifikasi dan dievaluasi, tim proyek mengembangkan rencana mitigasi risiko, yang merupakan rencana untuk mengurangi dampak kejadian tak terduga

E.Memindahkan resiko:melakukan backup data banyak tempat(serverlain)serta melakukan kerja jama dengan pengguna jasa yang berhubungan dengan perlindungan data asset

3. Teknologi usang dapat menjadi ancaman bagi keamanan teknologi karena teknologi usang merupakan teknologi yang tidak digunakan lagi/sudah lama,kebanyakan teknologi usang di indonesia biasanya dibuang begitu saja tidak seperti di negara-negara lain yang biasanya teknologi yang telah usang/sudah lama dihancurkan menggunakan mesin penghancur.hal ini sangat membahayakan karena memungkinkan orang bisa mengakses data yang ada di dalam teknologi yang usang tersebut.contohnya hardisk yang ada di tekologi usang jika tidak dimusnahkan/dihancurkan maka orang bisa mengambil data yang ada di dalam hardisk tersebut.

4. Sumber penyebab ancaman IT salah satunya adalah fraud atau penipuan yang memamfatakan celah di pengguna teknologi digital,fraud biasanya menincar kelengahan pengguna digital.fraud biasanya datang dari karyawan,eks karyawan dan sumber lainya yang mengeti kondisi yang ada di dalam perusahaan tersebut.contohnya Kasus transfer fiktif ini dilaporkan oleh Kepala BRI Kabupaten Kampar, Sudarman dan seorang pegawai di BRI Rustian Marta. Pencatatan palsu dalam pembukuan atau laporan maupun dokumen kegiatan usaha. Laporan atau transaksi rekening bank yang dilakukan tersangka sebesar Rp1,6 miliar itu tanpa disertai uangnya. Hanya dalam catatan ada transfer uang, faktanya fiktif. Seperti dilansir detikcom, kronologi transfer fiktif ini bermula pada Rabu (23/02) lalu. Saat tim pemeriksa internal dari BRI Cabang Bangkinang, Ibukota Kabupaten Kampar melakukanpemeriksaan ke Unit BRI Tapung, ditemukan kejanggalan transaksi. Hasil pemeriksaan itu menyebutkan, adanya kejanggalan antara jumlah saldo neraca dengan kas tidak seimbang. Setelah dilakukan pemeriksaan lebih lanjut, adanya pembukaan setoran kas sebanyak Rp1,6 miliar. Uang sebanyak itu diketahui ditransfer dari BRI Unit Pasir Pangaraian II ke Unit BRI

5. 1.COBIT

Merupakan singkatan dari singkatan dari *Control Objectives for Information and Related Technology* dimiliki dan didukung oleh ISACA Pertamakali di luncurkan pada tahun 1996 sebagai COBIT. Versi yang terbaru saat ini adalah COBIT 2019 namun hingga saat ini COBIT 5 masih digunakan secara luas sebagai framework TI untuk Tata Kelola TI. Di mana COBIT 5 merupakan gabungan dari framework COBIT 4.1, VAL IT 2.0, dan Risk IT. COBIT merupakan framework TI yang digunakan untuk membantu kita dalam mengoptimalisasikan *value* atau nilai suatu organisasi enterprise melalui TI dengan cara menjaga keseimbangan antara realisasi keuntungan, optimalisasi risiko, dan pemanfaatan sumberdaya. Kerangka kerja TI ini

mengcover baik bisnis maupun unit TI dalam keseluruhan organisasi. Memberikan model maturity atau model kematangan proses dan metriknya untuk mengukur apakah organisasi TI telah mencapai tujuannya. Sebagai tambahan, COBIT juga menjaga keseimbangan antara kebutuhan stakeholder baik internal maupun eksternal.

2.ISO/IEC 38500

ISO/IEC 38500 merupakan standar yang memberikan prinsip umum mengenai peran dan manejemen IT governance dengan tanggungjawab bisnis (contoh : BoD dan tim manajemen). Dapat digunakan secara luas untuk semua jenis dan ukuran organisasi baik perusahaan privat maupun publik termasuk organisasi non profit.

Standar ini mendukung manajemen bisnis dalam melaksanakan supervisi terhadap organisasi TI dan membantunya memastikan bahwa TI memberikan dampak positif terhadap kinerja perusahaan. Di mana standart terdiri dari 6 prinsip, sebagai berikut :

1. *Responsibility*
2. *Strategy*
3. *Acquisition*
4. *Performance*
5. *Conformance*
6. *Human behaviour*

Selain itu ISO/IEC 38500 juga menjamin bahwa manajemen telah melaksanakan konformitas dengan implementasi tata kelola organisasi yang baik (*good overnance*).

PERSAMAAN :

1. Dijadikan sebagai IT governance framework
2. Memberikan pedoman pada perusahaan bahwa keputusan-keputusan strategic IT tidak hanya berada pada CIO saja tetapi juga pada direksi, komisaris dan pemegang-saham.

PERBEDAAN:

 COBIT adalah standard yang cakupan areanya adalah menengah ke bawah sedangkan ISO 38500 cakupan areanya adalah menengah ke atas.

 COBIT cocok jika dijadikan sebagai IT management framework sedangkan ISO 38500 cocok jika digunakan sebagai IT governance framework.

 Kerangka kerja COBIT memasukkan hal-hal berikut ini : Maturity Models , Critical Success Factors (CSFs), Key Goal Indicators (KGIs), dan Key Performance Indicators (KPIs).

 Kerangka kerja COBIT digunakan untuk mengelola infrastruktur teknologi dan informasi dalam suatu organisasi, dan bagaimana memberikan pelayanan yang terbaik bagi para pengguna teknologi informasi.

 Kerangka kerja ISO 38500 digunakan bagi pemerintahan untuk membantu mereka pada tingkat tertinggi dari organisasi untuk memahami dan memenuhi kewajiban hukum, peraturan, dan etika mereka dalam hal penggunaan organisasi mereka IT.

Nama : **Rahmad Kartolo**
NIS : **182420119**
Kelas :**MTI Reguler B**

UAS IT Risk Management
Pertanyaan:

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!

2. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

3. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi?
4. Jelaskan sumber penyebab ancaman terhadap IT ! Lengkapi penjelasan tersebut menggunakan contoh

5. Dalam Manajemen Resiko IT digunakan framework sebagai guide dalam pelaksanaannya. Jelaskan persamaan dan perbedaan dari framework-framework IT Risk Management yang ada? (at least membandingkan 2 framework, more is better)

---- Selamat bekerja ----

Pembahasan :

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!

- **Reverse social engineering (RSE)**

Reverse social engineering attack adalah cara untuk mendapatkan hak akses ke suatu sistem dengan cara meyakinkan korban bahwa jika korban punya masalah tertentu sekarang atau dimasa depan penyerang/hacker punya solusi dan siap membantu menyelesaikan masalah. .

Tehnik Reverse Social Engineering dilakukan dengan 3 tahap yaitu:

a. **Merusak** – hacker akan berusaha melakukan pengrusakan terhadap infrastruktur network yang ada sehingga kinerja system akan terganggu dan tidak berjalan sebagaimana

mestinya,secara otomatis pemilik system akan berusaha mencari informasi untuk memperbaiki hal ini.

b. **Menawarkan Bantuan-** Iklan bisa dikirim ke alamat email pemilik sistem yang sebelum nya sender nya sudah di spoof seolah-olah email berasal dari perusahaan security terpercaya, atau bisa dilakukan dengan memberikan kartunama sebelum serangan dimulai agar ketika hacker mengacaukan sistem si korban akan menghubungi si hacker yang sebelum nya memberikan kartunama /iklan dalam bentuk email

c. **Beraksi-**Setelah korban melihat iklan dan mengontak teknisi untuk perbaikan sistem (yang sebenarnya adalah si hacker itu sendiri) alih-alih membantu malah si hacker sudah mendapat akses penuh ke sistem dan bisa melakukan hal yang berbahaya seperti menanam backdoor ke sistem,mengambil data rahasia dll

- **PiggyBack Ride Attack**

Piggyback attack adalah Cara mendapatkan hak akses dengan menumpang seseorang yang memiliki akses /wewenang agar kita mendapat hak akses seperti halnya orang tersebut.

Contoh Piggyback ride attack

Saat kamu berjalan dibelakang orang yang memiliki akses ke sebuah gedung,begitu orang tersebut membuka pintu dengan security key yang dimilikinya kita ngikut masuk dibelakang nya.

contoh lain seperti ketika hujan lebat kita sengaja membawa banyak barang /membawa kotak di kiri dan kanan kemudian dengan sopan kita meminta tolong seseorang yang ada di sekitar yang memiliki akses untuk membukakan pintu dengan alasan security key yang kita miliki susah diambil karena ada di kantong /tas /lupa di taruh di dalam kotak .dll

- **Techie Talk (berbicara layaknya ahli)**

Kebanyakan hacker sangat mahir dalam hal teknis, ketika hacker akan meakukan social engineering maka si hacker dapat berbicara lancar seperti ahli soal komputer untuk mendapatkan kepercayaan dari si korban.

Contoh Techie Talk Attack

Ketika hacker berpura-pura dari bagian helpdesk dan memberitahukan kepada korban bahwa sistem telah diretas dan si korban harus mengganti password baru ,maka si hacker akan memandu korban nya untuk mengganti password dan menanyakan password apa yang akan digunakan untuk memastikan password yang dipilih korban aman.

- **Phishing Attack (Scamming)**

Phising Attack adalah tehnik untuk mendapatkan informasi sensitif(Data pribadi atau akun) dari korban dengan cara menulis email yang seolah-olah berasal dari website resmi.

Contoh Phising Attack

Biasanya hacker akan menulis email yang menganjurkan korban untuk meng update data akun dan mengganti password akun dengan dalih akun korban disalah gunakan orang. Korban akan diminta klik link menuju website mirip100% seperti aslinya dimana website tersebut sebenarnya palsu ayng dibuat oleh hacker itu sendiri.

- **Whalling Attack (Memancing Paus)**

whalling attack adalah jenis phising attack yang mengincar korban dengan jabatan tinggi di suatu perusahaan dengan tujuan untuk mendapatkan data rahasia perusahaan,dengan pertimbangan makin tinggi jabaran maka punya hak akses lengkap ke data perusahaan.

Contoh Whalling Attack

Hacker bisa mendapat informasi penting seperti kartu kredit dan data pribadi lain nya dengan cara menggali informasi yang dipajang korban secara online.

- **Vishing attack (Voice or VoIP Phishing attack)**

Gagal dengan tehnik phishing atau whaling ? cobalah dengan tehnik vishing , dimana dalam tehnik ini menggunakan telephone utnuk mendapatkan informasi dari si kotban.

hacker bisa berpura-pura menjadi karyawan bank dan memberitahukan bahwa kartu kreditnya ada masalah dan perlu mengupdate data-data lama dengan yang baru.

Dalam percakapan nya korban secara tidak sadar akan ditanyakan nomer CC dan pin serta identitas diri.

- **Social (Engineer) Networking**

Media social seperti facebook,twitter,instagram dll menjadi surga bagi social engineer, di sini sebagian besar orang mengexpose data pribadinya seperti tempat tanggal lahir ,hobi,tempat tinggal,relasi,dll .

Social engineer bisa mendapat kepercayaan dengan menjalin pertemanan dengan korban dan mendapatkan kepercayaan.

Setelah terjalin kepercayaan hacker bisa menyalahgunakan kepercayaan yang telah diberikan oleh korban untuk hal yang merugikan korban.

2. strategy yang dapat diterapkan untuk memanajemen resiko adlah sebagai berikut !

- ***Internal Environment and Objective Setting*** **(Lingkungan Internal dan Sasaran)**
  Agar dapat menerapkan *risk management* di perusahaan dengan baik, Anda harus memulai dari pengenalan lingkungan internal. Pahami definisi dari *manajemen* risiko dan berbagai istilah di dalamnya. Hal ini akan membantu Anda untuk melakukan penerapan *risk management* dengan lebih baik dan tepat. Setelah mengenal berbagai hal terkait *risk management*, selanjutnya yang perlu dilakukan adalah menentukan sasaran organisasi untuk mengidentifikasi risiko secara dini.

  Contohnya, suatu perusahaan memiliki dua tujuan dalam *risk management*, yaitu tujuan objektif untuk mewujudkan visi-misi dan tujuan aktivitas untuk melaksanakan operasional.

- ***Risk Identification*** **(Identifikasi Risiko)**
  Tahapan selanjutnya, penerapan *risk management* dilanjutkan pada dilakukannya identifikasi risiko dalam perusahaan. Beberapa kejadian yang potensial mengganggu strategi dan pencapaian tujuan yang disebutkan sebelumnya digolongkan sebagai risiko. Biasanya kejadian yang potensial menjadi risiko adalah kejadian yang memberikan dampak negatif pada operasional perusahaan. Tujuan perusahaan pun akan sulit tercapai. Setelah setiap kejadian yang mungkin menjadi risiko selesai diidentifikasi, maka Anda bisa melanjutkan ke langkah penerapan berikutnya untuk melakukan penilaian.

  Contohnya, ada beberapa kejadian tidak pasti di mana setiap 1 minggu sekali terjadi pemadaman listrik. Tentunya pemadaman listrik akan menyebabkan terhambatnya produksi usaha dan dikategorikan sebagai risiko.

- ***Risk Assessment*** **(Penilaian Risiko)**
  Beberapa kejadian yang potensial menjadi risiko pada perusahaan kemudian harus dilakukan penilaian. Penilaian merupakan tindakan yang dilakukan untuk menentukan seberapa besar dampak dari terjadinya kejadian ini. Misalkan suatu kejadian dalam daftar risiko terjadi di perusahaan Anda, apa saja efeknya bisa diketahui dengan melakukan analisis dalam dua perspektif. Perspektif analisis yang pertama adalah perspektif peluang risiko dan yang kedua perspektif efek risiko. Jadi analisis risiko tersebut seberapa besar peluangnya terjadi dan seberapa besar efeknya jika terjadi.

  Contohnya, risiko listrik padam yang berpeluang terjadi 1 minggu sekali dan efeknya yang cukup besar dalam hal produksi perusahaan.

- ***Risk Response*** **(Tanggapan Risiko)**
  Tahap berikutnya adalah memberikan tanggapan pada risiko yang sudah dinilai sebelumnya. Tanggapan yang dimaksud adalah sebuah sikap yang dibutuhkan dalam menghadapi risiko yang terjadi pada perusahaan. Tentu bisa dikatakan fokus utama dari *risk management* ada pada tahapan ini. Beberapa jenis tanggapan terhadap suatu risiko yang telah diidentifikasi dan dinilai adalah *avoidance* (hindari), *reduction* (kurangi), *sharing* (pindahkan), atau *acceptance* (terima).

  Misalnya untuk jenis risiko pemadaman listrik tadi, tanggapan yang dilakukan tentu adalah menerima.

- ***Control Activities*** **(Pengendalian Aktivitas)**
  Selain menentukan tanggapan dari suatu risiko, *risk management* juga memiliki tahapan untuk mengendalikan aktivitas pelaksanaannya. Tahapan ini menjadi tahapan yang memastikan bahwa semua prosedur dari *risk management* dilakukan sesuai dengan kebijakan yang diatur.

Contoh berbagai aktivitas pengendalian dalam suatu *risk management* adalah pembuatan kebijakan dan panduan pelaksanaan, pengamanan aset organisasi, pemberian wewenang dan pemisahan tugas, juga supervisi atasan. Semuanya akan memastikan bahwa aktivitas *risk management* telah dikendalikan dengan baik.

❖ ***Information and Communication*** **(Informasi dan Komunikasi)**

Tahap berikutnya adalah penyampaian informasi yang sesuai terkait *risk management* yang telah dilakukan ke berbagai pihak terkait. Penyampaian informasi ini dapat dilakukan dengan menggunakan berbagai jenis media komunikasi. Pada tahapan ini, harus dipastikan bahwa penyampaian informasi dan komunikasi dilakukan dengan jelas pastikan kualitasnya, arahnya, dan alat yang digunakannya. Semua informasi yang disampaikan kemudian akan digunakan pada tahapan terakhir *risk management* dalam perusahaan.

❖ ***Monitoring and Evaluation*** **(Pemantauan dan Evaluasi)**

Terakhir, jangan lupa untuk menggunakan semua informasi dan komunikasi yang didapatkan dari *risk management* sebagai bahan *monitoring* dan evaluasi. Monitoring adalah pemantauan yang dilakukan secara terus menerus untuk mengetahui apakah *risk management* sudah dilakukan sesuai dengan kebijakan dan prosedurnya. Selain *monitoring*, dilakukan juga evaluasi untuk mengetahui apakah ada kendala dan yang perlu diperbaiki dari *risk management* yang sudah dilakukan.

Demikian penjelasan mengenai cara menerapkan *risk management* serta contohnya dan manfaat penerapannya. Kini Anda sudah tahu bahwa penerapan *risk management* ternyata memiliki pengaruh yang sangat baik untuk perkembangan usaha. Khususnya dalam hal menghindari hal-hal yang tidak diinginkan dari proses berjalannya usaha.

3. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi

- **Teknologi yang lama saya ambil contoh dari**

HTTP

HTTP (*Hypertext Transfer Protocol*) adalah protokol jaringan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hypermedia

Pengertian lain dari HTTP adalah seperangkat aturan untuk mentransfer file (teks, gambar, suara, video, dan semua file multimedia lainya) di World Wide Web. Setelah pengguna web membuka browser web mereka, secara tidak langsung mereka menggunakan HTTP.

HTTP adalah protokol aplikasi yang berjalan di atas protokol TCP / IP dari protokol (protokol dasar untuk Internet).

Karena pada http tidak terdapat SSL/TLS untuk mengkrispi komunikasi antara web server dan web client

- **Teknologi yang baru**

HTTPS

HTTPS (*Hypertext Transfer Protocol Secure*) adalah versi aman dari HTTP yang dilapisi SSL/TLS, sebagai protokol komunikasi data di *World Wide Web*. Dengan protokol HTTPS memungkinan komunikasi data antara web klien dan web server terenkripsi. Port yang digunakan pada HTTPS adalah 443.

Sedangkan pada HTTPS terdapat SSL/TLS untuk mengkrispi komunikasi antara web server dan web client

4. Ancaman terhadap IT dapat dibagi menjadi dua macam: ancaman aktif dan ancaman pasif
   • **Ancaman aktif** mencakup kecurangan dan kejahatan terhadap komputer
   • **Ancaman pasif** mencakup kegagalan sistem, kesalahan manusia, dan bencana alam.

   ➢ **Ancaman Aktif**
   - Penyelewengan aktivitas
   - Kecurangan dan kejahatan computer
   - Pengaksesan oleh orang yang tidak berhak
   - Sabotase
   - Pemogram yang jahat/jahil

   Contoh: virus,torjan,cacing,bom waktu dll

   Ancaman lain berupa kecurangan dan kejahatan komputer. Ancaman ini mendasarkan pada komputer sebagai alat untuk melakukan tindakan yang tidak benar. Penggunaan sistem berbasis komputer terkadang menjadi rawan terhadap kecurangan (*fraud*) dan pencurian.

   ➢ **Ancaman Pasif**

   a. Kesalahan manusia(human Error)
   Contoh: kesalahan memasukan data & penghapusan data

   b. Kegagalan sistem = Kegagalan sistem menyatakan kegagalan dalam peralatan-peralatan komponen (misalnya *hard disk)*.
   Contoh: kerusakan dalam system

   c. Bencana alam dan politik
   Contoh: banjir,gempa bumi,kebakaran,perang dll.

   Gangguan listrik, kegagalan peralatan dan kegagalan fungsi perangkat lunak dapat menyebabkan data tidak konsisten, transaksi tidak lengkap atau bahkan data rusak, Selain itu, variasi tegangan listrik yang terlalu tajam dapat membuat peralatan terbakar.

5. Persamaan dan perbedaan dari framework-framework IT Risk Management yang ada?

   Disini perbandingan 3 Framework yaitu COSO,ERM dan COBIT

NO	Framework	Persamaan	Perbedaan
1	❖ **COSO (Committee of Sponsoring Organizations)**	• COSO dan ERM sama-sama merupakan framework untuk mengelola risiko dan sekaligus menentukan	• **COSO** **t**erdiri atas 5 komponen (*Control Environment, Risk Assessment, Control Activities, Monitoring,*

	❖ **ERM** ❖ **COBIT**	bagaimana opsi perlakuan yang tepat untuk setiap risiko, yang notabene merupakan tanggung jawab manajemen. • Esensi penerapan COSO dan ERM tidak terbatas pada industri tertentu, artinya dapat diterapkan pada berbagai jenis industri seperi industri keuangan, perbankan dan sebagainya. • COSO dan ERM dirancang untuk mencapai objektivitas organisasi sesuai	*Information & Communication*) sedangkan • **ERM** terdiri atas 8 komponen yang merupakan COSO + Internal Control ERM (*Internal Environment, Objective Setting (OS), Event Identification (EI), Risk Assessment (RA), Risk Response (RR), Control Activities, Information & Communication, Monitoring*). • **COBIT** Terdiri dari 6 komponen yaitu excecutive summary, framework, control objecktif, audit guidelines, management guidelines, control practise • **Stakeholder dari COSO** adalah eksekutif, dewan direksi, regulator, penyusun standar, organisasi profesi • **sedangkan stakeholder dari ERM** adalah direksi dan manajemen. • **sedangkan stakeholder dari COBIT** adalah manager • **Objektivitas COSO** terdiri atas 3 (*operations*, financial

		kebijakan manajemen. • Dalam proses evaluasi kinerja, COSO dan ERM sama-sama membutuhkan auditor internal untuk menilai implementasinya	reporting, dan compliance) sedangkan • **objektivitas ERM** terdiri atas 4 (*strategic, operations, reporting, compliance*). • **objektivitas COBIT** terdiri atas 4 (*Planing and Organization, acquisition and implementation, delivery and support, monitoring*). • **COSO** menekankan pada efektivitas dan efisiensi organisasi pada unit aktivitas sedangkan • **ERM** mempertimbangkan seluruh aktivitas pada semua level organisasi. • **COBIT** mempertimbangkan prosedur penerapan serta struktur organisasi.

IT Risk Management

Pertanyaan:

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!

2. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

3. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi?
4. Jelaskan sumber penyebab ancaman terhadap IT ! Lengkapi penjelasan tersebut menggunakan contoh

5. Dalam Manajemen Resiko IT digunakan framework sebagai guide dalam pelaksanaannya. Jelaskan persamaan dan perbedaan dari framework-framework IT Risk Management yang ada? (at least membandingkan 2 framework, more is better)

---- Selamat bekerja ----

1. Bating

Baiting menjadi salah satu metode yang digunakan oleh social engineering hacker dalam Mendapatkan informasi userid dan password dari pengguna tertentu. Metode ini memanfaatkan Rasa ingin tahu atau penasaran dari sang korban. Hacker dapat membujuk korban agar membuka Berbahaya dengan iming-iming yang menawarkan pengguna unduhan musik atau film gratis. Mereka Juga bisa membuat iklan software gratis yang mengarahkan korban ke situs jahat menfiring korban Untuk mengunduh aplikasi yang sudah terinfeksi malware.

2. Salah satu contoh kasus IT yang mengganggu operasional organisasi

Yang terjadi di RSUD Tebing Tinggi Kabupaten Empat Lawang adalah terjadinya kesalahan pemberianObat yang dikarenkan penulisan resep yang terbalik nama pasiennya. Pasien berasal dari poliklinik penyakit dalam yang merupakan paseien langganan itu sudah sering berobat ke RS. Pasien beranam Rafani membawa rese dengan nama saibani. Namun pasien tidak mengecek nama yang tercantumDalam resep dan langsung menuju apotek rawat jalan..

Pada saat pasien menyerahkan resep kepada petugas penerima resep, kemudian di cek sediaan, Kekuatan dan jenis sediaan, dikerjakan etiket dan pengemasan seusai dengan diperintahkan dalam resep. Setelah obat siap diserahkan pada pasien yang bernama saibani. Petugas memberikan konseling mengenai sediaan yang diterima pasien. Namun kemudian pasien sedikit curiga dengan penjelasan yang diberikan oleh petugas kepada beliau. Menurut pasie

bahwa obat yang digunakan tidak sesuai dengan kondisi penyakit yang di derita pasien.
Kesimpulannya, terjadi kesalahan pada penulisan nama pasien pada resep yang dibawa pasien.
Hal ini dimungkinkan dokter penulis resep kurang berkonsentrasi pada saat pelayanan atau nama
Pasien yang berdekatan pada saat pemeriksaan rekam medis terbalik pengamatanya.

3. Karena teknologi usang memiliki tingkat keamanan yang sudah ketinggalan zaman sehingga Banyak metode dalam membobol sistem keamanan teknologi yang sudah usang tersebut. Meskipun Teknologi tersebut adalah teknologi yang paling canggih pada zamannya, teknologi tersebut pasti Akan ada waktunya untuk menjadi ketinggalan zaman dan sistem keamanan nya akan lebih mudah Di bobol menggunakan teknik dan metode-metode yang lebih canggih.

4. Ada beberapa sumber penyebab bagi ancaman IT salah satu contohnya adalah

Cyber Espionage

Pada kejahatan cyber espionge ini merupakan kejahatan yang memanfaatkan jaringan internet Untuk melakukn kegitan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan Komputer (computer network system) pihak korban. Kejahatan ini biasanya ditujukan terhadap Saingan bisnis yang dokumen ataupu data pentingnya (database) tersimpan dalam suatu sistem yang Computerized (tersambung dalam jaringan).

5. ISO 31000 vs COSO

Perbedaan dianatara ISO 31000 dan COSO memiliki banyak perbedaan yang melebihi kesamaannya, Inilah mengapa banyak organisasi yang menggunakan kombinasi dari kedua standard tersebut. Dan Beberapa perbedaanya adalah :

- Structure

  Versi terakhir dari ISO 31000 lebih berstandar dibandingkan dangan COSO, ini sepertinya Dikarenakan ISO 31000 ini dikembangkan oleh organisasi yang berstandar internasional. Standar iso hanya memiliki 16 halaman dan dapat di baca kurang dari 1 jam. Sebaliknya COSO memiliki lebih dari 100 halaman. Bahkan COSO memiliki visual yang lebih Dan karakteristik ini tidak mengikuti struktural standar yang biasa.

- Geography

  ISO 31000 sudah di adaptasi sebagai standar risk management yang official oleh standar Organisasi nasional di dalam 57 negara di akhir tahun 2015. Ketikan mendevelop versi 2018, Organisasi internasional untuk standarisasi menerima lebih dari 5000 komen dari lebih dari 70 negara.

  Sebaliknya COSO, mendevelop partnership dengan PwC, salah satu dari the “Big Four” Perusahaan akunting dan konsulting. Hampir semua dari principal contributors untuk update 2017 berolokasi di washington, D.C. atau new york city.

- Target Audience

  Selagi COSO memiliki origin yang berofokus dalam menyediakan internal control framework , standar dari COSO ERM lebih bertargetkan kepada orang-orang akunting dan audit. Pada sisi yang lain ISO 31000 di buat bagi siapapun yang tertarik pada risk management. Banyak organisasi memilih bergantung kepada ISO 31000 dikarenakan banyaknya standar ISO yang lainnya yang mungkin akan mereka gunakan.

- Focus

  Mungkin lagi dikarenakan origin nya yang berbasic audit dan internal control, COSO lebih berfokus kepada tata kelokak peruahaan umum.

ISO berfokus hampir secaa eksklusif pada resiko dan menggabukan nya kedalam
Proses perencanaan. ISO 31000 juga menyediakan informasi yang lebih spesifik untuk
Membantu dalam menetapkan dan memenuhi tanggung jawab kesalahan resiko mereka.

- Framewok and Procesess

ISO menyediakan perbedaan yang jelas antara framework dan proses. Walaupu prosesnya
Termasuk masih sangat tradsional, tetapi prosesnya lebih detail kepada dasar dari
Identfikasi resiko, penilaian dan banyak lagi.

- Risk appetite

ISO memiliki original risk management standar yang di kelarkan di tahun 2009
Tidak membahas konsep dari risk apetite sama sekali. Di tahun 2018 hanya membahas
Secara singkat topic dari risk “crtiteria” tetapi hanya sebagian kecil dan penggunaan
Terminologi yang berbeda dari sumber lain.

Nama : Rio Permata
NIM : 182420108
Kelas : MTI Reguler B
Mata Kuliah : IT Risk Management & Disaster Recovery

1. Metode-metode yang digunakan Social Engineering Hacker untuk mendapatkan username dan password pengguna yaitu

   a. Phishing

   Phishing sendiri merupakan Bahasa slang dari Fishing yang artinya memancing.

   Lewat teknik memancing ini hacker akan menjebak dengan mengirimkan email atau alamat web palsu berisi link palsu atau berbahaya untuk mencuri informasi-informasi seperti username dan password

   Contohnya : Pada tahun 2001, terjadi kasus phishing E-Banking Klik BCA. Pelaku membuat berbagai domain yang kemungkinan pengguna salah mengetikkan, serta tampilan web yang sangat mirip Klik BCA. Pengguna yang menggunakan website palsu tersebut secara otomatis akan terjebak dan pelaku mampu mendapatkan username dan password dari pengguna.

   b. Pretexting

   Pada metode pretexting, hacker menggunakan scenario palsu untuk melakukan serangan menggunakan telpon atau email untuk mendapatkan informasi penting dari korban.

   Contohnya : Seseorang yang mengaku dari IT support perusahaan menelpon seorang *user* dan menjelaskan bahwa ia sedang mencari kerusakan jaringan. Dia telah berhasil mengatasi bahwa kerusakan itu terjadi pada departemen tempat *user* itu berada tetapi ia memerlukan *user ID* dan *password* dari departemen itu untuk menyelesaikan masalah

   c. Baiting

   Serangan baiting mirip dengan serangan Phising namun yang membedakannya adalah serangan ini menawarkan umpan berupa barang kepada pengguna.

   Contohnya : Hacker berupaya membuat korban mengklik tautan berbahaya dengan iming-iming download film, musik dan software. Mereka juga bisa membuat iklan

software gratis yang mengarahkan korban ke situs jahat dan mendorong korban untuk mengunduh aplikasi yang sudah terinfeksi malware.

2. Strategi yang diterapkan dalam managemen resiko IT :

   a. Identifikasi proses dan asset IT.

   Melakukan identifikasi seluruh asset IT yang mendukung layanan IT. Contohnya data, hardware, software, CCTV dan lain-lain.

   b. Identifikasi Risiko

   Selanjutnya adalah mengidentifikasi jenis-jenis ancaman dan kerentanan dari asset IT serta dampaknya jika ancaman itu terjadi.

   c. Analisis Risiko

   Dampak yang telah diidentifikasi kemudian dianalisis dan diukur. Hasil pengukuran dampak akan memunculkan nilai resiko

   d. Mengevaluasi Kontrol

   Tahap ini mengidentifikasi control pengamanan layanan IT yang telah ada baik berupa kebijakan, prosedur, hardware, software dan mengevaluasi control tersebut untuk mengurangi kelemahan dan dampak sehingga dapat menurunkan nilai risiko.

   e. Mengukur Nilai Risiko Sisa

   Pada tahap ini mengukur nilai risiko yang masih ada atau yang tersisa setelah penerapan control terhadap asset IT.

   f. Evaluasi Penerimaan Risiko

   Tahap ini memeriksa apakah risiko yang tersisa dapat diterima sesuai dengan kriteria yang telah ditetapkan.

   g. Menetapkan Risk Treatment Plan (RTP)

   Jika risiko sisa diterima maka dilakukan pemantauan berkala untuk memeriksa kemungkinan perubahan risiko karena factor internal maupun eksternal. Tapi jika risiko sisa tidak diterima, maka perlu dilakukan perbaikan atau penambahan control baru agar nilai risiko sisa berada pada tingkat yang dapat diterima.

   h. Memantau dan Mereview Risiko

   Pada tahap ini akan dilakukan pemantauan pelaksanaan RTP dan mereview risiko lain yang ada dan belum diidentifikasi sebelumnya.

3. Teknologi yang sudah usang akan rentan menjadi ancaman bagi keamanan teknologi, hal ini dikarenakan teknologi yang sudah out of date tidak dapat lagi mensupport system dari teknologi yang ada sekarang.

   Sebagai contoh Windows sudah mengumumkan bagi para pengguna untuk tidak menggunakan Windows XP lagi karena sudah sangat rentan akan berbagai masalah compatible dan keamanan. Contoh lain softare antivirus yang telah usang harus selalu di update agar antivirus itu dapat berfungsi dengan baik dan mengenali berbagai macam virus-virus baru.

4. Sumber ancaman IT :
   a. **Ancaman dari luar**

      Yaitu potensi ancaman IT yang mungkin muncul dan berasal dari luar. Contohnya : virus, spam, scams, phishing

   b. **Ancaman dari dalam**

      Yaitu potensi ancaman IT yang penyebabnya dari dalam. Contohnya : Kelalaian staf dalam menggunakan system (human error)

   c. **Ancaman Fisik**

      Yaitu ancaman yang timbul dari pencurian data fisik. Contohnya : pencurian server.

   d. **Ancaman Lingkungan**

      Ancaman yang muncul dari berbagai gejala lingkungan/alam. Contohnya : banjir, kebakaran.

5. Perbandingan framework COSO ERM, ISO 31000, dan NIST SP 800-30

Perbedaan	**COSO ERM**	**ISO 31000**	**NIST SP 800 - 30**
Definisi resiko	“Kemungkinan terjadinya sebuah event yang dapat mempengaruhi pencapaian sasaran entitas.” Menurut Grant Purdy, seorang praktisi	“Efek dari ketidakpastian terhadap pencapaian sasaran organisasi.”	“Suatu ketidakpastian dimasa yang akan datang tentang kerugian yang harus dipikul sbuah organisasi”

	manajemen risiko veteran di Melbourne, definisi ini gagal menangkap potensi risiko yang dapat muncul akibat perubahan kondisi yang terjadi secara perlahan.		
Definisi manajemen resiko	"Proses yang dipengaruhi oleh Board of Directors, manajemen, dan personil lain dalam entitas, diaplikasikan pada pembentukan strategi dan pada seluruh bagian perusahaan, dirancang untuk mengidentifikasi kejadian potensial yang dapat mempengaruhi entitas, dan mengelola risiko selaras dengan risk appetite entitas, untuk menyediakan jaminan yang wajar terhadap pencapaian sasaran dari entitas."	"Aktivitas-aktivitas terkoordinasi yang dilakukan dalam rangka mengelola dan mengontrol sebuah organisasi terkait dengan risiko yang dihadapinya."	"Proses yang memungkinkan pemimpin organisasi untuk dapat menyeimbangkan biaya operasional dan ekonomi yang dikeluarkan untuk mengurangi resiko dan mencapai keuntungan dengan melindungi sistem teknologi informasi dan data yang mendukung misi atau tujuan organisasi."
Komponen manajemen resiko	Proses dan kerangka kerja manajemen risiko tidak dipaparkan secara terpisah. Menurut Grant Purdy hal ini dapat menimbulkan	Memaparkan kerangka kerja dan proses manajemen risiko secara terpisah. ISO 31000: 2009 juga menyediakan prinsip	

	kebingungan dan inefektivitas terhadap manajemen risiko, dimana kerangka kerja seharusnya dirancang pada top level management, sedangkan proses manajemen risiko seharusnya diterapkan pada proses-proses organisasi. Standar ini menekankan pada pengembangan pengendalian internal sebagai upaya perusahaan dalam mengelola risiko.	manajemen risiko yang harus diterapkan dalam kerangka kerja dan proses untuk mendukung efektivitas manajemen risiko. Standar ini menekankan penerapan manajemen risiko sebagai alat penciptaan dan pelindung nilai organisasi.	
Awal proses manajemen resiko	Dimulai dengan menetapkan sasaran perusahaan yang terdiri dari empat kategori yaitu strategis, operasi, pelaporan, dan pemenuhan.	Dimulai dengan membangun konteks untuk mengidentifikasi kondisi internal, kondisi eksternal, konteks manajemen risiko, dan kriteria risiko.	Dimulai dengan menentukan ruang lingkup usaha.
Identifikasi konteks eksternal	Sedikit dilakukan	Dilakukan secara menyeluruh	
Komponen proses	Terdiri dari 8 komponen, yaitu:	Terdiri dari lima komponen besar, yaitu:	Terdiri dari 3 komponen yaitu: Karakterisasi sistem

manajemen resiko	Identifikasi lingkungan internal; Penetapan sasaran manajemen risiko; Identifikasi kejadian; Penilaian risiko, perlakuan risiko; Aktivitas pengendalian; Informasi dan komunikasi; Pemantauan.	Komunikasi dan konsultasi; Membangun konteks; Penilaian risiko; Perlakuan risiko; Monitoring dan review.	Identifikasi ancaman Identifikasi kerentanan Analisis pengendalian Penentuan kemungkinan Analisis dampak Penentuan resiko Rekomendasi kontrol Dokumentasi hasil
Pengertian inherent risk	Inherent risk diartikan sebagai eksposur perusahaan terhadap risiko secara utuh. (dampak dari existing control tidak diperhitungkan)	Inherent risk diartikan sebagai eksposur perusahaan terhadap risiko setelah dilakukan pengendalian internal.	
Prinsip manajeman resiko	Tidak ada	Tersedia dan menjadi hal yang harus diterapkan pada kerangka kerja dan proses manajemen risiko untuk mendukung efektivitas penerapan manajemen risiko.	
Perbaikan berkelanjutan	Perbaikan hanya dilakukan apabila	Memfasilitasi perbaikan	

	diperlukan, berdasarkan hasil pemantauan.	berkelanjutan pada keseluruhan kerangka kerja dan proses manajemen risiko, sesuai dengan kebutuhan organisasi dan perkembangan konteks.	
Penyaluran informasi	Informasi hanya dikomunikasikan kepada pelaku manajemen risiko untuk mendukung pencapaian sasaran unit-unit tersebut. Keterlibatan stakeholders eksternal tidak diungkapkan pada standar ini.	Informasi mengenai risiko dan manajemen risiko dikomunikasikan dan dikonsultasikan dengan seluruh stakeholders perusahaan, baik internal maupun eksternal (sesuai prinsip “transparan dan inklusif”). Keterlibatan stakeholders diperlukan untuk mengidentifikasi kepentingan seluruh pihak agar menjadi bahan pertimbangan pengambilan keputusan.	
Aspek manusia dan budaya	Aspek manusia disebutkan sebagai	Memperhitungkan aspek manusia dan	

	batasan dari manajemen risiko dalam memberikan jaminan terhadap pencapaian sasaran organisasi.	budaya ke dalam manajemen risiko (prinsip "mempertimbangkan faktor budaya dan manusia"). Penerapan manajemen risiko turut mempertimbangkan kultur, persepsi, dan kapabilitas manusia, termasuk memperhitungkan perselisihan kepentingan antara organisasi dengan individu di dalamnya.	

IT Risk Management

Pertanyaan:

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!

2. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

3. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi?
4. Jelaskan sumber penyebab ancaman terhadap IT ! Lengkapi penjelasan tersebut menggunakan contoh

5. Dalam Manajemen Resiko IT digunakan framework sebagai guide dalam pelaksanaannya. Jelaskan persamaan dan perbedaan dari framework-framework IT Risk Management yang ada? (at least membandingkan 2 framework, more is better)

---- Selamat bekerja ----

JAWABAN..

1. **Whalling Attack (Memancing Paus)-** whalling attack adalah jenis phising attack yang mengincar korban dengan jabatan tinggai di suatu perusahaan dengan tujuan untuk mendapatkan data rahasia perusahaan,dengan pertimbangan makin tinggi jabaran maka punya hak akses lengkap ke data perusahaan.

   Contoh WhallingAttack

   Hacker bisa mendapat informasi penting seperti kartu kredit dan data pribadi lain nya dengan cara menggali informasi yang dipajang korban secara online.

   Semisal di dalam facebook page nya tertulis bahwa korban alumni universitas A dengan hobby golf, maka si hacker bisa membuat scam email yang seolah-olah resmi dikirim dari universitas A yang isinya ajakan untuk mengikuti turnamen golf antar alumni danmeminta untuk mengisi formulir yang telah disediakan sebagai syarat mengikuti turnamen tersebut.

Nah formulir yang disediakan adalah data pribadi yang harus diisi , dengan mengumpulkan data pribadi sepotong demi sepotong,si hacker bisa mendapat 100% data pribadi dari korban.

2. Strategy yang diterapkan.

1). Planning dalam manajemen keamanan informasi meliputi proses perancangan, pembuatan, dan implementasi strategi untuk mencapai tujuan. Ada tiga tahapannya yaitu:

a) *strategic planning* yang dilakukan oleh tingkatan tertinggi dalam organisasi untuk periode yang lama, biasanya lima tahunan atau lebih,

b) *tactical planning* memfokuskan diri pada pembuatan perencanaan dan mengintegrasi sumberdaya organisasi pada tingkat yang lebih rendah dalam periode yang lebih singkat, misalnya satu atau dua tahunan,

c) *operational planning* memfokuskan diri pada kinerja harian organisasi. Sebagi tambahannya, planning dalam manajemen keamanan informasi adalah aktifitas yang dibutuhkan untuk mendukung perancangan, pembuatan, dan implementasi strategi keamanan informasi supaya diterapkan dalam lingkungan teknologi informasi.

2). Policy

Dalam keamanan informasi, ada tiga kategori umum dari kebijakan yaitu:

a). Enterprise Information Security Policy (EISP) menentukan kebijakan departemen keamanan informasi dan menciptakan kondisi keamanan informasi di setiap bagian organisasi.

b). *Issue Spesific Security Policy (ISSP)* adalah sebuah peraturan yang menjelaskan perilaku yang dapat diterima dan tidak dapat diterima dari segi keamanan informasi pada setiap teknologi yang digunakan, misalnya e-mail atau penggunaan internet.

c). *System Spesific Policy (SSP)* pengendali konfigurasi penggunaan perangkat atau teknologi secara teknis atau manajerial.

3). Programs

Adalah operasi-operasi dalam keamanan informasi yang secara khusus diatur dalam beberapa bagian. Salah satu contohnya adalah program security education training

and awareness. Program ini bertujuan untuk memberikan pengetahuan kepada pekerja mengenai keamanan informasi dan meningkatkan pemahaman keamanan informasi pekerja sehingga dicapai peningkatan keamanan informasi organisasi.

4). Protection

Fungsi proteksi dilaksanakan melalui serangkaian aktifitas manajemen resiko, meliputi perkiraan resiko (*risk assessment*) dan pengendali, termasuk mekanisme proteksi, teknologi proteksi dan perangkat proteksi baik perangkat keras maupun perangkat keras. Setiap mekanisme merupakan aplikasi dari aspek-aspek dalam rencana keamanan informasi.

5). People

Manusia adalah penghubung utama dalam program keamanan informasi. Penting sekali mengenali aturan krusial yang dilakukan oleh pekerja dalam program keamanan informasi. Aspek ini meliputi personil keamanan dan keamanan personil dalam organisasi.

3. Karena teknologi yang sudah usang sangat rentan terhadap kerusakan dan memudahkan orang untuk menyalah gunakan data dan informasi yang ada didalam teknologi yang usang tersebut .

4. Sumber penyebab ancaman terhadap IT dan contohnya.
   1. Operating System attacks (Ex: seperti penggunaan windows palsu, OS Windows jarang di update)
   2. Application –level attacks (Ex: download file dari situs yang tidak terpercaya, menginstal program yang asal usul programnya tidak diketahui, penggunaan crack untuk register program).
   3. Shrink wrap kode attacks (Ex: adanya aplikasi keylogger pada computer warnet).
   4. isconfiguration attacks (Ex: Kecepatan internet yang menurun / lambat ketika download, pembatasan penggunaan internet di kantor, auto update suatu program)

5. perbandingan Framework Cobit 5 dan Iso 27002

   a.) COBIT (*Control Objectives for Information and related Technology*) adalah sebuah framework bisnis yang digunakan untuk tata kelola perusahaan IT.

   b.) Seperangkat standar an procedure dengan keamanan dan control informasi bisnis untuk menerapkam keamanan yang tepat.

PERBANDINGAN COBIT DAN ISO 27002
Kelebihan cobit

a.) Berhubungan dengan informasi yang relevan dan berkenaan dengan proses bisnis, dan sebaik mungkin informasi dikirim tepat waktu, benar, konsisten, dan berguna.
b.) Proteksi terhadap informasi yang sensitif dari akses yang tidak bertanggung jawab.

Kelebihan Iso 27002
a.) Menyediakan pendekatan untuk implementasi kebijakan control.
b.) Mendorong pengurangan biaya dengan pencegahan insiden keamanan informasi
c.) Organisasi yang lebih baik dengan proses dan mekanisme yang dirancang dan dikelola dengan baik

Spesesifikasi
1. COBIT
a.) tata kelola perusahaan terintegrasi secara keseluruhan
b.) Merencanakan, membangun, menjalankan dan mengawasi aktifitas perusahaan selaras dengan arah yang telah ditetapkan oleh badan governance.
2. ISO 27002
a.) sumber daya keamanan
b.) Keamanan informasi untuk organisasi
c.) Aspek keamanan informasi manajemen kesinambungan bisnis

Nama : Caesario Rian Saputra

NIM : 182420131

IT Risk Management

Pertanyaan:

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!

2. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

3. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi?
4. Jelaskan sumber penyebab ancaman terhadap IT ! Lengkapi penjelasan tersebut menggunakan contoh

5. Dalam Manajemen Resiko IT digunakan framework sebagai guide dalam pelaksanaannya. Jelaskan persamaan dan perbedaan dari framework-framework IT Risk Management yang ada? (at least membandingkan 2 framework, more is better)

---- Selamat bekerja ----

1. **Phising :** Phising adalah suatu metode yang di gunakan hacker untuk mencuri password dengan cara mengelabui target menggunakan fake form login pada situs palsu yang menyerupai situs aslinya. pada beberapa kasus, situs palsu tersebut tidak terlalu mirip namun karena target kurang berhati hati dan tidak punya pengalaman tentang metode phishing maka bisa saja terjebak.

   Contoh kasus : Phising Westpac Banking pelanggan internet banking milik Westpac Banking Corporation, sebuah bank senior di Australia. Modusnya adalah mengirimkan email spam yang berisi seakan-akan situs internet banking mereka akan melakukan upgrade software sistem, sehingga calon korban diminta meng-klik link yang tersedia dalam email tersebut dengan dalih mempermudah akses agar tidak perlu mengetik sendiri alamat yang harus dituju. User yang ceroboh tentunya akan langsung klik saja link yang disediakan, padahal secara tidak sadar link itu tidaklah menuju situs yang dibicarakan, melainkan ke situs jebakan milik penjebak, hanya saja tampilannya situs palsu itu sangat mirip dengan yang asli.

2. Mengingat seriusnya resiko keamanan aset teknologi informasi dan komunikasi management resiko maka akan diterapkan strategi menggunakan Risk reduction (mengurangi/mitigasi kemungkinan dampak resiko.

Contoh kasus : kemungkinan resiko pada Rumah Sakit Pusri Palembang

It Rosources

I. Application :
   - Peretasa Aplikasi
   - Aplikasi Crash (Down)
   - Aplikasi Diserang virus
   - Lemahnya Maintenance Aplikasi

II. Information :
   - Hilangnya data Terkini
   - Database Rusak/eror
   - Penyalahgunaan/pencurian data

III. Infrastructure :
   - Kerusakan Hardware
   - Server Diserang virus
   - Koneksi Jaringan Putus/rusak
   - Kegagalan sistem operasi
   - Bencana Alam

IV. People :
   - Penyalahgunaan Kedudukan
   - Melemahnya Loyalitas SDM
   - Pembeberan data dan informasi Rahasia

Program Penangan Resiko

No	IT Resources	Identifikasi Risiko	Program Penanganan Risiko
1	*Application*	1. Peretasan Aplikasi	Perbaikan sistem aplikasi melalui *update patch* dan penerapan sistem *firewall* disertai dengan peningkatan sistem keamanan (*security*)
		2. Aplikasi *crash* (*down*)	Perbaikan sistem aplikasi melalui *update patch* dan pencegahan instalasi aplikasi lain yang bisa menyebabkan aplikasi utama *crash*
		3. Aplikasi diserang virus	Review kinerja antivirus untuk komputer *client*, baik *update* antivirus maupun scan antivirus secara periodik
		4. Lemahnya *maintenance* aplikasi	Sementara aplikasi sedang dalam proses *maintenance* jangan sampai mengganggu sistem pelayanan terhadap pengguna data Lakukan *maintenance* pada *non-busy hour* atau gunakan mekanisme aplikasi cadangan
2	*Information*	5. Hilangnya data terkini	Data harus senantiasa memiliki backup melalui mekanisme syncronizing secara otomatis. Sehingga kehilangan data pada satu periode waktu tidak akan menjadi alasan bagi sitem untuk berhenti bekerja

		6. *Database* rusak/error	Database harus senantiasa memiliki backup melalui mekanisme mirroring dan lokasi *backup database* diterapkan pada beberapa lokasi *device*. Kerusakan *database* tidak akan menjadi alasan bagi sitem untuk berhenti bekerja
		7. Penyalahgunaan/pencurian data	Review manajemen puncak dalam hal mekanisme *security* data
3	*Infrastructure*	8. Kerusakan *hardware*	Review kinerja tim pemeriksaan fisik, perbaiki bila memungkinkan jika tidak segera lakukan penggantian
		9. *Server* diserang virus	Review kinerja antivirus, lakukan pembersihan (*scan*) secara periodik
		10. Koneksi jaringan putus/rusak	Review kinerja jaringan dengan pihak penyedia jaringan. Lakukan monitoring sistem dan kinerja jaringan secara periodik, baik instalasi jaringan maupun *bandwith*
		11. Kegagalan sistem operasi	Review kinerja tim pengelola sistem operasi dan *software*, lakukan perbaikan sesegera mungkin
		12. Bencana Alam	Usahakan memiliki lokasi penyimpanan *backup* yang memiliki risiko terkena bencana alam yang lebih kecil dibandingkan lokasi penyimpanan data utama.
			Terapkan mekanisme Disaster Recovery Planning (DRP) untuk mengantisipasi kerusakan infrastruktur TI dikarenakan bencana alam
4	*People*	13. Penyalahgunaan kedudukan	Sosialisasikan penerapan sanksi berat kepada setiap pegawai yang menyalahgunakan wewenang dan kedudukan. Berikan sanksi pada pegawai yang bersangkutan. Review manajemen puncak terhadap *fit and proper test* jabatan.
		14. Melemahnya loyalitas SDM	Review manajemen puncak terhadap tata kelola SDM Pengkajian kesesuaian hak dan kewajiban pegawai
		15. Pembeberan data dan informasi rahasia	Sosialisasikan penerapan sanksi berat kepada setiap pegawai yang melakukan pembeberan data dan informasi rahasia Berikan sanksi pada pegawai yang bersangkutan. Review manajemen puncak terhadap penilaian dan penempatan pegawai.

3. Teknologi yang usang dapat menjadi ancaman keamanan bukan saja ancaman, teknologi yang usang dapat membuat proses bisnis terhenti karna menurunnya performa teknologi informasi. Perangkat dan sistem butuh perkembangan menyesuaikan dengan kebutuhan dan kapasitas pengguna sebagai contoh perangkat mulai dari core,distribution sampai ke access standarnya dalam 5 tahun mengalami low performance dan kebutuhan access user yang berlebihan dapat membuat perangkat overload maka dari itu perlu peremajaan perangkat diperlukan untuk menjaga kestabilan proses bisnis, begitupun pada sistem license yang mati dan teknologi terbaru harus diikuti karna ancaman cyber bisa saja terjadi dari celah yang ditimbulkan oleh sistem yang usang.

4. Beberapa sumber penyebab ancaman terhadap IT diantarany
    1. Sumber ancaman yang berasal dari luar
       Kejahatan yang dilakukan dengan menyusup kedalam sistem jaringan komputer tanpa sepengetahuan dari pemilik sistem jaringan komputer. Contohnya : seorang pelaku kejahatan atau hacker melakukan sabotase terhadap informasi yang sangat penting atau mencuri informasi yang sangat penting dan rahasia.
    2. Sumber ancaman yang berasal dari dalam
       Kejahatan yg dilakukan karna ketidak sengajaan atau tidak pahamny user sehingga masuknya virus yang menyebabkan masalah dalam teknologi informasi. Contoh : user mendownload sebuah pesan dari email atau dari situs fake sehingga virus malware masuk dan menyebar dalam jaringan.

5. Persamaan dan perbedaan framework COBIT,ITIL, dan ISO 38500

   PERBEDAAN :
   - COBIT dan ITIL adalah standard yang cakupan areanya adalah menengah ke bawah
   - ISO 38500 cakupan areanya adalah menengah ke atas
   - COBIT dan ITIL cocok jika dijadikan sebagai IT management framework
   - ISO 38500 cocok jika digunakan sebagai IT governance framework.
   - Kerangka kerja COBIT memasukkan hal-hal berikut ini : (1) Maturity Models , (2) Critical Success Factors (CSFs), (3) Key Goal Indicators (KGIs), dan (4) Key Performance Indicators (KPIs).
   - Kerangka kerja yang digunakan untuk mengelola infrastruktur teknologi dan informasi dalam suatu organisasi, dan bagaimana memberikan pelayanan yang terbaik bagi para pengguna teknologi informasi.
   - Kerangka kerja digunakan bagi pemerintahan untuk membantu mereka pada tingkat tertinggi dari organisasi untuk memahami dan memenuhi kewajiban hukum, peraturan, dan etika mereka dalam hal penggunaan organisasi mereka ‘IT.

   PERSAMAAN :
   - Dijadikan sebagai IT governance framework
   - memberikan pedoman pada perusahaan bahwa keputusan-keputusan strategic IT tidak hanya berada pada CIO saja tetapi juga pada direksi, komisaris dan pemegang-saham

Nama : Dhea Noranita Putri

Nim : 182420112

Tugas : IT RISK MANAGEMENT

SOAL :

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!

2. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.

3. Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

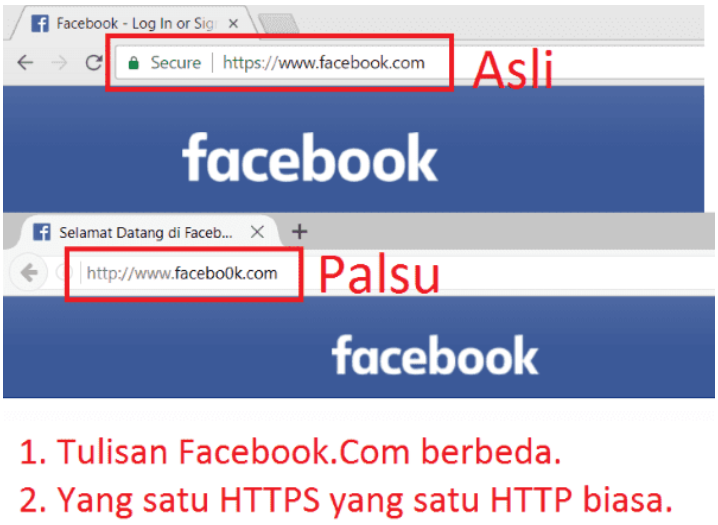
4. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi?

5. Jelaskan sumber penyebab ancaman terhadap IT ! Lengkapi penjelasan tersebut menggunakan contoh

6. Dalam Manajemen Resiko IT digunakan framework sebagai guide dalam pelaksanaannya. Jelaskan persamaan dan perbedaan dari framework-framework IT Risk Management yang ada? (at least membandingkan 2 framework, more is better)

Jawab :

1. Saya akan menjelaskan salah satu metode hacker untuk mendapatkan username dan password seseorang. Metode tersebut adalah metode phissing. Phising adalah suatu metode untuk melakukan penipuan dengan mengelabui target dengan maksud untuk mencuri akun target. Istilah ini berasal dari kata "fishing" = "memancing" korban untuk terperangkap dijebakannya. Phising bisa dikatakan mencuri informasi penting dengan mengambil alih akun korban. Phising biasanya sering digunakan pada email, dimana penyebaran melalui email ini dilakukan untuk memberikan informasi yang mengarah ke halaman palsu untuk maksud menjebak korban. Untuk menghindari phising, pengguna harus lebih berhati-hati dengan memperhatikan beberapa hal keamanan. Sebagai contoh, jika Anda mengakses suatu halaman website, maka pastikan anda berada di halaman website dengan url domain yang benar. Misalnya, untuk login facebook pastikan anda mengakses halaman https://facebook.com/ bukan halaman selain itu. Pada gambar 1 merupakan contoh halaman facebook yang palsu.



Gambar 1

Pada gambar diatas terlihat ada 2 halaman facebook, sekilas Nampak tidak ada perbedaan dari kedua halaman tersebut. Namun jika diperhatikan terlihat perbedaannya. Maka dari itu kita harus lebih teliti sebelum melakukan login akun.

2. Resiko yang biasa muncul pada lingkungan IT dan cara mengatasinya. Kasus serangan wannacry di Indonesia terbesar kedua di dunia.mengutip dari berita https://inet.detik.com/, serangan WannaCry sampai membuat perusahaan

otomotif Honda sampai menyetop produksi di pabrik kendaraannya selama sehari. Di Indonesia, Menteri Komunikasi dan Informatika (Menkominfo) Rudiantara kala itu mengatakan bahwa ada ribuan alamat IP di Indonesia yang terjangkit WannaCry.Salah satu contoh adalah dua rumah sakit di wilayah Jakarta disebut kena serangan ransomware ini. Serangan Wanna Cry ini bikin pelayanan kedua rumah sakit tersendat.

Berdasarkan penelitian, Avast telah memblok 54 juta serangan selama bulan Maret kemarin. Di Indonesia sendiri Avast telah berhasil memblok 17 juta lebih serangan WannaCry selama periode terhitung dari tanggal 5 Desember 2017 sampai 4 Januari 2018. Angka tersebut membuat Indonesia menjadi negara dengan serangan WannaCry terbesar di dunia setelah Rusia.

Mengingat hal tersebut, kita pasti cenderung berasumsi bahwa pengguna PC pribadi dan perusahaan-perusahaan aman dan telah memperbarui sistem mereka. Sayangnya, Avast mengungkapkan bahwa hampir sepertiga (29%) komputer berbasis Windows di seluruh dunia masih rentan terhadap serangan WannaCry yang disebabkan oleh beberapa faktor utama, yaitu ransomware mengeksploitasi kerentanan yang terdapat di banyak PC yang menggunakan sistem operasi lama dan tidak pernah melakukan update.Sebagian besar sistem operasi lama sudah tidak didukung pembaruan (update) dan karena itu rentan terhadap serangan malware; kemudian, WannaCry tidak memerlukan interaksi dari pengguna untuk menyebarkan diri karena diprogram sebagai worm. Maka dari itu melakukan update pada sistem operasi dan melakukan backup data merupakan hal yang penting untuk melindungi data perusahaan.

3. Strategi untuk memanajemen resiko, Untuk keamanan penggunaan Komputer di Indonesia, Kementerian Komunikasi dan Informatika menegaskan pentingnya semua Orang baik individu, perusahaan, kementerian, lembaga serta organisasi lainnya melakukan antisipasi dan pencegahan dari serangan malware WannaCry. #1. Lakukan Update security pada windows anda dengan install Patch MS17-010 yang dikeluarkan oleh microsoct. Lihat : https://technet.microsoft.com/en-us/library/security/ms17-010.aspx. Updating sebaiknya dilakukan dengan cara mengambil file patch secara download menggunakan komputer biasa, bukan komputer yang berperan penting.#2. Lakukan update AntiVirus. Contoh AV : Kapersky Total Security, Eset, Panda, Symantec yang bisa download versi trial untuk 30 hari gratis dengan fungsi atau fitur penuh dan update. Pastikan AV meliputi ANTI RANSOMWARE. #3. Non aktifkan fungsi SMB (Server Message Block) dan jangan mengaktifkan fungsi macros #4. Block Ports : 139/445 & 3389

4. teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi, pada kasus seranggan wannacry disebabkan oleh beberapa faktor utama, yaitu ransomware mengeksploitasi kerentanan yang terdapat di banyak PC yang menggunakan sistem operasi lama dan tidak pernah

melakukan update.Sebagian besar sistem operasi lama sudah tidak didukung pembaruan (update) dan karena itu rentan terhadap serangan malware; kemudian, WannaCry tidak memerlukan interaksi dari pengguna untuk menyebarkan diri karena diprogram sebagai worm.

5. Sumber penyebab ancaman it, salah satu contoh ancaman yang akhir-akhir ini menjadi perdebatan adalah trend bring your own device (BYOD). BYOD Adalah fenomena tren karyawan membawa perangkat eletronik mereka sendiri seperti laptop, handphone, tablet dan perangkat lain untuk bekerja dan terhubung dengan jaringan perusahaan. terdapat sisi negative dari fenomena ini, seperti meningkatnya celah pada keamanan sistem pada perusahaan yang mungkin bisa dimanfaatkan oleh pihak – pihak yang tidak bertanggung jawab. Maka dari itu dilakukan kebijakan agar ancaman tersebut dapat dicegah dan diatasi.

6. Framework yang baik bagi organisasi di Indonesia, standar ISO 31000:2009 layak untuk menjadi alternatif pilihan utama. dikarnakan Standar tersebut telah diadopsi oleh Badan Standarisasi Nasional (BSN) Indonesia. ISO 31000:2009 merupakan sebuah standar internasional yang disusun dengan tujuan memberikan prinsip dan panduan generik untuk penerapan manajemen risiko. standar ISO 31000: 2009 menyediakan tiga unsur utama sebagai arsitektur manajemen risiko yaitu berupa prinsip-prinsip, kerangka kerja, dan proses manajemen risiko. Selain ISO 31000 : 2009 ada framework lain yaitu Committee of Sponsoring Organizations of the Treadway Commission (COSO). Dalam kerangka manajemen risikonya, COSO ERM menuntut perusahaan untuk dapat menentukan terlebih dahulu sasaran perusahaannya, yang terdiri dari empat kategori yaitu:
   1. Strategis: sasaran yang mendukung dan selaras dengan misi perusahaan.
   2. Operasi: efektivitas dan efisiensi dari penggunaan sumber daya perusahaan.
   3. Pelaporan: keterpercayaan dari pelaporan.
   4. Pemenuhan: pemenuhan terhadap hukum dan regulasi yang berlaku.

   Menurut https://crmsindonesia.org/ Perbandingan pada kedua framework ini membawa keunggulan dan kelemahan tersendiri pada COSO ERM – Integrated Framework dan ISO 31000: 2009 Risk Management – Principles and Guidelines, standar ISO 31000: 2009 memiliki keunggulan esensial dalam memberikan panduan yang lebih mendetail dan komprehensif. Keberadaan prinsip manajemen risiko, penetapan konteks eksternal, dan pemisahan antara kerangka kerja dengan proses manajemen risiko menjadi keunggulan kompetitif yang dimiliki oleh ISO 31000: 2009. Fakta bahwa standar ISO 31000: 2009 telah diakui dan diadaptasi sebagai standar manajemen risiko di hingga 40 negara juga menunjukkan bahwa ISO 31000: 2009 telah bertahan dari uji kelayakan oleh berbagai negara. Namun pada akhirnya, dalam memilih standar terbaik untuk diimplementasikan, keunikan pada kedua standar tersebut perlu dipertimbangkan dan

disesuaikan dengan sasaran, karakteristik, dan regulasi yang berlaku pada organisasi.

NAMA : DINI RAHMADIA

NIM : 182420134

KELAS : MTI REG B

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!

   Jawab:

   Dalam memperoleh user id dan password, Social engineering dapat melakukan berbagai hal untuk mendapatkan akses informasi dengan cara memengaruhi psikis atau psikologi seseorang secara tanpa disadari oleh user itu sendiri, adapun salah satu metode atau teknik yang dilakukan oleh seorang social enggineering adalah hacker Techie Talk Attack (berbicara secara propesional layaknya ahli) yaitu hacker memberikan pemahaman kepada user agar user tepengaruhi dan hacker mendapat kepercayaan dari user/korban. Contohnya adalah ketika hacker berpura-pura dari perusahaan gojek memberitahukan kepada driver bahwa sistem korban/driver telah di retas oleh pihak lain, dan driver diwajibkan mengganti pasword baru, hacker akan memandu driver tersebut untuk mengganti pasword, kemudian hacker akan menanyakan id dan pasword yang telah diganti oleh driver untuk memastikan bahwa password yang dpilih driver/korban aman .

2. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.

   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

Jawab:

Manajemen resiko dibuat agar dapat meminimalisir kejadian yang disebabkan dari kecacatan fungsi dan proses internal perusahaan. Sumber kegagalan itu biasanya berasal dari human error, kegagalan sistem, dan faktor bencana alam. terdapat empat faktor menyebabkan risiko timbul diantaranya manusia, proses, sistem, dan eksternal

Dalam mengidentifikasi resiko terlebih dahulu staff/pengguna melakukan hal seperti

- ✓ Identifikasi risiko contohnya mengidentifikasi dari segi risiko dimasa lalu
- ✓ Analisis resiko contohnya meyiapkan laporan apa saja yang dibutuhkan
- ✓ Monitoring dan respon resiko contohnya jika tedapat sesuatu yang tidak sesuai segera melakukan respon dan menindaklanjutinya

Adapun strategi yang dapat dilakukan yaitu

- ✓ Menghindari risiko contohnya Ketika anda menghadapi risiko yang memiliki dampak yang terlalu tinggi maka anda dapat menghindarinya dengan cara menghentikan rencana yang berisiko tinggi.
- ✓ Risk Reduction (Mengurangi Resiko).Hal ini berarti mencari sebuah tindakan untuk mengurangi kerugian dari sebuah risiko yang dapat terjadi. Kemungkinan risiko terjadi tetap ada, namun dampaknya sebisa mungkin diminimalisasi. Misalnya, sistem *alarm* pendeteksi kebakaran, kebakaran tetap dapat terjadi namun risiko kerugian dapat dikurangi dengan sistem in
- ✓ Risk Retention (Menerima Risiko)Menerima artinya Anda hanya bisa merelakan kerugian tersebut terjadi. Sikap ini tentunya diambil jika tidak ada cara lain untuk menghadapinya. Contohnya jika Anda salah menghitung uang atau salah mengirim barang tentunya kerugian mau tidak mau harus Anda terima. Perlu diingat pula jika dampak kerugiannya terlalu besar maka lebih baik menghindari daripada menerimanya
- ✓ 4. Mengalihkan Risiko (Transfering Risk)

  Apabila seseorang mengalihkan risiko ke pihak lain, maka ia mengalihkan tanggung jawab financial atas risiko tersebut ke pihak lain, yang umumnya atas dasar pemberian imbalan. Cara yang paling umum bagi seseorang, keluarga atau perusaaan untuk mengalihkan risiko adalah dengan membeli pertanggungan asuransi. Risiko kerugian financial tersebut dialihkan ke perusahaan asuransi, dan apabila terjadi sesuatu kerugian yang spesifik, perusahaan asuransi tersebut akan membayarkan sejumlah uang, asalkan

perusahaan asuransi tersebut telah menerima sejumlah uang, yang disebut sebagai premi.

3. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi?

   Jawab:

   kemajuan yang sangat pesat dalam bidang teknologi, baik itu teknologi komunikasi, komputer, teknologi informasi serta teknik dan elektronika, sangat mempengaruhi sebuah sistem dan keamanan teknologi, tetapi terdapat beberapa perusahaan atau organisasi yang masih menggunakan teknologi usang, contohnya *https://ofiskita.com/articles/detail/teknologi-usang-ancam-keamanan-manufaktur*
   jaringan manufaktur serta sistem operasinya masih menggunakan teknologi yang sudah ketinggalan jaman sehingga dapat meningkatkan resiko keamanan, Sementara data yang dikumpulkan dari Smart Protection Network antara Juli dan Desember 2018 mengungkapkan hanya 29% dari produsen menggunakan Windows 10, 60% masih menggunakan Windows 7, dan 4,4% masih menggunakan Windows XP. Tidak mengherankan bila lingkungan manufaktur memiliki tingkat risiko keamanan yang tinggi.

4. Jelaskan sumber penyebab ancaman terhadap IT ! Lengkapi penjelasan tersebut menggunakan contoh

   Jawab:

   Ada berbagai macam dari sumber penyebab ancaman IT yaitu sebagai berikut;

   a) Ancaman IT melalui kontak fisik yaitu stop kontak/kabel listrik yang bisa saja terbakar/ jika kabel terputus karena kesalahan manusia
   b) Ancaman virus malware contohnya kasus binadarma sistem akademiknya yang terkena virus yang menyebabkan segala aktifitas terhenti
   c) Tidak menyimpan barang IT secara sembarangan, karena barang IT merupakan inti pokok dari suatu organisasi/perusahaan agar terhindar dari pencurian
   d) Menambahkan keamanan seperti CCTV, sistem alarm dan kontrak kebersihan
   e) Natural disasters yang memungkinkan data terancam hilang, untuk itu organisasi/perusahaan wajib menyediakan backup agar data-data penting tidak hilang

f) Dalam Manajemen Resiko IT digunakan framework sebagai guide dalam pelaksanaannya. Jelaskan persamaan dan perbedaan dari framework-framework IT Risk Management yang ada? (at least membandingkan 2 framework, more is better)

5. Dalam Manajemen Resiko IT digunakan framework sebagai guide dalam pelaksanaannya. Jelaskan persamaan dan perbedaan dari framework-framework IT Risk Management yang ada? (at least membandingkan 2 framework, more is better)

Jawab:

Perbedaan	COSO ERM – Integrated Framework	ISO 31000: 2009 Risk Management– Principles and Guidelines	COBIT (Control Objectives for Information and Related Technology)
Definisi risiko	"Kemungkinan terjadinya sebuah event yang dapat mempengaruhi pencapaian sasaran entitas." Menurut Grant Purdy, seorang praktisi manajemen risiko veteran di Melbourne, definisi ini gagal menangkap potensi risiko yang dapat muncul akibat perubahan kondisi yang terjadi secara perlahan.	"Efek dari ketidakpastian terhadap pencapaian sasaran organisasi."	"Resiko adalah segala hal yang mungkin berdampak pada kemampuan organisasi dalam mencapai tujuan-tujuannya."
Definisi manajemen risiko	“Proses yang dipengaruhi oleh Board of Directors, manajemen, dan personil lain dalam entitas, diaplikasikan pada pembentukan strategi dan pada seluruh bagian perusahaan, dirancang untuk mengidentifikasi kejadian potensial yang dapat mempengaruhi entitas, dan mengelola risiko selaras dengan risk appetite entitas, untuk menyediakan jaminan yang wajar terhadap pencapaian sasaran dari entitas.”	"Aktivitas-aktivitas terkoordinasi yang dilakukan dalam rangka mengelola dan mengontrol sebuah organisasi terkait dengan risiko yang dihadapinya."	Manajemen Resiko, Mendefinisikan tingkat resiko yang digunakan dan meningkatkan transparansi tentang resiko yang mungkin akan muncul dalam perusahaan
Komponen manajemen risiko	Proses dan kerangka kerja manajemen risiko tidak dipaparkan secara terpisah. Menurut Grant Purdy hal ini dapat menimbulkan kebingungan dan inefektivitas terhadap manajemen risiko, dimana kerangka kerja seharusnya dirancang pada top level management, sedangkan proses manajemen risiko seharusnya diterapkan pada proses-proses organisasi.	Memaparkan kerangka kerja dan proses manajemen risiko secara terpisah. ISO 31000: 2009 juga menyediakan prinsip manajemen risiko yang harus diterapkan dalam kerangka kerja dan proses untuk mendukung efektivitas manajemen risiko. Standar ini menekankan penerapan manajemen risiko sebagai alat penciptaan dan pelindung nilai organisasi.	menyediakan kebijakan yang jelas dan good practice untuk IT governance, membantu manajemen senior dalam memahami dan mengelola risiko-risiko yang berhubungan dengan IT. COBIT menyediakan kerangka IT governance dan

	Standar ini menekankan pada pengembangan pengendalian internal sebagai upaya perusahaan dalam mengelola risiko.		petunjuk control objective yang detail untuk manajemen, pemilik proses bisnis, user dan auditor
Awal proses \manajemen risiko	Dimulai dengan menetapkan sasaran perusahaan yang terdiri dari empat kategori yaitu strategis, operasi, pelaporan, dan pemenuhan.	Dimulai dengan membangun konteks untuk mengidentifikasi kondisi internal, kondisi eksternal, konteks manajemen risiko, dan kriteria risiko.	Dimulai dengan melakukan, pemahaman objectives, Identifikasi resiko, Penilaian resiko, Respon resiko, Pemantauan resiko
Identifikasi konteks eksternal	Sedikit dilakukan.	Dilakukan secara menyeluruh.	Sedikit dilakukan
Komponen proses manajemen risiko	Terdiri dari 8 komponen, yaitu: identifikasi lingkungan internal penetapan sasaran manajemen risiko identifikasi kejadian penilaian risiko, perlakuan risiko; aktivitas pengendalian informasi dan komunikasi; dan pemantauan.	Terdiri dari lima komponen besar, yaitu: (1) komunikasi dan konsultasi (2) membangun konteks (3) penilaian risiko (4) perlakuan risiko (5)monitoring dan review.	Terdiri dari lima komponen IT governance yaitu : Keselarasan strategi Penyampaian Nilai Pengelolaan Sumber Daya Manajemen Resiko, Mendefinisikan tingkat resiko yang digunakan. Pengukuran Kinerja
Pengertian inherent risk	Inherent risk diartikan sebagai eksposur perusahaan terhadap risiko secara utuh. (dampak dari existing control tidak diperhitungkan)	Inherent risk diartikan sebagai eksposur perusahaan terhadap risiko setelah dilakukan pengendalian internal.	Inherent risk diartikan sebagai eksposur perusahaan terhadap risiko Proses penilaian resiko bisa berupa resiko yang tidak dapat dipisahkan (inherent risks) dan sisa resiko (residual risks)
Prinsip manajemen risiko	Tidak ada.	Tersedia dan menjadi hal yang harus diterapkan pada kerangka kerja dan proses manajemen risiko untuk mendukung efektivitas penerapan manajemen risiko.	Tersedia namun tidak di terapkan pada kerangka kerja dan proses manajemen risiko
Perbaikan berkelanjutan	Perbaikan hanya dilakukan apabila diperlukan, berdasarkan hasil pemantauan.	Memfasilitasi perbaikan berkelanjutan pada keseluruhan kerangka kerja dan proses manajemen risiko, sesuai dengan kebutuhan organisasi dan perkembangan konteks.	Setiap langkah dimonitor dan dievaluasi untuk menjamin bahwa resiko dan respon berjalan sepanjang waktu
Penyaluran Informasi	Informasi hanya dikomunikasikan kepada pelaku manajemen risiko untuk mendukung pencapaian sasaran unit-unit tersebut. Keterlibatan stakeholders eksternal tidak diungkapkan pada standar ini.	Informasi mengenai risiko dan manajemen risiko dikomunikasikan dan dikonsultasikan dengan seluruh stakeholders perusahaan, baik internal maupun eksternal (sesuai prinsip “transparan dan inklusif”). Keterlibatan stakeholders diperlukan untuk mengidentifikasi kepentingan seluruh pihak agar menjadi bahan	Kriteria informasi dari COBIT dapat digunakan sebagai dasar dalam mendefinisikan objektif TI. Terdapat tujuh kriteria informasi dari COBIT yaitu : effectiveness, efficiency,

		pertimbangan pengambilan keputusan.	confidentiality, integrity, availability, compliance, dan reliability.
Aspek manusia dan budaya	Aspek manusia disebutkan sebagai batasan dari manajemen risiko dalam memberikan jaminan terhadap pencapaian sasaran organisasi.	Memperhitungkan aspek manusia dan budaya ke dalam manajemen risiko (prinsip "mempertimbangkan faktor budaya dan manusia"). Penerapan manajemen risiko turut mempertimbangkan kultur, persepsi, dan kapabilitas manusia, termasuk memperhitungkan perselisihan kepentingan antara organisasi dengan individu di dalamnya.	Identifikasi resiko merupakan roses untuk mengetahui resiko (baik itu yang sedang terjadi; fakta dilapangan; ataupun resiko2 yang akan terjadi; dengan melihat 7 komponen dari pemahaman objectives) Sumber resiko : Manusia, proses, dan teknologi Internal dan eksternal Bencana (hazard), uncertainty, dan opportunity