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?

---- Selamat bekerja ----

Nama : **Lailatur Rahmi**
Nim : **182420118**
Kelas : **MTI. 20A**
DosenPengasuh : **Dedy Syamsuar, PhD.**
Mata Kuliah : **IT Risk Management and Disaster Recovery**

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. 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

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

---- Selamat bekerja ----

Jawaban

1. Salah satu Metode yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu adalah **Pretexting. Pretexting** adalah suatu teknik yang menggunakan skenario yang dibuat yang bertujuan meningkatkan kemungkinan korban membocorkan informasinya. **Dalam metode pretexting**, hacker akan membuat skenario palsu untuk mencuri data pribadi korban. Serangan ini bisa dilakukan melalui telpon atau email. Hacker akan berpura-pura menjadi petugas bank, petugas lembaga negara, rekan kerja, atau bahkan staff IT perusahaan yang sedang membutuhkan info dari korban untuk tugas urgent. Keberhasilan pretexting ini tergantung dari kemampuan hacker dalam membangun kepercayaan dengan korban. **Contoh,** penerapan teknik banyak dijumpai pada kasus pembobolan di ATM. Skenario yang dijalankan adalah beberapa orang beritndak sebagai satpam palsu dan tukang bank palsu yang kemudian dimesin ATM telah di seting agar kartu ATM tidak bekerja sebagaimana mestinya. Dengan skenrio tersebut pelaku ini meyakinkan korban agar memberikan pin dan mampercayai perutas bank palsu tersebut.

2. Menyusun sebuah perencanaan manajemen risiko yang solid adalah salah satu hal terpenting yang dapat dilakukan untuk bisnis . Banyak perusahaan yang gagal sepanjang waktu, terkadang mereka menyalahkan nasib jelek, "keadaan ekonomi", dan keadaan lainnya yang tak tampak. Manajemen risiko adalah tentang mempersiapkan diri sebaik mungkin terhadap kemungkinan terjadinya kejadian yang tidak diinginkan ini, sehingga dapat, mengimbangi badai yang meruntuhkan kompetitor. Bencana tentu saja tetap dapat menenggelamkan sebuah rencana terbaik, namun dengan melakukan manajemen risiko secara serius akan dengan pasti meningkatkan peluang sukses jangka panjang.

a. Membuat Perencanaan

Setiap bisnis harus memiliki sebuah perencanaan manajemen risiko yang solid. Berikut merupakan panduan dalam menyusunnya. Format perencanaan tersebut dapat bervariasi, tergantung kepada kebutuhan perusahaan. Sebuah perencanaan manajemen risiko untuk perusahaan yang besar dan kompleks dapat dijalankan dengan mudah dalam ratusan halaman, sedangkan sebuah bisnis kecil mungkin hanya memerlukan sebuah spreadsheet kecil yang berfokus pada item utama.

Ada beberapa item penting untuk dicantumkan dalam perencanaan manajemen risiko, sebagai berikut:

- Daftar risiko
- Penilaian tiap risiko berdasarkan kecendrungan terjadi dan dampaknya
- Penilaian terhadap pengendalian saat ini
- Rencana tindakan

b. Menentukan Bagaimana Menangani Risiko

pada poin ini, kita telah mengidentifikasi seluruh risiko utama dalam bisnis, memprioritaskannya berdasarkan kecendrungan dan dampak, dan menilai efektifitas kendali sekarang ini.

Langkah berikutnya adalah menentukan apa yang harus dilakukan pada tiap risiko, sehingga kita dapat menanganinya dengan baik. Dalam dunia manajemen risiko, ada empat strategi utama:

1. Menghindarinya.
2. Menguranginya.
3. Memindahkannya.
4. Menerimanya.

Setiap strategi memiliki kelebihan dan kekurangannya masing - masing, dan perusahaan mungkin akan pada akhirnya menggunakan semuanya. Terkadang perusahaan mungkin perlu menghindari risiko, dan di saat lainnya perusahaan akan ingin menguranginya, memindahkannya, atau cukup menerimanya.

c. Monitor

Melakukan pengukuran tidak cukup; kita juga perlu memeriksa apakah hal tersebut bekerja, dan memonitor bisnis anda secara reguler untuk mengidentifikasi dan menangani risiko baru. Titik awalnya adalah perencanaan yang telah di tetapkan. perusahaan sekarang telah memiliki sebuah daftar seluruh risiko dalam bisnis, penilaian terhadap kecendrungan dan dampaknya, sebuah evaluasi terhadap kendali terkini, dan rencana tindakan untuk menanganinya

3. teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi **Karena,** dunia sedang dalam perjalanan untuk menyelesaikan digitalisasi. Sistem TI tertarik untuk menghasilkan data digital dari setiap aktivitas manusia dan memanfaatkannya. Sebagian besar bisnis, bank dan lembaga keuangan sudah dapat diakses melalui internet dan bertukar data sensitif *online*. Semua digitalisasi dan konektivitas ini telah meningkatkan setiap aspek kehidupan manusia, namun juga meningkatkan kekhawatiran akan keamanan data dan privasi. Selama beberapa tahun terakhir, banyak organisasi telah menjadi mangsa insiden keamanan data.
   Dengan rencana manajemen krisis keamanan *cyber* yang efisien, organisasi dapat menghemat banyak waktu, upaya, dan uang untuk memulihkan sistem mereka dan memulihkan kontinuitas bisnis. Karena meningkatnya ancaman terhadap keamanan informasi, banyak organisasi telah beralih ke biometrik untuk meletakkan keamanan data untuk menghilangkan kekurangan metode usang seperti kata sandi.

Nama : **Lily Pebriana**
Nim : **182420114**
Kelas : **MTI. 20A**
DosenPengasuh : **Dedy Syamsuar, PhD.**
Mata Kuliah : **IT Risk Management and Disaster Recovery**

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. 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

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

---- Selamat bekerja ----

Jawaban

1. **Metode Tailgating,** Teknik tailgating ini hampir sama dengan teknik phising dalam menjalankannya yaitu sama-sama menggunakan scenario yang sudah direncanakkan. Perbedaaanya adalah dalam teknik tailgating ini dijalankan dengan membuntuti orang yang memiliki hak akses. **Contoh** penerapanya ketik dalam sebuah kantor terdapat seorang pegawai yang ingin masuk kedalam ruagan tertentu dengan menggunakana identitas yang dimilikinya, Sipelaku mengikuti korban dan menyatakna bahwa ia lupa membawa identitasnya. Dengan khilaf si korban meminjamkan kartu identitasnya untuk memberikan akses kepada pelaku agar dapat masuk.

2. **Strategi-strategi** dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan. **Contoh** dari keamanan informasi antara lain :

1. Physical security adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan

tempat kerja dari berbagai ancaman yang meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.

2. Personal security adalah keamanan informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup physical security.
3. Operasional security adalah keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan.
4. Communication security adalah keamanan informasi yang bertujuan mengamankan media komunikasi, teknologi komunikasi serta apa yang masih ada didalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
5. Network security adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringannya, data organisasi, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

   Masing masing komponen tersebut berkontribusi dalam program keamanan informasi secara keseluruhan. Jadi keamanan informasi melindungi informasi baik sistem maupun perangkat yang digunakan untuk menyimpan dan mengirimkannya.

   Jaminan kemanan informasi dapat dicapai melalui aktivitas penerapan sejumlah kontrol yang sesuai. Kontrol yang dimaksud meliputi penerapan berbagai kebijakan, prosedur, struktur, praktek, danfungsi - fungsi tertentu. Keseluruhan kontrol tersebut harus diterapkan oleh organisasi agar seluruhsasaran keamanan yang dimaksud dapat tercapai.

   Manajemen keamanan informasi menjadi penting diterapkan agar informasi yang beredar di perusahaan dapat dikelola dengan benar sehingga perusahaan dapat mengambil keputusan berdasarkan informasi yang ada dengan benar pula dalam rangka memberikan layanan yang terbaik kepada pelanggan.

3. **Karena,** teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi oleh karena itu teknologi Deepfake merupakan salah satu teknologi yang bisa usang kapan saja. DEepfake adalah teknologi yang memungkinkan seseorang untuk memanipulasi video dan audio dengan cara yang amat sangat nyata. Ini adalah teknologi berbasis kecerdasan buatan, di mana wajah objek bisa dipasang di sebuah video, tanpa cela sekalipun.Saat ini, deepfake telah makin canggih dan amat sulit dibedakan apakah video ini nyata atau tidak. Pakar keamanan dunia maya pun makin khawatir soal teknologi ini. Tak cuma bisa menyebar informasi palsu, deepfake rawan digunakan untuk penipuan phising, di mana peretas berlaku menjadi orang lain untuk membuat korban memu memberi informasi kepada peretas.

M. ANGGA OKTAHARISETIA

182420123 – MTI2A1 – IT RISK MANAGEMENT AND DISASTER RECOVERY

UAS

1.

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

- PiggyBack Ride Attack
  Piggiback attack adalah Cara mendapatkan hak akses dengan menumpang seseorang yang memiliki akses / wewenang agar kita mendapat hak akses seperti halnya orang tersebut.
  - Contoh :
    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 :
    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

2.

Beberapa pertimbangan yang menjadi risiko dalam melakukan migrasi aplikasi bisnis yang kritis beserta data – data ke Cloud.

- Untuk perusahaan yang baru saja berkembang strategi manajemen risiko yang baik dan efektif akan sangat membantu perusahaan tersebut. Dengan adanya strategi yang efektif risiko yang terjadi dapat diminimalisir atau bahkan bisa dihilangkan, itu sangat membantu perusahaan untuk menghindari terjadinya kegagalan perusahaan akibat risiko yang ditimbulkan. Jika risiko yang terjadi tidak signifikan dampaknya mungkin perusahaan bisa menghandel risiko tersebut, melainkan jika risiko yang terjadi sangatlah besar, maka kecil kemungkinan perusahaan yang baru berkembang untuk bangkit dari risiko yang telah terjadi. Sehingga, untuk menghindari hal yang tidak diinginkan, berikut akan dijabarkan strategi untuk melakukan manajemen risiko secara efektif dan efisien untuk perusahaan yang sedang berkembang :

  - **Melakukan perencanaan manajemen risiko**, Langkah awal yang dilakukan adalah melakukan perencanaan manajemen risiko. Dengan melakukan

perencanaan kita dapat memutuskan bagaimana manajemen risiko yang baik dan sesuai untuk proyek yang akan dilakukan. Perencanaan manajemen risiko mempertimbangkan lingkup proyek, rencana manajemen proyek, faktor lingkungan perusahaan, maka tim proyek dapat mendiskusikan dan menganalisis aktivitas manajemen risiko untuk proyek-proyek tertentu. Untuk membuat perencanaan risiko ada hal –hal yang pendukung perencanaan seperti project charter, kebijakan manajemen risiko, susunan peran dan tanggung jawab, toleransi stackholder terhadap risiko, template untuk rencana manajemen risiko dan work breakdown structure (WBS).

- **Melakukan pengidentifikasian risiko**, Setelah kita merancang bagaimana manajemen risiko yang akan diterapkan di perusahaan, langkah selanjutnya adalah melakukan pengidentifikasian risiko dengan memahami terlebih dahulu risiko yang akan terjadi pada proyek yang dijalankan. Identifikasi risiko dapat dilakukan dengan analisis sumber risiko dan analisis masalah Analisis sumber risiko yaitu analisis risiko dengan melihat darimana risiko berasal. Ada tiga sumber risiko yang sudah banyak dikenal yakni Risiko internal yakni risiko yang bersumber dari internal organisasi yang dapat dikategorikan dalam non technical risk (manusia, material, keuangan) dan technical risk (disain, konstruksi dan operasi). Beberapa perusahaan dan industri melihat daftar periksa risiko berdasarkan pengalaman dari proyek-proyek masa lalu. Daftar periksa ini dapat membantu manajer proyek dan tim proyek dalam mengidentifikasi risiko yang spesifik pada daftar periksa dan memperluas pemikiran tim. Pengalaman masa lalu dari tim proyek, pengalaman proyek di dalam perusahaan, dan para ahli di industri ini dapat menjadi sumber berharga untuk mengidentifikasi potensi risiko pada sebuah proyek.
- **Mengevaluasi risiko**, Setelah risiko potensial teridentifikasi, tim proyek kemudian mengevaluasi setiap risiko berdasarkan probabilitas kejadian risiko akan terjadi dan potensi kerugian yang terkait dengannya. Tidak semua risikonya sama. Beberapa kejadian berisiko lebih mungkin terjadi daripada yang lain, dan biaya risiko bisa sangat bervariasi. Mengevaluasi kemungkinan terjadinya risiko dan tingkat keparahan atau potensi kerugian proyek adalah langkah selanjutnya dalam proses manajemen risiko.
- **Melakukan rencana mitigasi**, Setelah risiko diidentifikasi dan dievaluasi, tim proyek mengembangkan rencana mitigasi risiko, yang merupakan rencana untuk mengurangi dampak kejadian tak terduga. Tim proyek mengurangi risiko dengan berbagai cara yaitu risk avoidance, risk sharing, risk reduction dan risk transfer. Masing-masing teknik mitigasi ini bisa menjadi alat yang efektif dalam mengurangi risiko individu dan profil risiko proyek. Rencana mitigasi risiko akan melakukan pendekatan mitigasi untuk setiap kejadian risiko yang teridentifikasi dan tindakan yang akan diambil oleh tim manajemen proyek untuk mengurangi atau menghilangkan risiko tersebut.
- **Memindahkan Risiko**, Jika risiko tidak bisa ditangani oleh perusahaan secara internal, maka risiko tersebut bisa dipindahkan kepada pihak-pihak yang bisa membantu untuk menangani risiko tersbut. Maksud pihak yang bisa membantu menangani risiko yang ada adalah perusahaan asuransi. Jika risiko yang terjadi adalah hal-hal yang berhubungan dengan kejadian tak terduga seperti kebakaran, pencurian atau kerusakan, maka jasa perusahaan asuransi akan meringankan beban perusahaan dalam menangani risikonya.

3.

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

- Sejak dulu teknologi sudah ada atau manusia sudah menggunakan teknologi. Seseorang menggunakan teknologi karena manusia memiliki akal dan pikiran. Dengan akalnya ia ingin keluar dari masalah, ingin hidup lebih baik, lebih aman dan sebagainya. Perkembangan teknologi terjadi karena seseorang menggunakan akalnya dan pikirannya untuk menyelesaikan setiap masalah yang dihadapinya.

  Di Negara-negara yang sedang berkembang, tentunya memerlukan begitu banyak hal untuk mendukung perkembangan negara mereka. Negara-negara tersebut saling meningkatkan berbagai kemampuan mereka dalam segala aspek kehidupan masyarakat seperti pada aspek pertanian serta industri. Kemudian, selain itu mereka juga mengadakan investasi dalam aspek kesehatan masyarakat begitu pula dalam aspek Pendidikan.

  Dan saat ini, segala aspek kehidupan tersebut telah mampu berkembang dengan pesatnya, perkembangan tersebut beriringan pula dengan perkembangan masyarakat dari masyarakat yang tradisional menjadi masyarakat moderen, kemudian secara otomatis perkembangan tersebut menuntut masyarakat menuju kearah globalisasi. Penyebab utama yang paling terasa pada perubahan tersebut adalah pada aspek Teknologi Informasi, contoh paling sederhana tentang hal ini adalah bila pada masyarakat yang masih tradisional dahulu dalam pencapaian informasi dari jarak jauh memerlukan waktu yang begitu lamanya, karena saat itu masih menggunakan cara pengiriman pesan masih sederhana yaitu surat-menyurat, kemudian berkembang menjadi faksimile kemudian telepon dan sekarang pada tingkat yang lebih moderen telah muncul telepon genggam dalam beragam jenis dan fitur-fitur canggih yang mendominasinya.

  Tentu kemajuan teknologi ini menyebabkan perubahan yang begitu besar pada kehidupan umat manusia dengan segala peradaban dan kebudayaannya. Perubahan ini juga memberikan dampak yang begitu besar terhadap transformasi nilai-nilai yang ada di masyarakat. Khususnya masyarakat dengan budaya dan adat ketimuran seperti Indonesia. Saat ini, di Indonesia dapat kita saksikan begitu besar pengaruh kemajuan teknologi terhadap nilai-nilai kebudayaan yang di anut masyarakat, baik masyarakat perkotaan maupun pedesaan (modernisasi). Kemajuan teknologi seperti televisi, telepon dan telepon genggam (HP), bahkan internet bukan hanya melanda masyarakat kota, namun juga telah dapat dinikmati oleh masyarakat di pelosok-pelosok desa. Akibatnya, segala informasi baik yang bernilai positif maupun negatif, dapat dengan mudah di akses oleh masyarakat. Dampak positif misalnya, kemudahan dalam berkomunikasi lewat telepon seluler atau internet, mudahnya mendapatkan informasi dari internet, sekarang masyrakat tidak hanya bisa berkomunikasi lewat telepon seluler sedangkan hal negatifnya ialah, banyaknya kasus penipuan lewat sms, akun facebook yang dibobol, dan yang lebih parah lagi sandi atau password ATM yang mudah dibobol oleh orang-orang yang tidak bertanggung jawab. Dan

di akui atau tidak, perlahan-lahan mulai mengubah pola hidup dan pola pemikiran masyarakat dengan segala image yang menjadi ciri khas mereka.

- Berikut beberapa langkah yang bisa ditempuh dalam rangka mengurangi risiko keamanan terhadap pada peralihan manufaktur menjadi Industry 4.0
    - Pembatasan pemberian izin terhadap individu yang bisa mengakses data dan sistem.
    - Mengidentifikasi mesin-mesin yang sudah diatur agar bisa saling ‘berkomunikasi’ Seharusnya ada pembatasan untuk perangkat mana dalam jaringan TI yang harus mampu bertukar informasi dengan perangkat mana dalam jaringan operational technology (OT).
    - Layanan yang tidak perlu ada di dalam jaringan harus dinonaktifkan. Melakukan hal itu dapat membantu mencegah eksploitasi layanan yang rentan.

Nama : Mefta Eko Saputra

NIM : 182420113

Kelas : MTI20A

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?

---- Selamat bekerja ----

1. Banyak cara yang dapat di gunakan oleh social enggineering hacket untuk mendapatkan userid dan password pengguna salah satunya dengan teknik **Pretexting. Pretexting** adalah bentuk lain dari social engineering dimana penyerang membuat scenario yang kelihatannya baik bagi taget, dengan cara ini mereka mencoba untuk mendapatkan informasi pribadi korban atau target. Taktik pretexting ini merupakan teknik yang digunakan hacker dengan cara berbicara layaknya para ahli. Hacker yang kita ketahui sangat mahir dalam hal teknis, tapi ketika hacker menggunakan social engineering, maka hacker bisa berbicara sangat lancar seperti seorang ahli. Hacker akan berpura-pura menjadi petugas bank, petugas lembaga negara, rekan kerja, atau bahkan staff IT perusahaan yang sedang membutuhkan info dari korban untuk tugas urgent. Keberhasilan pretexting ini tergantung dari kemampuan hacker dalam membangun kepercayaan dengan korban. **Contoh Kasusnya adalah** yang sekarang marak terjadi yaitu pembobolan terhadap akun pengguna **GO-JEK** yang mana hacker menelpon untuk memberikan hadiah **Go-Pay** kepda pengguna dan mencoba masuk dengan kode **OTP** yang di dapatkan dengan cara teknik **Pretexting.**

2. Strategi yang dapat di ambil dalam yaitu dengan melakukan kontrol terhadap resiko yang akan terjadi. ada 5 bentuk sikap yang dapat diambil yaitu :

   Risk Avoidance (Menghindari Risiko) Sikap berikut sering kali tidak efektif karena dengan menghindari risiko ini berarti Anda tidak berani mengambil kesempatan untuk

berusaha dan mengatasi risiko, Anda bahkan tidak belajar akan apapun. Tindakan ini berarti Anda tidak melakukan tindakan yang dapat menyebabkan risiko tersebut terjadi, termasuk tidak jadi melakukan suatu strategi usaha yang telah disusun. **Contoh :** saat anda takut dengan serangan hacker dari luar. Maka anda akan membuat jaringan sendiri yang hanya bisa di akses oleh orang yang ada di organisasi anda sendiri.

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 **Contohnya :** sistem *alarm* pendeteksi kebakaran, kebakaran tetap dapat terjadi namun risiko kerugian dapat dikurangi dengan sistem ini.

Risk Transfer (Memindahkan Risiko) Selain menghindari dan mengurangi risiko, Anda juga bisa mengalihkan risiko. Anda bisa mengalihkan tanggung jawab kepada pihak lain dengan membayar jasa tersebut. **Contoh** : jika Anda memiliki perusahaan barang pecah belah dan harus mengirimkannya ke tempat yang cukup jauh dan jalan yang kurang memadai, daripada Anda sendiri atau karyawan sendiri yang mengantar lebih baik Anda memilih membayar jasa pengantar yang memiliki asuransi barang pecah belah. Tentu risikonya akan Anda pindahkan ke pihak pengantar ini.

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.

3. Menurut pendapat saya kenapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi adalah karena perkembangan teknologi informasi sangatlah cepat dan pesat. Contohnya saja adalah handphone tidak sampai 1 tahun brand yang sama bisa mengeluakan lebih dari 3 produknya. Teknologi yang usang akan memberikan banyak celah kepada orang yang ingin berniat jahat kepada kita. Karna sudah bnyak sekali tools untuk bisa meng hack sistem bahkan sistem yang "**Canggih" dan "Baru"** bisa di retas oleh para hecker. Semua teknologi yang usang memiliki kelemahan yang ssdah di ketahui oleh bnyak orang. Bahkan bisa di cari di internet. Dengan mempedulikan dan mebiarkan teknologi usang maka dapat dikatakan anda "**Bunuh Diri"** dizaman skarang ini yang mana informasi sangat mudah di dapatkan dan sangat cepat tersebar.

Nama : **Miftahul Fallah**
Nim : **182420132**
Kelas : **MTI. 20A**
DosenPengasuh : **Dedy Syamsuar, PhD.**
Mata Kuliah : **IT Risk Management and Disaster Recovery**

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. 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

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

---- Selamat bekerja ----

Jawaban :

1. **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 untuk maksud tertentu. 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, 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. **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. Phising banyak memakan korban di sektor social media, hal itu dikarenakan social media merupakan akun harian yang sering digunakan oleh pengguna, tanpa sadar pengguna memasuki halaman jebakan yang menyebabkan pengguna bisa saja terjebak karena halaman palsu tersebut. Tidak hanya itu, phising juga terkadang bisa terjadi manipulasi dimana komputer yang terinfeksi bisa saja memanipulasi beberapa hal yang membuat halaman itu merupakan halaman aslinya, sehingga perlu diperhatikan untuk komputer anda tidak terkena virus untuk menghindari kasus ini. Banyak sekali kasus kejahatan phising yang sering dilakukan, terlebih hal itu bisa saja mencuri banyak informasi anda seperti akses akun Anda, email, social media, bahkan akun Bank Anda. Untuk menghindari phising, pengguna harus lebih berhati-hati dengan memperhatikan beberapa hal keamanan.

2. Untuk perusahaan yang baru saja berkembang strategi manajemen risiko yang baik dan efektif akan sangat membantu perusahaan tersebut. Dengan adanya strategi yang efektif risiko yang terjadi dapat diminimalisir atau bahkan bisa dihilangkan, itu sangat membantu perusahaan untuk menghindari terjadinya kegagalan perusahaan akibat risiko yang ditimbulkan. Jika risiko yang terjadi tidak signifikan dampaknya mungkin perusahaan bisa menghandel risiko tersebut, melainkan jika risiko yang terjadi sangatlah besar, maka kecil kemungkinan perusahaan yang baru berkembang untuk bangkit dari risiko yang telah terjadi. Sehingga, untuk menghindari hal yang tidak diinginkan, berikut akan dijabarkan strategi untuk melakukan manajemen risiko secara efektif dan efisien untuk perusahaan yang sedang berkembang :
   1. Melakukan perencanaan manajemen risiko, Langkah awal yang dilakukan adalah melakukan perencanaan manajemen risiko. Dengan melakukan perencanaan kita dapat memutuskan bagaimana manajemen risiko yang baik dan sesuai untuk proyek yang akan dilakukan. Perencanaan manajemen risiko mempertimbangkan lingkup proyek, rencana manajemen proyek, faktor lingkungan perusahaan, maka tim proyek dapat mendiskusikan dan menganalisis aktivitas manajemen risiko untuk proyek-proyek tertentu. Untuk membuat perencanaan risiko ada hal –hal yang pendukung perencanaan seperti project charter, kebijakan manajemen risiko, susunan peran dan tanggung jawab, toleransi stackholder terhadap risiko, template untuk rencana manajemen risiko dan work breakdown structure (WBS).
   2. Melakukan pengidentifikasian risiko, Setelah kita merancang bagaimana manajemen risiko yang akan diterapkan di perusahaan, langkah selanjutnya adalah melakukan pengidentifikasian risiko dengan memahami terlebih dahulu risiko yang akan terjadi pada proyek yang dijalankan. Identifikasi risiko dapat dilakukan dengan analisis sumber risiko dan analisis masalah Analisis sumber risiko yaitu analisis risiko dengan melihat darimana risiko berasal. Ada tiga sumber risiko yang sudah banyak dikenal yakni Risiko internal yakni risiko yang bersumber dari internal organisasi yang dapat dikategorikan dalam non technical risk (manusia, material, keuangan) dan technical risk (disain, konstruksi dan operasi). Beberapa perusahaan dan industri melihat daftar periksa risiko berdasarkan pengalaman dari proyek-proyek masa lalu. Daftar periksa ini dapat membantu manajer proyek dan tim proyek dalam mengidentifikasi risiko yang spesifik pada daftar periksa dan memperluas pemikiran tim. Pengalaman masa lalu dari tim proyek, pengalaman proyek di dalam perusahaan, dan para ahli di industri ini dapat menjadi sumber berharga untuk mengidentifikasi potensi risiko pada sebuah proyek.
   3. Mengevaluasi risiko, Setelah risiko potensial teridentifikasi, tim proyek kemudian mengevaluasi setiap risiko berdasarkan probabilitas kejadian risiko akan terjadi dan potensi kerugian yang terkait dengannya. Tidak semua risikonya sama. Beberapa kejadian berisiko lebih mungkin terjadi daripada yang lain, dan biaya risiko bisa sangat bervariasi. Mengevaluasi kemungkinan terjadinya risiko dan tingkat keparahan atau potensi kerugian proyek adalah langkah selanjutnya dalam proses manajemen risiko.
   4. Melakukan rencana mitigasi, Setelah risiko diidentifikasi dan dievaluasi, tim proyek mengembangkan rencana mitigasi risiko, yang merupakan rencana untuk mengurangi dampak kejadian tak terduga. Tim proyek mengurangi risiko dengan berbagai cara yaitu risk avoidance, risk sharing, risk reduction dan risk transfer. Masing-masing teknik mitigasi ini bisa menjadi alat yang efektif dalam mengurangi risiko individu dan profil risiko proyek. Rencana mitigasi risiko akan melakukan pendekatan mitigasi untuk setiap kejadian risiko yang teridentifikasi dan tindakan yang akan diambil oleh tim manajemen proyek untuk mengurangi atau menghilangkan risiko tersebut.
   5. Memindahkan Risiko, Jika risiko tidak bisa ditangani oleh perusahaan secara internal, maka risiko tersebut bisa dipindahkan kepada pihak-pihak yang bisa

membantu untuk menangani risiko tersbut. Maksud pihak yang bisa membantu menangani risiko yang ada adalah perusahaan asuransi. Jika risiko yang terjadi adalah hal-hal yang berhubungan dengan kejadian tak terduga seperti kebakaran, pencurian atau kerusakan, maka jasa perusahaan asuransi akan meringankan beban perusahaan dalam menangani risikonya.

3. **Karena** yang perlu digaris bawahi dalam membuat rencana sistem keamanan adalah menganalisis risiko-risiko yang mungkin ada, termasuk risiko yang timbul dari dalam sistem. Perlu diingat ancaman keamanan sistem tak hanya bisa ditemukan dari luar sistem. Kemungkinan ancaman dari dalam sistem pun banyak ditemukan. Untuk minimalisir hal tersebut perlu dibuat pemetaan atau rencana penanggulangan risiko TI, baik dari dalam maupun dari luar, misalnya dengan membuat rencana kontrol hak akses sistem atau menempatkan *firewall* di dalam sistem jaringan. Masih berkaitan dengan ancaman dari dalam, semua orang yang berada di dalam sistem harus memiliki dasar keamanan TI. Hal ini untuk mencegah kasus bocornya data atau masuknya perangkat lunak berbahaya ke dalam sistem. Pengetahuan dasar keamanan juga berguna untuk memberikan wawasan mengenai ancaman keamanan dan cara pencegahannya. **Contohnya**, untuk mencegah pegawai dari tipuan *phising* yang sering mengincar orang awam atau orang-orang yang tidak memiliki pengetahuan tentang ancaman keamanan. **Contoh lain**, mencegah penggunaan flashdisk yang sembarangan, membuat *password* yang tidak mudah ditebak, dan pengelolaan akun yang baik.

Nama **:Moh Fajri Al Amin**

NIM **:182420121**

Kelas **:MTI 20 A**

Dosen Pengajar **:Dedy SyamsuarPhD.**

Mata Kuliah **:IT Risk Management and Disaster Recovery**

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?

---- Selamat bekerja ----

Jawab

1. Pada dasarnya metode yang umum digunakan seorang hacker di dalam mengambil data userID dan password pengguna adalah dengan cara phishing. Secara istilah phishing ini berasal dari kata”fishing” yang berarti memancing. Cara kerja phishing sendiri adalah dengan menipu korbannya melalui email atau bahkan situs tiruan yang dibuat sedemikian rupa senhingga dapat mengelabuhi target dan korban pun akan memasukkan id serta password ke web palsu tersebut yang nantinya akan digunakan oleh si hacker.salah satu pencegahan nya agar tidak terkena phishing adalah dengan memastikan web yang kita akses itu asli. Semisal membuka situs elearning.binadarma.ac.id yang notabene adalah situs yang asli, pastikan web yang kita akses url nya sama dan tidak ada perubahan seperti domail atau symbol yang berbeda.

2. Manajemen risiko dibuat guna untuk melindungi suatu perusahaan atau organisasi yang juga mencakup karyawan, properti, reputasi dan lainnya dari sebuah bahaya yang sewaktu – waktu dapat terjadi. Dapat kita ketahui bahwa tidak semua risiko dapat dihilangkan atau dihindari, oleh karena itu diperlukan tindakan – tindakan pencegahan atau tindakan untuk menghadapi risiko yang telah teridentifikasi tersebut. Dalam artikel ini akan dijelaskan beberapa langkah yang dapat dilakukan dalam proses manajemen risiko untuk membantu

organisasi merancang dan mengimplementasikan rencana manajemen risiko yang efektif dan proaktif. Berikut adalah langkah – langkah yang dapat dilakukan, yaitu:

1. Risk Identification

Langkah pertama yang dilakukan adalah mengidentifikasi kemungkinan risiko yang dapat terjadi pada organisasi atau perusahaan. Ini bertujuan untuk mengetahui keadaan yang akan dihadapi oleh organisasi atau perusahaan tersebut dalam berbagai aspek seperti sosial, hukum, ekonomi, produk/jasa, pasar, dan teknologi yang ada. Risiko dari setiap aspek akan diklasifikasikan menurut kategorinya masing – masing agar mempermudah proses selanjutnya.

2. Risk Assessment

Setelah risiko telah diidentifikasi pada perusahaan atau organisasi tersebut, selanjutnya akan dinilai potensi keparahan kerugian dan kemungkinan terjadinya. Dalam hal ini, diperlukan kemampuan individu disetiap bidangnya untuk memberikan penilaian terhadap risiko – risiko yang telah diidentifikasi. Tujuannya adalah agar setiap risiko berada pada prioritas yang tepat.

3. Risk Response

Proses ini dilakukan untuk memilih dan menerapkan langkah – langkah pengelolaan risiko. Tantangan bagi manajer risiko adalah untuk menentukan portofolio yang tepat untuk membentuk sebuah strategi yang terintegrasi sehingga risiko dapat dihadapi dengan baik. Tanggapan risiko umumnya terbagi dalam kategori seperti berikut:

1. Risk Avoidance, Mengambil tindakan untuk menghentikan kegiatan yang dapat menyebabkan risiko terjadi
2. Risk Reduction, Mengambil tindakan untuk mengurangi kemungkinan atau dampak atau keduanya, biasanya melalui pengandalian di bagian internal perusahaan/organisasi
3. Risk Sharing or Transfer, Mengambil tindakan untuk mentransfer beberapa risiko melalui asuransi, outsourcing atau hedging.
4. Risk Acceptence, Tidak mengambil tindakan apapun untuk menganggulangi risiko, melainkan menerima risiko tersebut terjadi.
5. Create a Risk Management Plan

Membuat penanggulangan risiko yang tepat untuk setiap masing – masing kategori risiko. Mitigasi perlu mendapat persetujuan oleh level manajemen yang sesuai, berikut adalah contoh tabel manajemen risiko:

4. Implementation

Melaksanakan seluruh metode yang telah direncanakan untuk mengurangi atau menanggulangi pengaruh dari setiap risiko yang ada.

5. Evaluate and Review

Perencanaan yang telah direncanakan di awal tidak akan seluruhnya dapat berjalan dengan lancar. Perubahan keadaan atau lingkungan yang tidak diprediksi sebelumnya akan menyebabkan perubahan rencana manajemen risiko yang telah dibuat, oleh karena itu perlu dilakukan perubahan rencana untuk menanggulangi risiko yang akan mungkin terjadi

3. Pada dasarnya ancaman yang dapat terjadi di dalam system tidak hanya berasal dari luar system, tetapi juga dapat dari dalam. Pada fase ini bias disebut dengan end of support, yaitu masa dimana suatu teknologi suatu teknologi sudah habis masa service nya. Ada banyak sekali resiko didalam penggunaan teknologi yang sudah using. Sebut saja salah satunya dengan resiko kehilangan data karena virus, malware, atau hacking jarak jauh. Di jaman yang sudah maju ini tentu saja banyak sekali pihak yang meretas data dengan teknologi yang canggih, untuk mencegahnya tentu saja kita membutuhkan suatu upgrade berkala agar dapat meminimalisir kemungkinan resiko yang akan terjadi.atau juga dengan menggunakan teknologi cloud computing agar mengelola data semakin mudah tanpa takut apabila terjadi kerusakan hardware data akan hilang begitu saja.

MOH. RENDY SEPTIYAN

182420103

MTI20A

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?

---- Selamat bekerja ----

Jawaban No.1

a. Pakai Kamus Password

Cara pertama yang sering dipakai hacker untuk meretas akun korban adalah menggunakan kamus password. Di dalam kamus tersebut berisi sejumlah kombinasi password yang paling sering dipakai. Jadi kombinasi password seperti 123456, qwerty, password, princess, gantengbingit, itu pasti tercantum di dalamnya.

Kelebihan kamus password ini yaitu penyerang dapat menemukan password korban dengan sangat cepat, karena yang membaca database kamus tersebut adalah perangkat komputer. Maka dari itu, jika akun dan password kalian ingin aman dari hacker, maka salah satu caranya adalah dengan membuat password yang kuat dan tidak mudah ditebak oleh siapa pun. Atau cara alternatif lainnya adalah dengan memanfaatkan program password manager seperti LastPass.

b. Brute Force

Selanjutnya cara kedua yang perlu kita waspadai adalah **serangan brute force**, yang mana serangan ini berfokus pada **kombinasi karakter** yang digunakan dalam password. Keyword yang

dipakai biasanya **sesuai dengan algoritma** yang dimiliki password manager, misalnya kombinasi antara beberapa huruf besar, huruf kecil, angka-angka, dan beberapa karakter simbol.

Serangan brute force ini akan **mencoba beberapa kombinasi** dari karakter alfanumerik yang paling banyak dipakai, misalnya seperti **1q2w3e4r5t, zxcvbnm, dan qwertyuiop**. Nah, apakah kalian termasuk yang menggunakan password seperti itu?

Kelebihan cara ini adalah dapat **menambah variasi serangan** daripada hanya menggunakan kamus password saja. Jika akun kalian ingin aman dari serangan brute force, maka gunakan kombinasi karakter yang **lebih bervariasi**. Bila memungkinkan gunakan juga **simbol-simbol ekstra** untuk meningkatkan kompleksitas kata sandi.

c. Phising

Phising adalah salah satu cara yang paling populer untuk mendapatkan akun milik korban sampai saat ini. Jadi, phising adalah usaha untuk mengelabui target supaya mereka tidak menyadari jika mereka sedang ditipu.

Saat ini email phising menjadi salah satu cara populer untuk mendapatkan akun milik korban, dan juga setiap harinya terdapat miliaran email palsu yang dikirim ke semua pengguna internet di seluruh dunia. Modusnya adalah korban akan menerima email palsu yang mengaku bahwa mereka berasal dari organisasi atau bisnis yang terpercaya. Biasanya isi email ini mengharuskan korban untuk melakukan sesuatu seperti menyerahkan informasi pribadi dan lain-lain.

Selain itu, email palsu juga terkadang berisi informasi yang mengarahkan target untuk mengklik tautan situs tertentu, yang bisa berupa malware atau situs web palsu yang dibuat mirip dengan web aslinya. Sehingga dalam kasus ini korban tidak menyadari jika mereka sedang diarahkan untuk menyerahkan informasi pribadi yang penting.

d. Social Engineering

Social engireening mirip dengan teknik phising, namun teknik ini lebih dipakai dalam kehidupan nyata. Misalnya kasus mama minta pulsa juga menggunakan teknik ini, si korban yang tidak menyadari bisa dengan mudah langsung percaya dengan isi pesan tersebut dan langsung mengikuti arahan yang diberikan si penipu.

Teknik social engireening ini sudah ada sejak dulu dan hal ini malah disalahkangunakan sebagai metode untuk menipu korban secara tidak langsung, seperti meminta password atau meminta sejumlah uang.

e. Rainbow Table

Rainbow table adalah bentuk serangan dengan memanfaatkan database akun dan password yang sudah didapat. Dalam kasus ini penyerang sudah mengantongi daftar username target dan kata sandi, tetapi dalam bentuk enkripsi. Kata sandi yang terenkripsi ini memiliki tampilan yang sangat berbeda dengan aslinya, misalnya kata sandi yang didapat adalah 'Jalantikus , maka bentuk enkripsi hash MD5 nya berbentuk 8f4047e3233b39e4444e1aef240e80aa , rumit bukan?

Namun dalam kasus tertentu, penyerang hanya menjalankan daftar password plaintext lewat algoritma *hashing*, lalu kemudian membandingkan hasilnya dengan data password yang masih berbentuk enkripsi. Ya, bisa dibilang algoritma enkripsi tidak seratus persen aman serta sebagian besar password yang terenkripsi pun ternyata masih mudah dibobol.

Inilah mengapa metode rainbow table paling relevan saat ini, alih-alih penyerang harus memproses jutaan password dan mencocokkan nilai hash yang dihasilkannya, rainbow table sendiri sudah merupakan daftar nilai hash dari algoritma yang telah dihitung sebelumnya.

Metode ini dapat mengurangi waktu yang dibutuhkan untuk memecahkan kata sandi target. Nah, hacker sendiri dapat membeli rainbow table yang telah terisi penuh oleh jutaan kombinasi password yang potensial dan banyak dipakai. Jadi, hindari situs yang masih menggunakan metode enkripsi SHA1 atau MD5 sebagai algoritma hashing password karena metode ini telah ditemukan celah keamanannya.

f. Malware/Keylogger

Cara lain yang bisa membahayakan akun dan informasi penting di internet adalah karena adanya malware atau program jahat. Malware ini telah tersebar di seluruh jaringan internet dan berpotensi untuk terus berkembang. Bahayanya lagi jika kita sampai terkena malware dalam bentuk keylogger, maka secara tak sadar setiap aktivitas kita di komputer bisa diketahui oleh penyerang.

Program malware ini sendiri secara khusus dapat menargetkan data pribadi, lalu penyerang bisa dengan mudah mengendalikan komputer korban dari jarak jauh untuk mencuri setiap informasi yang berharga.

Bagi kalian yang tidak ingin terkena malware, maka jangan pernah menggunakan aplikasi bajakan. Lalu jangan malas untuk memperbarui software antivirus dan antimalware yang ada. Selain itu selalu berhati-hati saat *browsing* internet dan jangan asal downlad file dari sumber yang tidak jelas.

g. Spidering

Spidering adalah teknik untuk menemukan informasi dengan cara mencari berbagai petunjuk atau serangkaian data-data yang berkaitan dengan si target. Penyerang bisa memulainya dengan mencari data-data pribadi dan menyusunnya untuk dirangkai menjadi sebuah informasi berharga. Cara ini biasa disebut sebagai teknik spidering atau pencarian jaring laba-laba.

Maka dari itu, jangan membuat username dan password yang berhubungan dengan informasi pribadi, misalnya seperti tanggal lahir, nama pasangan, nama hewan peliharaan, dan lain sebagainya yang berhubungan dengan data diri kita. Hal ini karena informasi tersebut sangat mudah ditebak dan ditelusuri.

Sumber : ***https://jalantikus.com/tips/cara-hacking-password/***

Jawaban No. 2

Setelah mengetahui ancaman-ancaman yang dapat terjadi, maka mulailah kita dapat mengelola risiko TI dengan tahapan :

- Mengidentifikasi risiko
- Menilai risiko
- Mengurangi risiko
- Mengembangkan rencana respon
- Mengkaji prosedur manajemen risiko

Kerangka kerja (*Framework*) pengelolaan risiko yang dapat digunakan misalnya adalah dengan pendekatan ISO 31000:2009, ISO 27005:2011, COSO dan lain-lain.

Sebagai contoh dari hasil assessment pada risiko TI adalah perencanaan kelangsungan bisnis (*business continuity*). Organisasi yang memiliki risiko yang teridentifikasi dan dampak bisnis kemungkinan, pengembangan rencana kesinambungan bisnis dapat membantu bisnis Anda bertahan dan pulih dari krisis IT. Sebuah rencana kesinambungan bisnis mengidentifikasi kegiatan bisnis penting, risiko, rencana respon dan prosedur pemulihan.

Sumber : https://itgid.org/manajemen-risiko-teknologi-informasi-part-i/

Jawaban No. 3

Sistem lawas masih merajalela di sebagian besar industri dan tidak bisa dengan mudah diperbaharui atau diganti. Sistem-sistem ini sering mengandung kerentanan perangkat lunak yang diketahui oleh publik dan dapat dimanfaatkan untuk menembus jaringan perusahaan. Pada saat yang sama, peretas menjadi semakin canggih dan memiliki lebih banyak insentif untuk melakukan serangan siber.

Pemerintah dan perusahaan mengakui ancaman baru ini dan menerapkan solusi keamanan modern, namun akan memakan waktu bertahun-tahun untuk menghentikan dan memperbaharui semua sistem. tahun 2018 kembali menjadi salah satu tahun dimana kelemahan tersebut kembali menghantui kita. Lebih penting lagi, kita perlu mulai merencanakan masa depan untuk menghadapi ancaman-ancaman baru yang ditimbulkan oleh Internet of Things (IoT), yang akan melebihi apa yang telah kita alami dalam serangan siber. Meskipun sistem manufaktur digunakan dalam lingkungan yang terisolasi, untuk kemudahan administrasi tetap saja masih terhubung dengan jaringan internet publik untuk, sehingga ancaman keamanan akan selalu ada. Keamanan sangat penting untuk keberhasilan adopsi *Industry 4.0*. Ketahanan proses produksi sangat tergantung pada kesadaran perusahaan manufaktur akan ancaman saat ini dan kerangka kerja keamanan yang digunakan untuk melindungi dari serangan.

IT Risk Management

Ujian Akhir Semester

Muhammad Devian Saputra

NIM 182420128

MTI20A

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?

---- Selamat bekerja ----

1. Metode yang digunakan untuk memperoleh User ID dan password dengan menggunakan Phising yaitu adalah tehnik untuk mendapatkan informasi sensitif(Data pribadi atau akun) dari korban dengan cara menulis email yang seolah-olah berasal dari website resmi.

   Contoh : 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

2. Lima strategi dasar untuk mengendalikan risiko

   Pertahanan - Menerapkan perlindungan yang menghilangkan atau mengurangi risiko yang tidak terkendali yang tersisa

   Contoh : dalam suatu jaringan computer LAN/WAN di pasang suatu hardware / software firewall untuk mencegah masuknya suatu virus atau aplikasi yang dapat menyusup dan merusak data dalam suatu jaringan.

   Transfer - Mengalihkan risiko ke area lain atau ke entitas luar

   Contoh : mengasuransikan seluruh asset dalam perusahaan sehingga apabila terjadi suati bencana yang diluar dugaan akan menjadi tanggung jawab pihak asuransi.

Mitigasi - Mengurangi dampak aset informasi jika penyerang berhasil mengeksploitasi kerentanan

Contoh : dalam mengelola suatu system IT penggunaan media backup misalnya server back up, power backup dan infrastructure jaringan internet back up disiapkan untuk mengantisipasi terjadinya suatu kegagalan dalam system .

Penerimaan - Memahami konsekuensi dari memilih untuk meninggalkan risiko yang tidak terkendali dan kemudian dengan benar mengakui risiko yang tetap tanpa upaya pengendalian

Contoh : dalam suatu perusahaan IT ada beberapa resiko keamanan yang sangat mungkin terjadi diantaranya pencurian informasi, penggunaan user yang tidak terotorisasi, perubahan data yang berlangsung tanpa disadari dan penghancuran data atau software yang dapat merusak suatu system dalam perusahaan, semua resiko itu tetap diupayakan pengendaliannya dengan mempersiapkan suatu system keamanan informasi yang di siapkan dalam suatu system baik hardware maupun software.

Pengakhiran - Menghapus atau menghentikan aset informasi dari lingkungan operasi organisasi

Contoh :apabila terdeteksi suatu serangan dalam sebuah system informasi maka seorang system engineer atau admin akan melakukan cut off dari suatu jaringan internet yang menghubungkan ke internet sehingga dapat segera dilakukan pengamanan data dan perbaikan celah2 yang berhasil ditembus oleh para penyusup dalam suatu jaringan.

3. Teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi karena teknologi yang lama memiliki celah2 keamanan yang dapat ditembus oleh orang – orang yang memanfaatkan keahlianya untuk melakukan kejahatan dalam dunia IT, misalnya dengan perkembangan penciptaan virus dan apliaksi yang bertujuan untuk memperoleh data authentifikasi user dan password. Bilamanana dengan teknologi yang lama tidak segera dilakukan upgrade atau update maka keamanan yang relative rendah akan mudah disusupi oleh virus dan aplikasi2 yang bisa merugikan .

NAMA : PUTRI ARMILIA PRAYESY
NIM : 182420125
KELAS : MTI 20A
MATA KULIAH : IT RISK MANAGEMENT AND DISASTER RECOVERY

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?

---- Selamat bekerja ----

1. Metode yang digunakan oleh seorang social enggineering hacker

Phishing : Phishing menjadi jenis serangan paling umum dalam social Engineering

Contoh : Hacker akan menggunakan email yang berisi pesan palsu dan link berbahaya untuk memancing korban agar memberikan informasi penting. Agar korban percaya, 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

Whalling attack : Jenis serangan phishing yang mengincar korban dengan jabatan yang

Contoh : Teknik ini mengadopsi teknik yang sama dengan email phishing, yang membedakan adalah target yang diserang. Email dibuat menyerupai email bisnis penting yang dikirim oleh otoritas resmi. Untuk melakukan metode ini, hacker membutuhkan lebih banyak penelitian dan perencanaan daripada metode phishing biasa. Mereka harus mencari banyak informasi terkait profil perusahaan atau target, agar email lebih mudah dipercaya oleh user yang akan diserang.

Pretexting : Hacker akan membuat skenario palsu untuk mencuri data pribadi korban. Serangan ini bisa dilakukan melalui telpon atau email.

Contoh : Hacker akan berpura-pura menjadi petugas bank, petugas lembaga negara, rekan kerja, atau bahkan staff IT perusahaan yang sedang membutuhkan info dari korban untuk tugas urgent. Keberhasilan pretexting ini tergantung dari kemampuan hacker dalam membangun kepercayaan dengan korban.

Baiting : Metode ini memanfaatkan rasa ingin tahu dari korban.

Contoh : Hacker dapat membujuk korban agar membuka tautan 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 dan mendorong korban untuk mengunduh aplikasi yang sudah terinfeksi malware.

2. Strategy yang dapat diterapkan untuk memanajemen resiko ini adalah Migrasi yang bertujuan untuk mengurangi dampak buruk dari pemanfaatan suatu sistem dengan melakukan perencanaan dan persiapan penanganan dampak buruk dari serangan tersebut, misal dengan Disaster Recovery Plan

Contoh : ***Amazon Web Services (AWS)***

Merupakan penyedia cloud terbesar di dunia yang pada 28 Februari 2017 yang lalu mengalami downtime selama 5 jam. Downtime yang terjadi pada layanan cloud AWS menyebaban Netflix, Tinder, Airbnb, Reddit dan IMDb menjadi offline.

Kejadian downtime tersebut disebabkan karena kesalahan coding konfigurasi pada salah satu sensor yang menyebabkan masalah katastropik. Namun, untuk perusahaan dengan sistem yang sangat kompleks, AWS mampu melakukan pemulihan dalam waktu 5 jam merupakan hal yang cukup baik. Tentunya hal ini tidak baik secara biaya dan kerugian para pelanggan.

AWS menggunakan lingkungan DevOps dan orkestrasi infrastruktur teknologi informasi. Sehingga segala masalah yang timbul dapat cepat mereka kembalikan normal. Ini disebut dengan istilah rollback. Hanya saja, semakin kompleks maka semakin lama waktu yang dibutuhkan untuk dapat kembali pulih.

3. Keamanan dalam sistem informasi merupakan faktor yang sangat penting keberadaannya dalam mengoperasian sistem informasi itu sendiri. Bagaimana tidak banyak ancaman-ancaman yang terjadi pada sistem informasi yang akan merugikan banyak pihak, baik individu, masyarkat, dan lain sebagainya.

Teknologi yang telah usang pun berkontribusi ancaman bagi keamanan teknologi yang mendorong tingkat dan sifat kerugian. Misalnya, potensi hilangnya produktivitas akibat aset yang dihancurkan atau dicuri tergantung pada seberapa penting aset itu bagi produktivitas organisasi. Jika aset penting diakses secara tidak sah, tidak ada kerugian produktivitas langsung. Demikian pula, penghancuran aset yang sangat sensitif yang tidak memainkan peran penting dalam produktivitas tidak akan secara langsung mengakibatkan hilangnya produktivitas yang signifikan. Namun, aset yang sama itu, jika diungkapkan, dapat mengakibatkan hilangnya keunggulan kompetitif atau reputasi secara signifikan, dan menghasilkan biaya hukum. Intinya adalah kombinasi aset dan jenis tindakan terhadap aset yang menentukan sifat dasar dan tingkat kerugian. Tindakan yang diambil oleh agen ancaman akan didorong terutama oleh motif agen tersebut (misalnya, keuntungan finansial, balas dendam, rekreasi, dll.) Dan sifat aset. Misalnya, agen ancaman yang bertekad mendapatkan keuntungan finansial lebih kecil kemungkinannya menghancurkan server yang kritis daripada mencuri aset yang mudah digadaikan seperti laptop.

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. Mengingatseriusnyaresikokeamananakan asset TeknologyInformasidankomunikasi (TIK), managemenresikosecaraefektifmenjadibagianpentinguntukmengurangidampakburuk yang dapatditimbulkannya. Ditambahlagi, penggunaan TIsemakinmenjadibagian integral dari proses bisnisdimanagangguandengan TIK berdampaklangsungterhadapkelancaranoperasionalorganisasi. Berlatarbelakanghaltersebutmakamenjadipentingbaikbagipihakmanajemenmaupunseluruh staff memahamiresikoapa yang mungkinmunculdilingkungan IT merekadanbagaimanaresikotersebutdapatdikurangiataubahkandihilangkan. Sehubungandenganhalinibagaimana strategy yang dapatditerapkanuntukmemanajemenresikoini…? Jelaskandengancontoh

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

---- Selamatbekerja ----

1. Metode yang sering digunakan hacker untuk memperoleh userid dan password salah satunya adalah dengan metode situs web palsu. Contohnya situs web bank, situs web bank digandakan semirip mungkin dengan aslinya dan situs web palsu itu meminta Anda untuk memasukkan ID dan *password* Anda. Jika Anda melakukannya, maka si pembuat situs web palsu akan menggunakan ID dan *password* Anda untuk mengakses rekening.

2. Strategi yang diterapkan ;

    1. Risk Identification

Langkah pertama yang dilakukan adalah mengidentifikasi kemungkinan risiko yang dapat terjadi pada organisasi atau perusahaan. Ini bertujuan untuk mengetahui keadaan yang akan dihadapi oleh organisasi atau perusahaan tersebut dalam berbagai aspek seperti sosial, hukum, ekonomi, produk/jasa, pasar, dan teknologi yang ada. Risiko dari setiap aspek akan diklasifikasikan menurut kategorinya masing – masing agar mempermudah proses selanjutnya.

    2. Risk Assessment

Setelah risiko telah diidentifikasi pada perusahaan atau organisasi tersebut, selanjutnya akan dinilai potensi keparahan kerugian dan kemungkinan terjadinya. Dalam hal ini, diperlukan kemampuan individu disetiap bidangnya untuk memberikan penilaian terhadap risiko – risiko yang telah diidentifikasi. Tujuannya adalah agar setiap risiko berada pada prioritas yang tepat.

    3. Risk Response

Proses ini dilakukan untuk memilih dan menerapkan langkah – langkah pengelolaan risiko. Tantangan bagi manajer risiko adalah untuk menentukan portofolio yang tepat untuk membentuk sebuah strategi yang terintegrasi sehingga risiko dapat dihadapi dengan baik. Tanggapan risiko umumnya terbagi dalam kategori seperti berikut:

1. Risk Avoidance, Mengambil tindakan untuk menghentikan kegiatan yang dapat menyebabkan risiko terjadi
2. Risk Reduction, Mengambil tindakan untuk mengurangi kemungkinan atau dampak atau keduanya, biasanya melalui pengandalian di bagian internal perusahaan/organisasi
3. Risk Sharing or Transfer, Mengambil tindakan untuk mentransfer beberapa risiko melalui asuransi, outsourcing atau hedging.

4. Risk Acceptence, Tidak mengambil tindakan apapun untuk menganggulangi risiko, melainkan menerima risiko tersebut terjadi.
5. Create a Risk Management Plan

Membuat penanggulangan risiko yang tepat untuk setiap masing – masing kategori risiko. Mitigasi perlu mendapat persetujuan oleh level manajemen yang sesuai, berikut adalah contoh tabel manajemen risiko:

4. Implementation

Melaksanakan seluruh metode yang telah direncanakan untuk mengurangi atau menanggulangi pengaruh dari setiap risiko yang ada.

5. Evaluate and Review

Perencanaan yang telah direncanakan di awal tidak akan seluruhnya dapat berjalan dengan lancar. Perubahan keadaan atau lingkungan yang tidak diprediksi sebelumnya akan menyebabkan perubahan rencana manajemen risiko yang telah dibuat, oleh karena itu perlu dilakukan perubahan rencana untuk menanggulangi risiko yang akan mungkin terjadi.

3. teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi karena dengan berkembangnya teknologi sekarang beserta internet, menciptakan ancaman-ancaman baru yang juga lebih maju, sehingga teknologi harus lebih maju.

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?

---- Selamat bekerja ----

Jawaban :

1. Cara yang dilakukan dengan metode Pendekatan secara Psikologi, Kreatifitas menjadi kunci utama dari sosial Engineering. Untuk target orang terdekat biasa lebih mudah untuk mendapatkan userid dengan password dengan cara sering berinteraksi dengan target, membaca kebiasaan sehari-hari, kesukaan, hobby, aktifitas atau bisa juga menganalisa melalui Medsos. Dan selanjutnya, untuk target lain ada banyak cara salah satu menyisipkan Backdoor /malware agar tidak terlihat oleh korban. Misalnya menyisipkan exploit ke dalam file dokumen, menyisipkan backdoor kedalam aplikasi yang terlihat resmi, menyisipkan exploit pada flashdisk yang dijatuhkan di dekat lokasi target (begitu ada yang nemu biasanya penasaran untuk colok ke komputer). Selain itu, 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. Dalam managemen resiko keamanan asset Teknology Informasi dan Komunikasi (TIK), terlebih dulu kita harus paham ancaman apa saja yang biasa terjadi atau beberapa serangan yang dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Pertama kita haru pahami dulu 1. Reverse social engineering (RSE) : yaitu 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. Teknik ini biasanya menggunakan 3 langkah, Merusak, Menawarkan bantuan, dan beraksi. Dan dengan tahu tipe RSE ini kita bisa meminimalisir akibat yang akan ditimbulkan dengan cara membuat cadangan data, dan juga memperkuat sistem keamanan baik dari AntiVirus dan software lainnya.

3. Bagi saya teknologi usang yang menjadi ancaman bagi keamanan teknologi, salah satunya teknologi yang digunakan pada mesin ATM, Beberapa indikasi mengapa prasarana perbankan kurang aman lebih dari 80 persen mesin ATM di Indonesia masih menggunakan Windows XP, padahal Microsoft sudah menghentikan dukungan keamanannya (termasuk di daerah saya) waktu mau mengambil uang di ATM, tampilan muncul windows XP yang stuck di logo. Selain itu, teknologi kartu magnetik sekarang ini banyak digunakan pada kartu ATM nasabah merupakan teknologi lama (usang). Pita magnetik tidak dilengkapi dengan enkripsi sehingga dapat dibaca oleh semua alat pembaca pita magnetik. Bayangkan saja dengan teknologi usang yang masih digunakan, dalam hal keamanan masih sangat beresiko. Bagaimana solusi nya...menurut saya hardware dan software harus segera di upgrade mengikuti perkembangan teknologi.

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?

---- Selamat bekerja ----

Jawaban

1. **Brute Force**
   a. Brute Force berfokus pada kombinasi karakter yang digunakan dalam password. Keyword yang dipakai biasanya sesuai dengan algoritma yang dimiliki password manager, misalnya kombinasi antara beberapa huruf besar, huruf kecil, angka-angka, dan beberapa karakter simbol.
   Serangan brute force ini akan mencoba beberapa kombinasi dari karakter alfanumerik yang paling banyak dipakai, misalnya seperti 1q2w3e4r5t, zxcvbnm, dan qwertyuiop. Nah, apakah kalian termasuk yang menggunakan password seperti itu?
   Kelebihan cara ini adalah dapat menambah variasi serangan daripada hanya menggunakan kamus password saja. Jika akun kalian ingin aman dari serangan brute force, maka gunakan kombinasi karakter yang lebih bervariasi. Bila memungkinkan gunakan juga simbol-simbol ekstra untuk meningkatkan kompleksitas kata sandi.
   b. Malware/Keylogger
   Cara lain yang bisa membahayakan akun dan informasi penting di internet adalah karena adanya malware atau program jahat. Malware ini telah tersebar di seluruh jaringan internet dan berpotensi untuk terus berkembang. Bahayanya lagi jika kita sampai terkena malware dalam bentuk keylogger, maka secara tak sadar setiap aktivitas kita di komputer bisa diketahui oleh penyerang.
   Program malware ini sendiri secara khusus dapat menargetkan data pribadi, lalu penyerang bisa dengan mudah mengendalikan komputer korban dari jarak jauh untuk mencuri setiap informasi yang berharga.
   Bagi kalian yang tidak ingin terkena malware, maka jangan pernah menggunakan aplikasi bajakan. Lalu jangan malas untuk memperbarui software antivirus dan antimalware yang ada. Selain itu selalu berhati-hati saat browsing internet dan jangan asal downlad file dari sumber yang tidak jelas.

2. **Avoidance**
   a. Penghindaran isk adalah penghapusan bahaya, aktivitas, dan paparan yang dapat berdampak negatif terhadap aset organisasi.
      Sedangkan manajemen risiko bertujuan untuk mengendalikan kerusakan dan konsekuensi keuangan dari peristiwa yang mengancam, penghindaran risiko berusaha untuk menghindari peristiwa yang sepenuhnya dikompromikan.
      Walaupun jarang sekali menghilangkan semua risiko, strategi penghindaran risiko dirancang untuk menangkis ancaman sebanyak mungkin untuk menghindari konsekuensi yang mahal dan mengganggu dari peristiwa yang merusak. Metodologi penghindaran risiko berupaya meminimalkan kerentanan yang dapat menimbulkan ancaman. Penghindaran dan mitigasi risiko dapat dicapai melalui kebijakan dan prosedur, pelatihan dan pendidikan serta implementasi teknologi.

   b. Sebagai contoh, anggaplah seorang investor ingin membeli saham di perusahaan minyak, tetapi harga minyak telah turun secara signifikan selama beberapa bulan terakhir. Ada risiko politik yang terkait dengan produksi minyak dan risiko kredit yang terkait dengan perusahaan minyak. Dia menilai risiko yang terkait dengan industri minyak dan memutuskan untuk menghindari mengambil saham di perusahaan. Ini dikenal sebagai penghindaran risiko.

   c. Pengurangan Risiko
      Di satu sisi, pengurangan risiko berkaitan dengan memitigasi potensi kerugian. Misalnya, misalkan investor ini sudah memiliki stok minyak. Ada risiko politik yang terkait dengan produksi minyak, dan stok memiliki tingkat risiko tidak sistematis yang tinggi. Dia dapat mengurangi risiko dengan mendiversifikasi portofolionya dengan membeli saham di industri lain, terutama yang cenderung bergerak berlawanan arah dengan ekuitas minyak.
      Untuk terlibat dalam manajemen risiko, seseorang atau organisasi harus mengukur dan memahami kewajibannya. Evaluasi risiko keuangan ini adalah salah satu aspek yang paling penting dan paling sulit dari rencana manajemen risiko. Namun, sangat penting untuk kesejahteraan aset seseorang untuk memastikan Anda memahami cakupan penuh risiko Anda.
      Misalkan investor mendiversifikasikan portofolionya dan berinvestasi di berbagai sektor pasar. Namun, ia saat ini menghadapi risiko sistematis karena penurunan ekonomi. Investor dapat mengurangi risikonya melalui lindung nilai. Sebagai contoh, investor dapat melindungi posisi buy dan mengurangi risiko dengan membeli opsi put untuk posisi buy. Dia dilindungi dari potensi penurunan nilai portofolionya karena dia mampu menjual sahamnya dengan harga yang telah ditentukan dalam periode tertentu.
      Investor yang menghindari risiko kehilangan potensi keuntungan yang dimiliki stok minyak. Di sisi lain, investor yang mengurangi risikonya masih memiliki potensi keuntungan. Jika pasar saham bergerak lebih tinggi, posisi buynya akan menghargai nilainya. Namun, jika posisinya menurun nilainya, ia dilindungi oleh opsi putnya.
      Diversifikasi keuangan adalah salah satu strategi pengurangan risiko yang paling dapat diandalkan. Ketika risiko keuangan Anda terdiversifikasi, efek samping yang merugikan akan terdilusi. Jika Anda memiliki beberapa aliran pendapatan, misalnya, kehilangan satu aliran tidak akan banyak merugikan jika hanya 25% dari pendapatan seseorang berasal dari aliran itu.

3. **Sistem dan Aplikasi tidak pernah di update**
   Sistem lawas masih merajalela di sebagian besar industri dan tidak bisa dengan mudah diperbaharui atau diganti. Sistem-sistem ini sering mengandung kerentanan perangkat lunak yang diketahui oleh publik dan dapat dimanfaatkan untuk menembus jaringan perusahaan. Pada saat yang sama, peretas menjadi semakin canggih dan memiliki lebih banyak insentif untuk melakukan serangan siber.

Pemerintah dan perusahaan mengakui ancaman baru ini dan menerapkan solusi keamanan modern, namun akan memakan waktu bertahun-tahun untuk menghentikan dan memperbaharui semua sistem. tahun 2018 kembali menjadi salah satu tahun dimana kelemahan tersebut kembali menghantui kita. Lebih penting lagi, kita perlu mulai merencanakan masa depan untuk menghadapi ancaman-ancaman baru yang ditimbulkan oleh Internet of Things (IoT), yang akan melebihi apa yang telah kita alami dalam serangan siber.

Meskipun sistem manufaktur digunakan dalam lingkungan yang terisolasi, untuk kemudahan administrasi tetap saja masih terhubung dengan jaringan internet publik untuk, sehingga ancaman keamanan akan selalu ada. Keamanan sangat penting untuk keberhasilan adopsi *Industry 4.0*. Ketahanan proses produksi sangat tergantung pada kesadaran perusahaan manufaktur akan ancaman saat ini dan kerangka kerja keamanan yang digunakan untuk melindungi dari serangan.

IT Risk Management

Ujian Akhir Semester

Agus Sumitro

NIM 182420126

MTI20A

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?

---- Selamat bekerja ----

1. Metode yang digunakan untuk memperoleh User ID dan password dengan menggunakan Phising yaitu adalah tehnik untuk mendapatkan informasi sensitif(Data pribadi atau akun) dari korban dengan cara menulis email yang seolah-olah berasal dari website resmi.

   Contoh : 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

2. Lima strategi dasar untuk mengendalikan risiko

   Pertahanan - Menerapkan perlindungan yang menghilangkan atau mengurangi risiko yang tidak terkendali yang tersisa

   Contoh : dalam suatu jaringan computer LAN/WAN di pasang suatu hardware / software firewall untuk mencegah masuknya suatu virus atau aplikasi yang dapat menyusup dan merusak data dalam suatu jaringan.

   Transfer - Mengalihkan risiko ke area lain atau ke entitas luar

   Contoh : mengasuransikan seluruh asset dalam perusahaan sehingga apabila terjadi suati bencana yang diluar dugaan akan menjadi tanggung jawab pihak asuransi.

Mitigasi - Mengurangi dampak aset informasi jika penyerang berhasil mengeksploitasi kerentanan

Contoh : dalam mengelola suatu system IT penggunaan media backup misalnya server back up, power backup dan infrastructure jaringan internet back up disiapkan untuk mengantisipasi terjadinya suatu kegagalan dalam system .

Penerimaan - Memahami konsekuensi dari memilih untuk meninggalkan risiko yang tidak terkendali dan kemudian dengan benar mengakui risiko yang tetap tanpa upaya pengendalian

Contoh : dalam suatu perusahaan IT ada beberapa resiko keamanan yang sangat mungkin terjadi diantaranya pencurian informasi, penggunaan user yang tidak terotorisasi, perubahan data yang berlangsung tanpa disadari dan penghancuran data atau software yang dapat merusak suatu system dalam perusahaan, semua resiko itu tetap diupayakan pengendaliannya dengan mempersiapkan suatu system keamanan informasi yang di siapkan dalam suatu system baik hardware maupun software.

Pengakhiran - Menghapus atau menghentikan aset informasi dari lingkungan operasi organisasi

Contoh :apabila terdeteksi suatu serangan dalam sebuah system informasi maka seorang system engineer atau admin akan melakukan cut off dari suatu jaringan internet yang menghubungkan ke internet sehingga dapat segera dilakukan pengamanan data dan perbaikan celah2 yang berhasil ditembus oleh para penyusup dalam suatu jaringan.

3. Teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi karena teknologi yang lama memiliki celah2 keamanan yang dapat ditembus oleh orang – orang yang memanfaatkan keahlianya untuk melakukan kejahatan dalam dunia IT, misalnya dengan perkembangan penciptaan virus dan apliaksi yang bertujuan untuk memperoleh data authentifikasi user dan password. Bilamanana dengan teknologi yang lama tidak segera dilakukan upgrade atau update maka keamanan yang relative rendah akan mudah disusupi oleh virus dan aplikasi2 yang bisa merugikan .

AGUS WIRANTO - UAS

182420102 ➢ MTI2A1 ➢ 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!
   Jawaban:
   - **Metode Brute Force**
     Teknik hacking Brute Force adalah salah satu teknik hacking untuk meretas password sebuah server, jaringan, atau host, dengan cara mencoba semua kemungkinan kombinasi password yang ada pada wordlist atau "kamus password". Metode ini dijamin akan berhasil menemukan password yang ingin diretas. Namun proses untuk meretas password dengan menggunakan metode ini akan memakan banyak waktu.

     Mengapa disebut sebagai Brute Force? Nama "brute force" sendiri merupakan gabungan kata dari bahasa inggris, yang jika diterjemahkan ke dalam Bahasa Indonesia, memiliki arti "memaksa secara kasar". Hal tersebut sesuai dengan prinsip kerja dari teknik ini, dimana hacker akan berusaha menjebol password sebuah sistem dengan mencoba berbagai kombinasi password yang tertulis di dalam sebuah "kamus" berupa wordlist.

     Jika Anda mencoba memahami cara kerja dari teknik ini, Anda akan menemukan bahwa teknik ini akan melakukan penyerangan dari bagian depan saja. Anda membuka sebuah sistem, memasukan username seperti biasa, lalu Anda mencoba password mulai dari AAAA, AAAB, AAAC hingga ZZZZ. Yup, Anda seakan sedang berusaha mendobrak "pintu masuk" sebuah website dengan bekal "kamus password."

     Teknik ini sendiri sebenarnya tergolong sangat ampuh. Dengan suatu perangkat lunak khusus hacking, Anda bisa memasukan password sebuah sistem secara otomatis. Namun, jumlah password yang dimasukan mulai dari huruf A hingga ZZZZZ bisa jadi sangat banyak. Bahkan Anda harus memasukkan password ratusan kali. Memang, hal tersebut bisa dilakukan secara otomatis menggunakan perangkat lunak, tapi kamu juga harus menunggu perangkat lnuak tersebut memasukkan semua kemungkinan password hingga password berhasil ditemukan. Hal tersebut tentu saja akan memakan banyak waktu.

     Teknik brute force juga bisa memakan lebih banyak waktu lagi jika seandainya password yang hendak dijebol jumlah karakternya banyak. Bisa saja, password yang Anda jebol ternyata memiliki unsur @L4Y, misalkan saja "s1Be83PcanTique". Kemungkinan makan waktu pun bertambah jika server yang ingin Anda hack ternyata menerapkan rentang waktu 5 menit setiap sekali Anda memasukan password. Teknik ini juga tergantung dari kecepatan prosesor komputer yang digunakan untuk melakukan teknik brute force. Sehingga, bisa jadi total waktu yang dibutuhkan untuk melakukan teknik Brute Force ini dapat memakan waktu hingga 1000 tahun lamanya.

     Hal-hal yang perlu diperhatikan dalam menggunakan metode brute force attack :

     a. Asumsikan bahwa password diketik dalam huruf kecil (lower case).
        Pada kasus ini, waktu yang dibutuhkan akan cenderung sama tetapi jika password mengandung huruf kapital (upper case) cara ini tidak akan berhasil.

b. Coba semua kemungkinan.
   Tujuh karakter lower case membutuhkan sekitar 4 jam untuk berhasil mendapatkan password tetapi jika dicoba semua kemungkinan kombinasi antara karakter upper case dan lower case akan membutuhkan waktu sekitar 23 hari.
c. Metode ketiga adalah trade-off
   Hanya kombinasi-kombinasi yang mungkin yang dimasukkan dalam pencarian, sebagai contoh “password”, “PASSWORD” dan “Password”. Kombinasi rumit seperti “pAssWOrD” tidak dimasukkan dalam proses. Dalam kasus ini, lambatnya proses dapat tertangani tetapi ada kemungkinan password tidak ditemukan.

- **Contohny:**

Gambar di bawah ini mencontohkan 3 buah password dan waktu yang diperlukan tiap kelas komputer untuk menemukan passwordnya :

Sample Passwords		Class of Attack					
Pwd	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
[illegible]	308.4 Million	[illegible]	[illegible]	5 Mins	30 Secs	3 Secs	Instant
Lan$gu	3.5 Trillion	11 Years	1 Year	41 Days	4 Days	10 Hours	58 Mins
[illegible]	7.2 Quadrillion	[illegible]	[illegible]	229 Years	23 Years	2½ Years	9½ Days

Salah satu kasus yang dapat diteliti dengan algoritma ini adalah kasus untuk sebuah PIN ATM : PIN ATM kita yang menggunakan seluruhnya angka (C =10) dengan jumlah karakter 4 (n = 4) atau 6 (n = 6), maka dengan menggunakan algoritma/cara yang sama serangan dengan serangan dengan menggunakan bruteforce attack dapat ditabulasikan sbb:

Pass C=10	Kelas Serangan					
n	A	B	C	D	E	F
4	1s	0.1s	0.01s	0.001s	0.0001s	0.00001s
6	2m	10s	1s	0.1s	0.01s	0.001s

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

Jawaban:
Manfaat yang maksimal dari penerapan teknologi informasi akan dapat diperoleh dengan memiliki tata kelola teknologi informasi yang baik. Salah satu fokus area dari tata kelola teknologi informasi tersebut adalah pengelolaan risiko teknologi informasi

Perusahaan menyadari manfaat dari pengelolaan risiko apabila dilakukan, salah satunya adalah untuk menjamin keamanan informasi peru sahaan dan meminimalkan kerugian, sehingga perusahaan memiliki atensi yang tinggi untuk menjaga kemanan aset tenknologi informasi agar tidak hilang, tidak rusak dan terkelola dengan baik, mengingat, perkembangan teknologi informasi tidak terlepas dari kemungkinan risiko yang disebabkan oleh beberapa faktor. Menurut UU no 24 tahun 2007 faktor tersebut terdiri dari faktor alam, faktor nonalam, faktor ulah manusia, dan faktor teknologi. Atensi perusahaan akan diwujudkan dengan membuat pengelolaan risiko.

Contohnya pada Organisasi XYZ merupakan salah satu organisasi yang memiliki tugas pokok dan fungsi dalam bidang keamanan dan keselamatan di wilayah yurisdiksi laut NKRI. Dalam menjalankan tugas pokok dan fungsinya, secara umum organisasi XYZ memiliki sistem pengoperasian deteksi dini berbasis sistem teknologi informasi dalam upaya mencegah terjadinya pelanggaran-pelanggaran di wilayah kelautan NKRI yang dapat menyebabkan terganggunya stabilitas keamanan. Untuk mengetahui tingkat kematangan teknologi informasi yang dimiliki oleh organisasi XYZ dalam upayanya menjaga keamanan dan keselamatan laut Indonesia, organisasi XYZ telah mengikuti Desktop Assessment pada tahun 2014 yang menggunakan indeks KAMI versi 2.3 berbasis SNI ISO/IEC 27001:2009 . Berdasarkan hasil yang ada, organisasi XYZ berada pada tingkat kematangan I dari V tingkat kematangan. Sedangkan, menurut hasil evaluasi tingkat kesiapan dan capaian dari standar ISO tersebut, peran TI yang ada pada organisasi XYZ berada dalam status kesiapan dengan nilai 73 dari 588 pada kategori sedang. Hasil lainnya pada pemeringkatan indeks KAMI di tahun 2015 dengan menggunakan versi 3.1 berbasis SNI ISO/IEC 27001, hasil penilaian berupa kelengkapan penerapan standar tersebut terhadap sistem elektronik yang dimiliki oleh organisasi XYZ adalah 85 dari 645 untuk kategori dengan kerawanan tinggi.

Untuk mengatasi berbagai permasalahan tersebut, diperlukan suatu metode yang tepat untuk mencari akar dari dari berbagai jenis penyebab yang berpotensi menimbulkan kerawanan sistem dan membuat analisis untuk perbaikan dengan menggunakan Failure Mode and Effect Analysis (FMEA). FMEA merupakan teknik yang digunakan untuk mendefinisikan, mengidentifikasi, memprioritaskan dan menghilangkan permasalahan kegagalan sistem, baik permasalahan yang telah diketahui maupun yang potensial terjadi pada sistem. Metode FMEA dipilih karena metode ini mudah digunakan dan sudah populer digunakan pada bidang teknik industri. Bagaimana pun untuk penerapan di bidang sistem informasi masih sangat jarang dilaporkan. Dengan demikian tulisan ini ingin mengeksplorasi lebih jauh penggunaan metode FMEA di bidang sistem informasi

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

   Jawaban:

   Pemimpin global dalam solusi keamanan siber, mengumumkan penelitian baru yang mengacu kepada ancaman yang dihadapi jaringan manufaktur yang masih menggunakan teknologi yang sudah ketinggalan zaman, termasuk risiko terhadap kekayaan intelektual dan proses produksi. Diketahui hampir dua pertiga organisasi manufaktur menjalankan sistem operasi yang sudah ketinggalan zaman, sehingga meningkatkan risiko 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.

   Laporan ini menyoroti ancaman yang dihadapi manufaktur, termasuk risiko yang terkait dengan TI, *operational technology (OT)*, dan *IP.* Untuk membantu mengurangi dampak ancaman *Industry 4.0*, Trend Micro merekomendasikan produsen mengingat dasar-dasar keamanan siber, seperti membatasi akses pengguna dan menonaktifkan daftar direktori, serta mengidentifikasi dan memprioritaskan aset-aset utama untuk dilindungi.

   Meskipun sistem manufaktur digunakan dalam lingkungan yang terisolasi, untuk kemudahan administrasi tetap saja masih terhubung dengan jaringan internet publik untuk, sehingga ancaman keamanan akan selalu ada. Keamanan sangat penting untuk keberhasilan adopsi *Industry 4.0*. Ketahanan proses produksi sangat tergantung pada kesadaran perusahaan manufaktur akan ancaman saat ini dan kerangka kerja keamanan yang digunakan untuk melindungi dari serangan.

   Berikut beberapa langkah yang bisa ditempuh dalam rangka mengurangi risiko keamanan terhadap pada peralihan manufaktur menjadi Industry 4.0

1. Pembatasan pemberian izin terhadap individu yang bisa mengakses data dan sistem
2. Mengidentifikasi mesin-mesin yang sudah diatur agar bisa saling ‘berkomunikasi’ Seharusnya ada pembatasan untuk perangkat mana dalam jaringan TI yang harus mampu bertukar informasi dengan perangkat mana dalam jaringan operational technology (OT)
3. Layanan yang tidak perlu ada di dalam jaringan harus dinonaktifkan. Melakukan hal itu dapat membantu mencegah eksploitasi layanan yang rentan

Nama : Anshori

MTI 19 A.

Nim : 182420051

Konsentrasi : IT Insfrakstruktur.

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. Ditambahlagi, penggunaan TIse makin 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?

---- Selamatbekerja ----

Jawaban.

1. Metode yang digunakan oleh seorang social enggineering hacker adalah pertama-tama 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. 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 dai si korban.
contohnya ketika hacker berpura-pura dari bagian helpdesk dan memberitahukan kepada korban nya bahwa sistem nya 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. secara gak langsung si hacker dapet password baru dari si korban.

2. strategy yang dapat diterapkan untuk memanajemen resiko: Definisi umum dari Tata Kelola TI adalah pertanggung-jawaban eksekutif dan direksi yang melibatkan kepemimpinan, struktur organisasi, dan proses - dalam memastikan bahwa TI menjadi pendukung dan bagian dari realisasi strategi serta pencapaian tujuan organisasi. Terdapat lima bidang utama dalam Tata Kelola TI, yaitu:

1. *Stategic Aligment* : Keharmonisan antara TI dengan bisnis.
2. *Value Delivery*: Memastikan pemanfaatan penerapan TI.
3. *Risk Management*: Pengelolaan resiko penerapan TI dan pemanfaatan TI untuk mengendalikan resiko bisnis.
4. *Resource Management*: Pengelolaan kemampuan organisasi untuk menerapkan TI.
5. *Performance Measurement*: Pemantauan kinerja layanan TI

Bidang-bidang Tata Kelola TI di atas dilaksanakan secara berkesinambungan dengan melibatkan review dan evaluasi secara periodik. Selanjutnya bagaimana caranya untuk memulai implementasi Tata Kelola TI. Berikut ini proses-proses yang dapat dilakukan untuk menjadikan organisasi meraih *Good IT Governance*.

- Jadikan penerapan tatakelola TI sebagai suatu program penyempurnaan oranisasi secara berkesinambungan (bukan sekaligus dalam satu proyek)
- Pastikan bahwa hasil implementasi menjadi bagian dari operasional sehari-hari.
- Kita harus menyadari bahwa penerapan Tata Kelola TI juga melibatkan perubahan budaya. Pemberian motivasi dan insentif adalah salah satu kuncinya.
- Memastikan bahwa semua pihak yang berkepentingan mengetahui dan memahami tujuan yang akan dicapai.
- Menyamakan persepsi dan ekspektasi, bahwa penerapan Tata Kelola TI yang berhasil membutuhkan waktu dan penyempurnaan yang berkesinambungan.
- Secara berkesinambungan, fokuskan mulai dari yang paling mudah dan memberi dampak yang dapat dirasakan.
- Usahakan mendapat dukungan dan kepemilikan dari pimpinan puncak, terutama dengan menonjolkan prinsip-prinsip pengelolaan investasi TI yang baik.
- Hindari kesan yang hanya berupa pelembagaan birokrasi.
- Hindari pendekatan checklist yang tidak terfokus.

Contohnya: Dengan penerapan manajemen risiko secara terstruktur dan terintegrasi, organisasi akan mampu beradaptasi dengan memahami kondisi lingkungan sekitar sekaligus dapat memberikan kebijakan yang tepat untuk mencapai tujuan program.

3. ancaman yang dihadapi jaringan manufaktur yang masih menggunakan teknologi yang sudah ketinggalan zaman, termasuk risiko terhadap kekayaan intelektual dan proses produksi. Diketahui hampir dua pertiga organisasi manufaktur menjalankan sistem operasi yang sudah ketinggalan zaman, sehingga meningkatkan risiko 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.

Nama : Arie Ansyah
NIM : 182420117
IT Risk Management

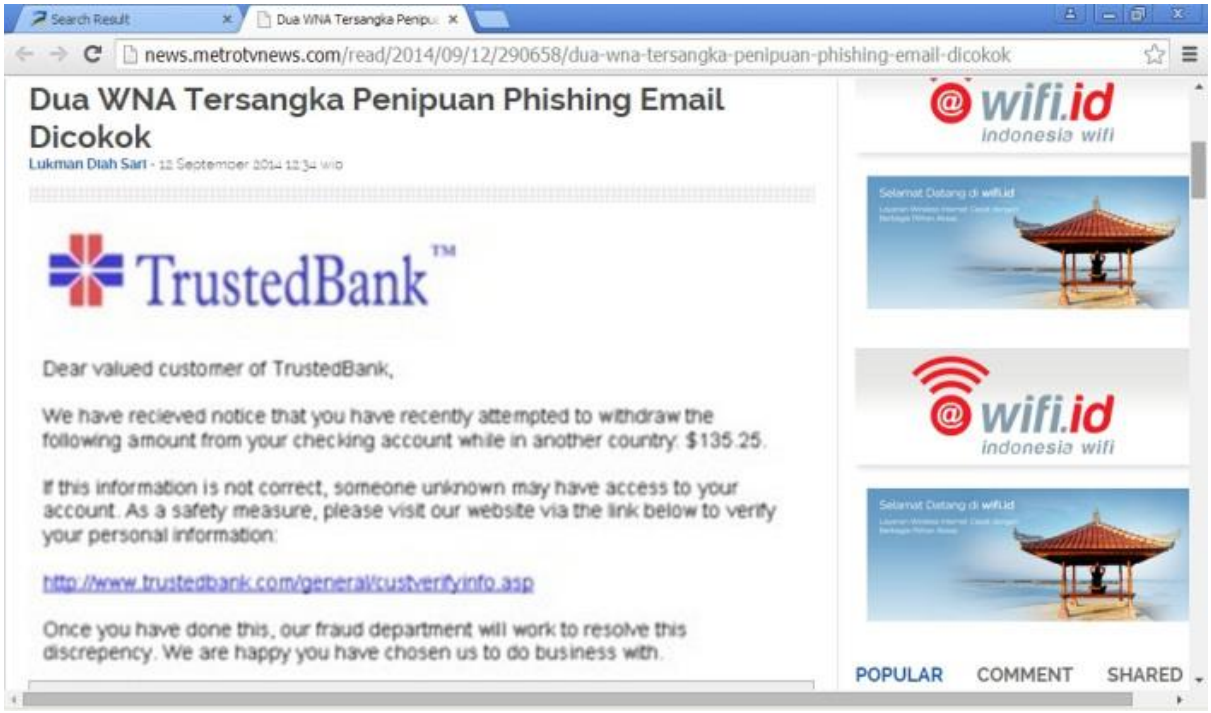
Pertanyaan:

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

    Phishing Attack

Phising adalah tindakan memperoleh informasi pribadi seperti User ID,Password dan data-data sensitive lainnya dengan menyamar sebagai orang atau oraganisasi yang berwenang melalui sebuah email. Istilah ini berasal dari Bahasa Inggris *fishing* yang berarti memancing. Dalam hal ini memancing target untuk memberikan informasi penting seperti informasi keuangan dan password yang dimilikinya.

Sebagai contoh pada kasus yang pernah terjadi pada Paypal. Dalam email phising tersebut akan tertulis untuk mengupdate data paypal dan mengganti password paypal karena akun yang korban miliki disinyalir telah disalahgunakan orang dan disertakan link menuju ke website yang mirip 100% seperti paypal yang sebenarnya website tersebut adalah buatan dari si hacker itu sendiri. Dengan cara ini hacker mendapatkan semua data yang diperlukan untuk mengambil alaih akun seseorang. Teknik ini bisa dikembangkan labih lanjut untuk mendapatkan sasaran tertarget atau yang bisa dikenal dengan spear phishing attack. Selain email, teknik ini juga menggunakan media social media seperti facebook untuk mendapatkan korban nya. Contoh lain :



Perusahan USA mengalami kerugian total lebih dari Rp. 3 miliar dengan delavan AG Pumps inc senilai USD 227,882.04 dan McNeilus Companies sebesar USD 101,430.74.

“Para hacker melakukan intercept, seolah-olah email yang komunikasi antara keduanya berasal dari China. Sehingga transaksi keuangan, bisa beralih ke perusahaan yang seolah-olah berasal China,” jelasnya.
Perusahaan USA digiring mentransfer pembayaran kepada perusahaan di Tiongkok menggunakan email seakan asli. “Mengarahkan kepada masing-masing perusahaan USA, mentransfer ke rekening Bank Mandiri atas nama PT.Kandva.

Setelah uang masuk ke rekening bank Mandiri, kemudian ditransfer lagi ke beberapa rekening dan ditarik tunai. Uang juga digunakan untuk belanja oleh yang menguasai rekening tersebut.

Dalam Resiko Managemen IT dikenal dengan Strategy Kontrol (Control Strategies). Strategi ini berguna untuk merespon setiap resiko terhadap penggunaan IT. Ada 4 strategi yang dikenal untuk mengatasi resiko IT. Disini anda diminta untuk mencocokan strategi tersebut dengan definisi atau strategi yang selayaknya dilakukan untuk merenspn suatu Resiko IT

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

   Untuk kegiatan perencanaan dalam IT Risk Manajemen dilakukan dengan beberapa step.

   Step pertama adalah indentifikasi setiap asset perusahaan termasuk asset digital (bisa berupa data, text, foto, chart dan sebaginya) maupun asset hardware (physical).

   Setelah itu, step kedua adalah kita harus mengidentifikasi resiko resiko atau ancaman yang mungkin terjadi pada setiap asset yang sudah kita indentifikasikan tersebut. Resiko resiko atau ancaman sangat banyak macamnya, bisa karena human error, pelanggaran HAKI, pencurian, serangan dunia maya, pengrusakkan secara pisik, bencana alam, kualitas service (mati listrik atau internet), peralatan rusak karena sudah berumur dan sebagainya.

Step ketiga adalah melakukan identifikasi kontrolnya, dalam hal ini maksudnya adalah untuk setiap resiko dan ancaman yang sudah ditulis dalam step dua tersebut diatas, dituliskan langkah langkah apa saja yang sudah dilakukan untuk mengurangi dampak resiko atau ancaman apabila ancaman tersebut benar benar terjadi.

Step ke empat adalah melakukan assessment, dimana pada intinya step ke empat ini adalah memberikan bobot untuk setiap asset sehingga kita dapat mengetahui asset mana saja yang sangat penting bagi perusahaan. Nantinya asset asset dengan bobot yang tinggi harus lebih diperhatikan ancamannya, kalau bisa kita harus menghilangkan ancaman atau resiko terhadap asset yang mempunyai bobot yang tinggi. Akhirnya kita harus membuat scenario bagaimana setiap resiko atau ancaman yang sudah kita identifikasikan itu bisa terjadi. Setelah ini semua selesai maka sekarang kita sudah dapat membuat rencana bagaimana untuk mengantisipasi apabila ancaman atau resiko tersebut benar benar terjadi. Dengan membuat rencana antisipasi ini maka diharapkan kita sudah siap apabila resiko atau ancaman tersebut benar benar terjadi sehingga perusahaan dapat tetap berjalan seperti biasa. Atau walaupun berhenti, maka perusahaan akan berhenti tidak akan terlalu lama.

cara mengurangi kecenderungan ancaman atau mengurangi dampak dengan cara melakukan kontrol terhadap kecenderungan dan dampak. Kecenderungan bisa dikurangi misalnya dengan melakukan maintenance regular terhadap sistem berbasis IT. Dampak bisa dikurangi misalnya dengan penyediaan backup system IT. Jika kecenderungan dan dampak dapat dikurangi maka secara keseluruhan tingkat risiko juga bisa dikurangi. Tingkat risiko sisa setelah dilakukan kontrol disebut "residual risk".

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

Dengan banyaknya perkembangan teknologi zaman sekarang baik dari segi infrakstruktur, jaringan dan telekomunikasi. Salah satu perkembangan teknologi tersebut adalah Cloud. Cloud bisa disebut sebuah teknologi yang mana dapat diakses dimanapun menggunakan jaringan internet. Menurut [1] cloud juga dapat mengarah kepada software dan service yang berjalan di internet dibandingkan di computer sendiri. Beberapa contoh layanan penyedia cloud diantaranya : Apple iCLoud, Dropbox, Netflix, Amazon cloud drive, Google Driver dan lain-lain. Banyak keuntungan yang didapatkan

jika menggunakan cloud diantaranya setiap data yang disimpan di Cloud, dapat diakses dimana saja dan kapanpun dengan menggunakan koneksi internet. Disamping beberapa keuntungan yang dimiliki oleh CLoud, cloud juga juga memiliki beberapa resiko keamanan. Risiko keamanan tersebut diantaranya

1. R1: Accountability & Data Risk
2. R2: User Identity Federation
3. R3: Regulatory Compliance
4. R4: Business Continuity & Resilliency
5. R5: User Privacy and Secondary Usage of Data
6. R6: Service and Data Integration
7. R7: Multi Tenancy and Physical Security
8. R8: Incidence Analysis and Forensic Support
9. R9: Infrastructure Security
10. R10: Non Production Environment Exposure

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?

---- Selamat bekerja ----

Jawaban menurut saya:

---

1. **A. Brute Force**
   Brute Force berfokus pada kombinasi karakter yang digunakan dalam password. Keyword yang dipakai biasanya sesuai dengan algoritma yang dimiliki password manager, misalnya kombinasi antara beberapa huruf besar, huruf kecil, angka-angka, dan beberapa karakter simbol.
   Serangan brute force ini akan mencoba beberapa kombinasi dari karakter alfanumerik yang paling banyak dipakai, misalnya seperti 1q2w3e4r5t, zxcvbnm, dan qwertyuiop. Nah, apakah kalian termasuk yang menggunakan password seperti itu?
   Kelebihan cara ini adalah dapat menambah variasi serangan daripada hanya menggunakan kamus password saja. Jika akun kalian ingin aman dari serangan brute force, maka gunakan kombinasi karakter yang lebih bervariasi. Bila memungkinkan gunakan juga simbol-simbol ekstra untuk meningkatkan kompleksitas kata sandi.

   B. Malware/Keylogger
   Cara lain yang bisa membahayakan akun dan informasi penting di internet adalah karena adanya malware atau program jahat. Malware ini telah tersebar di seluruh jaringan internet dan berpotensi untuk terus berkembang. Bahayanya lagi jika kita sampai terkena malware dalam bentuk keylogger, maka secara tak sadar setiap aktivitas kita di komputer bisa diketahui oleh penyerang. Program malware ini sendiri secara khusus dapat menargetkan data pribadi, lalu penyerang bisa dengan mudah mengendalikan komputer korban dari jarak jauh untuk mencuri setiap informasi yang berharga.Bagi kalian yang tidak ingin terkena malware, maka jangan pernah menggunakan aplikasi bajakan. Lalu jangan malas untuk memperbarui software antivirus dan antimalware yang ada. Selain itu selalu berhati-hati saat browsing internet dan jangan asal downlad file dari sumber yang tidak jelas.

2. **Avoidance**
   a. Penghindaran isk adalah penghapusan bahaya, aktivitas, dan paparan yang dapat berdampak negatif terhadap aset organisasi.
      Sedangkan manajemen risiko bertujuan untuk mengendalikan kerusakan dan konsekuensi keuangan dari peristiwa yang mengancam, penghindaran risiko berusaha untuk menghindari peristiwa yang sepenuhnya dikompromikan.
      Walaupun jarang sekali menghilangkan semua risiko, strategi penghindaran risiko dirancang untuk menangkis ancaman sebanyak mungkin untuk menghindari konsekuensi yang mahal dan mengganggu dari peristiwa yang merusak. Metodologi penghindaran risiko berupaya meminimalkan kerentanan yang dapat menimbulkan ancaman. Penghindaran dan mitigasi risiko dapat dicapai melalui kebijakan dan prosedur, pelatihan dan pendidikan serta implementasi teknologi.

   b. Sebagai contoh, anggaplah seorang investor ingin membeli saham di perusahaan minyak, tetapi harga minyak telah turun secara signifikan selama beberapa bulan terakhir. Ada risiko politik yang terkait dengan produksi minyak dan risiko kredit yang terkait dengan perusahaan minyak. Dia menilai risiko yang terkait dengan industri minyak dan memutuskan untuk menghindari mengambil saham di perusahaan. Ini dikenal sebagai penghindaran risiko.

   c. Pengurangan Risiko
      Di satu sisi, pengurangan risiko berkaitan dengan memitigasi potensi kerugian. Misalnya, misalkan investor ini sudah memiliki stok minyak. Ada risiko politik yang terkait dengan produksi minyak, dan stok memiliki tingkat risiko tidak sistematis yang tinggi. Dia dapat mengurangi risiko dengan mendiversifikasi portofolionya dengan membeli saham di industri lain, terutama yang cenderung bergerak berlawanan arah dengan ekuitas minyak.
      Untuk terlibat dalam manajemen risiko, seseorang atau organisasi harus mengukur dan memahami kewajibannya. Evaluasi risiko keuangan ini adalah salah satu aspek yang paling penting dan paling sulit dari rencana manajemen risiko. Namun, sangat penting untuk kesejahteraan aset seseorang untuk memastikan Anda memahami cakupan penuh risiko Anda.
      Misalkan investor mendiversifikasikan portofolionya dan berinvestasi di berbagai sektor pasar. Namun, ia saat ini menghadapi risiko sistematis karena penurunan ekonomi. Investor dapat mengurangi risikonya melalui lindung nilai. Sebagai contoh, investor dapat melindungi posisi buy dan mengurangi risiko dengan membeli opsi put untuk posisi buy. Dia dilindungi dari potensi penurunan nilai portofolionya karena dia mampu menjual sahamnya dengan harga yang telah ditentukan dalam periode tertentu.
      Investor yang menghindari risiko kehilangan potensi keuntungan yang dimiliki stok minyak. Di sisi lain, investor yang mengurangi risikonya masih memiliki potensi keuntungan. Jika pasar saham bergerak lebih tinggi, posisi buynya akan menghargai nilainya. Namun, jika posisinya menurun nilainya, ia dilindungi oleh opsi putnya. Diversifikasi keuangan adalah salah satu strategi pengurangan risiko yang paling dapat diandalkan. Ketika risiko keuangan Anda terdiversifikasi, efek samping yang merugikan akan terdilusi. Jika Anda memiliki beberapa aliran pendapatan, misalnya, kehilangan satu aliran tidak akan banyak merugikan jika hanya 25% dari pendapatan seseorang berasal dari aliran itu.

3. **Sistem dan Aplikasi tidak pernah di update**
   Sistem lawas masih merajalela di sebagian besar industri dan tidak bisa dengan mudah diperbaharui atau diganti. Sistem-sistem ini sering mengandung kerentanan perangkat lunak yang diketahui oleh publik dan dapat dimanfaatkan untuk menembus jaringan perusahaan. Pada saat yang sama, peretas menjadi semakin canggih dan memiliki lebih banyak insentif untuk melakukan serangan siber.
   Pemerintah dan perusahaan mengakui ancaman baru ini dan menerapkan solusi keamanan modern, namun akan memakan waktu bertahun-tahun untuk menghentikan dan memperbaharui semua sistem. tahun 2018 kembali menjadi salah satu tahun dimana

kelemahan tersebut kembali menghantui kita. Lebih penting lagi, kita perlu mulai merencanakan masa depan untuk menghadapi ancaman-ancaman baru yang ditimbulkan oleh Internet of Things (IoT), yang akan melebihi apa yang telah kita alami dalam serangan siber. Meskipun sistem manufaktur digunakan dalam lingkungan yang terisolasi, untuk kemudahan administrasi tetap saja masih terhubung dengan jaringan internet publik untuk, sehingga ancaman keamanan akan selalu ada. Keamanan sangat penting untuk keberhasilan adopsi *Industry 4.0*. Ketahanan proses produksi sangat tergantung pada kesadaran perusahaan manufaktur akan ancaman saat ini dan kerangka kerja keamanan yang digunakan untuk melindungi dari serangan.

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?

---- Selamat bekerja ----

1. Beberapa metode apa yang digunakan oleh seorang social engineering hacker untuk memperoleh userid dan password dari pengguna tertentu adalah :

a. **Brute Force** yaitu suatu percobaan memasukan segala kemungkinan kombinasi dari angka, huruf hingga karakter spesial dengan tujuan untuk bisa menebak password. Contoh aplikasi hydra

b. **Malware** ialah suatu cara dengan menggunakan aplikasi tertentu yang disebar & tertanam pada komputer tujuan. Contoh virus, worm, Trojan, backdoor dll..

c. **Phising** merupakan suatu metode mengelabui pengguna/taget sehingga mendapatkan infomasi yang dikendaki. Contoh dengan membuat halaman web palsu yang menyerupai halaman aslinya. halaman palsu tersebut, si korban akan memberikan username dan juga passwordnya.

2. Secara umum strategi untuk menerapan manajemen resiko di suatu organisasi adalah

a. **Kesadaraan semua pihak (yang paling penting manajemen puncak) tetang resiko.**

Dengan semua pihak mengetahui resiko, tahap selanjutnya mereka akan aware (peduli). Pihak yang paling diharapakan peduli dalam adalah manajemen puncak. Sehingga dapat membuat kebijakan.

b. **Membuat kebijakan dan struktur organisasi terhadap manajemen resiko IT.**

Setelah peduli, manajemen puncak membuat kebijakan dan prioritas terhadap resiko yang dimiliki

Untuk mengimplementasikan kebijakan tersebut, manajemen harus membuat struktur organisasi yang melibatkan semua pihak. Dimana dalam struktur organisasi tersebut memuat uraian tugas dan tanggun jawab.

c. Membuat rencana dan program kerja manajemen risiko keseluruh lini perusahaan.

Setelah kebijakan & struktur organisasi, membuat rencana dan program kerja terkait sehingga implementasi lebih terarah, sestimatis dan terukur.

d. Melakukan monitoring, pelaporan dan evaluasi berkala manajemen resiko.

Monitoring & pelaporan diperlukan terhadap rencanan dan program kerja yang telah ditentukan. Monitoring dan pelaporan diperlukan sebagai bahan evaluasi untuk improvement.

e. Menjadikan manajemen risiko IT budaya dan nilai-nilai dalam suatu organisasi.

Dengan menjadikan manajemen resiko IT budaya dan nilai di suatu organisasi, membuat penerapan menjadi efektif.

3.Teknologi yang usang berkontribusi menjadi ancaman karena :

a. **Keandalan**. Teknologi usang biasanya biasanya ditemukan bug/celah & sudah tidak dapat update. Dan disisi lain teknologi baru telah menutup celah dan membuat lebih efektif & efisien. Dan teknologi baru sudah menjadi trend sehingga mengalami kendala dalam hubungan berbisnis.

b.**Kerentanan keamanan**. Teknologi using dapat membuat menjadi target utama untuk serangan cyber. Faktanya, penelitian menunjukkan bahwa lebih dari 10.000 ancaman malware baru ditemukan setiap jam. Jika teknologi tidak selalu mutakhir, risiko akan terus meningkat.

Nama : Ekariva Annas Asmara
NIM : 182420133
Kelas : Reguler A

UAS IT RISK MANAGEMENT

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

   Jawaban :

   - **Apa itu Social engineering attack?**

     Social engineering adalah manipulasi psikologis seseorang dengan tujuan untuk mendapatkan informasi/hak akses tertentu guna melakukan hal tertentu dengan cara menipu user secara halus tanpa user sadari.

   - **Bagaimana Social Enginnering attack dilakukan?**

     Manipulasi psikologis dikakukan dengan berbagai media yang tujuan nya untuk mempengaruhi pikiran korban,misalnya :

     - ✓ Menggunakan suara saat menipu seseorang penipu bisa berbicara untuk meyakinkan korban
     - ✓ Menggunakan gambar/video spammer memasang gambar/video yang erotis/menarik agar di klik
     - ✓ Menggunakan tulisan hacker menulis artikel yang persuasif dan meyakinkan dengan menulis tutorial cara hack akun facebook, tapi

akhirnya korban dituntun untuk menginstall tool hacking yang aslinya adalah malware.

- **Siapa Pelaku Social Engineering Attack**

  Semua kriminal 100% menggunakan tehnik ini untuk mendapatkan informasi dari korban nya. mulai dari tukang copet yang menyamar sebagai penumpang biasa, penipu yang menjanjikan hal luar biasa pada korban nya,sexpredator yang menggunakan facebook untuk berinteraksi dengan korban nya.

- **Kenapa Menggunakan Social Engineering Attack?**

  Social engineering mentargetkan rantai terlemah dalam sistem keamanan komputer, yaitu user atau pengguna atau manusia itu sendiri.

  Bug atau celah keamanan ini bersifat universal, tidak tergantung platform, sistem operasi, protocol, software ataupun hardware.

  Dengan artian,semua sistem tercanggih di planet ini memiliki celah keamanan tersebut.

- **User Adalah Titik Terlemah Dalam Sistem Keamanan**

  Untuk mendapatkan sebuah akses ke sebuah sistem (komputer,gedung,relasi,komunitas,rasa percaya kita) bisa dilakukan dengan melakukan pendekatan dengan manusia itu sendiri untuk mendapatkan kepercayaan agar pelaku social engineer bisa melakukan apa yang dia inginkan tanpa korban sadari.

  ketika sadar itu sudah sangat terlambat. jadi yang disebut sistem disini bukan hanya komputer tetapi bisa juga pikiran kita sendiri,keamanan sebuah gedung,sebuah kommunitas dll.

Contoh Social Engineering Attack Yang Populer

Dalam dunia security ada beberapa tehnik social engineering yang biasa digunakan antara lain:

1) **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:

- **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.

- **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

- **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. Tehnik ini sering kita lihat di filem-filem box office. dimana pemeran utama menyamar menjadi teknisi atau IT konsultan untuk bisa mengakses perangkat secara fisik/remote dan menanam backdoor.

2) **PiggyBack Ride Attack**

Piggiback 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

3) **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.

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

Jawaban :

Kegunaan sistem informasi dalam mendukung proses bisnis organisasi semakin nyata dan meluas. Sistem informasi membuat proses bisnis suatu organisasi menjadi lebih efisien dan efektif dalam mencapai tujuan. Sistem informasi bahkan menjadi *key-enabler* (kunci pemungkin) proses bisnis organisasi dalam memberikan manfaat bagi *stakeholder*s. Maka dari itu, semakin banyak organisasi, baik yang berorientasi profit maupun yang tidak, mengandalkan sistem informasi untuk berbagai tujuan. Di lain pihak, seiring makin meluasnya implementasi sistem informasi maka kesadaran akan perlunya dilakukan review atas pengembangan suatu sistem informasi semakin meningkat. Kesadaran ini muncul karena munculnya berbagai kasus yang terkait dengan gagalnya sistem informasi, sehingga memberikan akibat yang sangat mempengaruhi kinerja organisasi.

- Terdapat beberapa resiko yang mungkin ditimbulkan sebagai akibat dari gagalnya pengembangan suatu sistem informasi, antara lain:
  1. Sistem informasi yang dikembangkan tidak sesuai dengan kebutuhan organisasi.

2. Melonjaknya biaya pengembangan sistem informasi karena adanya "scope creep" (atau pengembangan berlebihan) yang tanpa terkendali.
3. Sistem informasi yang dikembangkan tidak dapat meningkatkan kinerja organisasi

Risiko Keamanan Informasi (Information Security Risk) didefinisikan sebagai potensi output yang tidak diharapkan dari pelanggaran keamanan informasi oleh Ancaman keamanan informasi. Semua risiko mewakili tindakan yang tidak terotorisasi. **Risiko-risiko seperti ini dibagi menjadi empat jenis yaitu**:

1. Pengungkapan Informsi yang tidak terotoritasis dan pencurian. Ketika suatu basis data dan perpustakaan peranti lunak tersedia bagi orang-orang yang seharusnya tidak memiliki akses, hasilnya adalah hilangnya informasi atau uang.
2. Penggunaan yang tidak terotorisasi. Penggunaan yang tidak terotorisasi terjadi ketika orang-orang yang biasanya tidak berhak menggunakan sumber daya perusahaan mampu melakukan hal tersebut.
3. Penghancuran yang tidak terotorisasi dan penolakan layanan. Seseorang dapat merusak atau menghancurkan peranti keras atau peranti lunak, sehingga menyebabkan operasional komputer perusahaan tersebut tidak berfungsi.
4. Modifikasi yang terotorisasi. Perubahan dapat dilakukan pada data, informasi, dan peranti lunak perusahaan yang dapat berlangsung tanpa disadari dan menyebabkan para pengguna output sistem tersebut mengambil keputusan yang salah.

- **Contoh resiko penggunaan system informasi dalam perusahaan**

  Teknologi informasi memiliki peranan penting bagi setiap organisasi baik lembaga pemerintah maupun perusahaan yang memanfaatkan teknologi informasi pada kegiatan bisnisnya, serta merupakan salah satu faktor

dalam mencapai tujuan organisasi. Peran TI akan optimal jika pengelolaan TI maksimal. Pengelolaan TI yang maksimal akan dilaksanakan dengan baik dengan menilai keselarasan antara penerapan TI dengan kebutuhan organisasi sendiri.

Semua kegiatan yang dilakukan pasti memiliki risiko, begitu juga dengan pengelolaan TI. Pengelolaan TI yang baik pasti mengidentifikasikan segala bentuk risiko dari penerapan TI dan penanganan dari risiko-risiko yang akan dihadapi. Untuk itu organisasi memerlukan adanya suatu penerapan berupa Tata Kelola TI (*IT Governance*) (Herawan, 2012).
Pemanfaatan dan pengelolaan Teknologi Informasi (TI) sekarang ini sudah menjadi perhatian di semua bidang dikarenakan nilai aset yang tinggi yang mempengaruhi secara langsung kegiatan dan proses bisnis. Kinerja TI terhadap otomasi pada sebuah organisasi perlu selalu diawasi dan dievaluasi secara berkala agar seluruh mekanisme manajemen TI berjalan sesuai dengan perencanaan, tujuan, serta proses bisnis organisasi. Selain itu, kegiatan pengawasan dan evaluasi tersebut juga diperlukan dalam upaya pengembangan yang berkelanjutan agar TI bisa berkontribusi dengan maksimal di lingkungan kerja organisasi.

- **Penilaian risiko keamanan informasi (*Information Security Risk Assessment*)**

a) Membangun dan memelihara kriteria risiko keamanan informasi yang meliputi:
   1. kriteria *risk acceptance*
   2. kriteria untuk melakukan penilaian risiko keamanan informasi

b) Memastikan bahwa penilaian risiko keamanan informasi yang dilakukan secara berulang menghasilkan hasil yang konsisten, valid, dan dapat diperbandingkan (*comparable)*

c) Mengidentifikasi risiko keamanan informasi :

1. menerapkan proses penilaian risiko keamanan informasi untuk mengidentifikasi risiko yang berkaitan dengan hilangnya aspek *confidentiality*, *integrity*, dan *availability* untuk informasi di dalam ruang lingkup sistem manajemen keamanan informasi
2. mengidentifikasi *risk owner*

d) Menganalisis risiko keamanan informasi:
1. menilai potensi konsekuensi berdasarkan risiko yang telah teridentifikasi
2. menilai.kemungkinan (*likelihood*) kejadian berdasarkan risiko yang telah teridentifikasi
3. menentukan tingkatan risiko

e) Mengevaluasi risiko keamanan informasi:
1. membandingkan hasil dari analisis risiko dengan kriteria yang telah dibuat
2. menentukan prioritas untuk melakukan *risk treatme*

- **Strategi Penanganan Risiko Keamanan Informasi (*Information Security Risk Treatment*)**

a) memilih opsi penanganan risiko yang sesuai
b) menentukan semua kendali yang mencukupi untuk mengimplementasikan pilihan penanganan risiko keamanan informasi
c) membandingkan kendali yang telah ditentukan dengan Annex A dan melakukan verifikasi untuk memastikan bahwa tidak ada kendali penting yang diabaikan.
d) menghasilkan *Statement of Applicability* yang mengandung kendali yang dibutuhkan serta justifikasi yang menentukan apakah kendali telah diimplementasikan atau tidak.
e) memformulasikan perencanaan penanganan risiko keamanan informasi
f) memperoleh persetujuan dari *risk owner* terkait perencanaan

penanganan risiko keamanan informasi dan persetujuan dari resiko residu keamanan informasi

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

Jawaban :

Teknologi Usang (obsolete) adalah teknologi yang sudah tidak lagi dikembangkan karena munculnya teknologi pengganti yang lebih baik

Penggunaan teknologi informasi menyimpan potensi ancaman terhadap keamanan data, keamanan fisik, keamanan dari perangkat, regulasi, privasi, enkripsi, otentikasi, dan segudang ancaman lain yang perlu ditangani agar kendala tersebut tidak mengganggu di kemudian harinya. Hal ini serupa dengan yang terjadi pada tren komputasi cloud, sebagai pendukung dari IoT, beberapa tahun lalu. Kasus-kasus hacking data antar perusahaan yang santer diberitakan menjadi contoh dari kelalaian perhatian terhadap segi keamanan konsep IoT ini. Hal lain yang patut diperhatikan adalah, Internet of Things bukan saja melulu mengenai "Things" atau perangkatnya, melainkan aplikasi dan layanan yang menjadi pendukung dari IoT. Semakin banyak perangkat terkoneksi, maka akan semakin banyak pula aplikasi dan layanan yang berjalan. Seperti misalnya, penghitungan meteran listrik otomatis, jam tangan pintar yang dapat mengukur detak jantung dan langsung menampilkan hasilnya di layar ponsel, dan sebagainya. Di baliknya, terdapat berbagai aplikasi yang bekerja secara simultan atau pun bersamaan untuk menghasilkan data-data tersebut. Risiko seperti aplikasi yang 'macet' di tengah jalan sudah umum terjadi dan ini memerlukan perhatian khusus.

Kecanggihan yang ada di dalam IoT itu sendiri menebar ancaman. Seperti beberapa waktu lalu ketika ada *hacker* asal Rusia yang melakukan *surveillance* melalui webcam dan memonitor aktivitas manusia di dunia. Hal tersebut hanyalah satu di antara ancaman yang bisa terjadi ketika IoT sudah

sepenuhnya terpasang. Ancaman itu sendiri akan semakin rumit dan beragam manakala IoT telah terintegrasi di smart city. Richard Moulds, VP Strategy di Thales e-Security mengatakan bahwa IoT menjadikan semua data yang ada menjadi semakin tebal dan hal ini menurutnya sangat rentan terhadap ancaman siber. “Masalahnya adalah perangkat yang digunakan untuk IoT itu sering kali berada di wilayah yang tidak aman,” papar Moulds. Hal lainnya yang menjadikan ancaman IoT itu semakin kompleks karena perangkat yang terintegrasi mengikuti tingkah laku manusia dan dapat memfungsikan dirinya sendiri. Brandon Creighton dari Veracode menyatakan, “Sangat sulit diprediksi seperti apa keadaan IoT di masa depan. Satu hal yang pasti, keamanan siber jangan sampai diabaikan.” Salah satu saran yang ia kemukakan dalam persoalan keamanan IoT ini adalah semua perangkat harus tersambung ke cloud. “Di sanalah aspek keamanan diterapkan,” papar Creighton.

Dalam blog Symantec berjudul ‘The Internet Of Things–New Threats Emerge in a Connected World’, perusahaan sekuriti ini membahas tentang potensi ancaman keamanan yang telah terjadi, bahkan ketika IOT masih dalam tahap awal.

Salah satu contoh utama adalah worm yang menargetkan komputer yang berjalan dengan Linux OS, yang baru-baru ini ditemukan oleh Kaoru Hayashi, penyidik Symantec. Worm ini awalnya tampaknya biasa-biasa saja–meninggalkan backdoor pada komputer yang telah tersusupi, yang memungkinkan penyerang untuk mengeluarkan perintah-perintah kepadanya. Meskipun komputer sering di-patched, Hayashi menemukan bahwa perangkat seperti home routers, set-top boxes, kamera-kamera keamanan, dan sistem kontrol industri rentan karena beberapa vendor tidak menyediakan update, disebabkan karena keterbatasan hardware atau **teknologi yang usang, seperti ketidakmampuan untuk menjalankan versi-versi terbaru dari software.**

FAJAR PRAYOGA
182420136

Pertanyaan :

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh user id 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. 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

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

---- Selamat bekerja ----

Jawaban :

1. **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 untuk maksud tertentu. 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, 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. **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. Phising banyak memakan korban di sektor social media, hal itu dikarenakan social media merupakan akun harian yang sering digunakan oleh

pengguna, tanpa sadar pengguna memasuki halaman jebakan yang menyebabkan pengguna bisa saja terjebak karena halaman palsu tersebut. Tidak hanya itu, phising juga terkadang bisa terjadi manipulasi dimana komputer yang terinfeksi bisa saja memanipulasi beberapa hal yang membuat halaman itu merupakan halaman aslinya, sehingga perlu diperhatikan untuk komputer anda tidak terkena virus untuk menghindari kasus ini. Banyak sekali kasus kejahatan phising yang sering dilakukan, terlebih hal itu bisa saja mencuri banyak informasi anda seperti akses akun Anda, email, social media, bahkan akun Bank Anda. Untuk menghindari phising, pengguna harus lebih berhati-hati dengan memperhatikan beberapa hal keamanan.

2. Untuk perusahaan yang baru saja berkembang strategi manajemen risiko yang baik dan efektif akan sangat membantu perusahaan tersebut. Dengan adanya strategi yang efektif risiko yang terjadi dapat diminimalisir atau bahkan bisa dihilangkan, itu sangat membantu perusahaan untuk menghindari terjadinya kegagalan perusahaan akibat risiko yang ditimbulkan. Jika risiko yang terjadi tidak signifikan dampaknya mungkin perusahaan bisa menghandel risiko tersebut, melainkan jika risiko yang terjadi sangatlah besar, maka kecil kemungkinan perusahaan yang baru berkembang untuk bangkit dari risiko yang telah terjadi. Sehingga, untuk menghindari hal yang tidak diinginkan, berikut akan dijabarkan strategi untuk melakukan manajemen risiko secara efektif dan efisien untuk perusahaan yang sedang berkembang :

1. Melakukan perencanaan manajemen risiko, Langkah awal yang dilakukan adalah melakukan perencanaan manajemen risiko. Dengan melakukan perencanaan kita dapat memutuskan bagaimana manajemen risiko yang baik dan sesuai untuk proyek yang akan dilakukan. Perencanaan manajemen risiko mempertimbangkan lingkup proyek, rencana manajemen proyek, faktor lingkungan perusahaan, maka tim proyek dapat mendiskusikan dan menganalisis aktivitas manajemen risiko untuk proyek-proyek tertentu. Untuk membuat perencanaan risiko ada hal –hal yang pendukung perencanaan seperti project charter, kebijakan manajemen risiko, susunan peran dan tanggung jawab, toleransi stackholder terhadap risiko, template untuk rencana manajemen risiko dan work breakdown structure (WBS).

2. Melakukan pengidentifikasian risiko, Setelah kita merancang bagaimana manajemen risiko yang akan diterapkan di perusahaan, langkah selanjutnya adalah melakukan pengidentifikasian risiko dengan memahami terlebih dahulu risiko yang akan terjadi pada proyek yang dijalankan. Identifikasi risiko dapat dilakukan dengan analisis sumber risiko dan analisis masalah Analisis sumber risiko yaitu analisis risiko dengan melihat darimana risiko berasal. Ada tiga sumber risiko yang sudah banyak dikenal yakni Risiko internal yakni risiko yang bersumber dari internal organisasi yang dapat dikategorikan dalam non technical risk (manusia, material, keuangan) dan technical risk (disain, konstruksi dan operasi). Beberapa perusahaan dan industri melihat daftar periksa risiko berdasarkan pengalaman dari proyek-

proyek masa lalu. Daftar periksa ini dapat membantu manajer proyek dan tim proyek dalam mengidentifikasi risiko yang spesifik pada daftar periksa dan memperluas pemikiran tim. Pengalaman masa lalu dari tim proyek, pengalaman proyek di dalam perusahaan, dan para ahli di industri ini dapat menjadi sumber berharga untuk mengidentifikasi potensi risiko pada sebuah proyek.

3. Mengevaluasi risiko, Setelah risiko potensial teridentifikasi, tim proyek kemudian mengevaluasi setiap risiko berdasarkan probabilitas kejadian risiko akan terjadi dan potensi kerugian yang terkait dengannya. Tidak semua risikonya sama. Beberapa kejadian berisiko lebih mungkin terjadi daripada yang lain, dan biaya risiko bisa sangat bervariasi. Mengevaluasi kemungkinan terjadinya risiko dan tingkat keparahan atau potensi kerugian proyek adalah langkah selanjutnya dalam proses manajemen risiko.

4. Melakukan rencana mitigasi, Setelah risiko diidentifikasi dan dievaluasi, tim proyek mengembangkan rencana mitigasi risiko, yang merupakan rencana untuk mengurangi dampak kejadian tak terduga. Tim proyek mengurangi risiko dengan berbagai cara yaitu risk avoidance, risk sharing, risk reduction dan risk transfer. Masing-masing teknik mitigasi ini bisa menjadi alat yang efektif dalam mengurangi risiko individu dan profil risiko proyek. Rencana mitigasi risiko akan melakukan pendekatan mitigasi untuk setiap kejadian risiko yang teridentifikasi dan tindakan yang akan diambil oleh tim manajemen proyek untuk mengurangi atau menghilangkan risiko tersebut.

5. Memindahkan Risiko, Jika risiko tidak bisa ditangani oleh perusahaan secara internal, maka risiko tersebut bisa dipindahkan kepada pihak-pihak yang bisa membantu untuk menangani risiko tersbut. Maksud pihak yang bisa membantu menangani risiko yang ada adalah perusahaan asuransi. Jika risiko yang terjadi adalah hal-hal yang berhubungan dengan kejadian tak terduga seperti kebakaran, pencurian atau kerusakan, maka jasa perusahaan asuransi akan meringankan beban perusahaan dalam menangani risikonya.

3. **Karena** yang perlu digaris bawahi dalam membuat rencana sistem keamanan adalah menganalisis risiko-risiko yang mungkin ada, termasuk risiko yang timbul dari dalam sistem. Perlu diingat ancaman keamanan sistem tak hanya bisa ditemukan dari luar sistem. Kemungkinan ancaman dari dalam sistem pun banyak ditemukan. Untuk minimalisir hal tersebut perlu dibuat pemetaan atau rencana penanggulangan risiko TI, baik dari dalam maupun dari luar, misalnya dengan membuat rencana kontrol hak akses sistem atau menempatkan *firewall* di dalam sistem jaringan. Masih berkaitan dengan ancaman dari dalam, semua orang yang berada di dalam sistem harus memiliki dasar keamanan TI. Hal ini untuk mencegah kasus bocornya data atau masuknya perangkat lunak berbahaya ke dalam sistem. Pengetahuan dasar keamanan juga berguna untuk memberikan wawasan mengenai ancaman keamanan dan cara pencegahannya. **Contohnya**, untuk mencegah pegawai dari tipuan *phising* yang sering mengincar orang awam atau orang-orang yang tidak memiliki pengetahuan tentang ancaman keamanan. **Contoh**

lain, mencegah penggunaan flashdisk yang sembarangan, membuat *password* yang tidak mudah ditebak, dan pengelolaan akun yang baik.

Nama : Gian Pratama

NIM : 182420116

Kelas : MTI20A

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?

---- Selamat bekerja ----

1. Social Engineering adalah sebuah metode hacking dengan memanfaatkan kelemahan sisi psikologi manusia. Dilakukan dengan cara memanipulasi korban secara halus, tanpa korban sadari, demi mendapat userid & password. Biasanya teknik ini dilakukan dengan menipu & mempengaruhi pikiran korban. Beberapa ragam teknik yang dikenal, antara lain: Phising, Pretexting, Baiting, Quid Pro Quo, dan Tailgating. Sebagai contoh, teknik penipuan menggunakan phising dapat dilakukan dengan cara berpura-pura mengatasnamakan situs resmi seperti bank, social media facebook, atau perusahaan lain yang mengharuskan korban untuk memasukkan email & password, padahal sebenarnya situs/aplikasi tersebut palsu buatan si hacker.

---

2. Misalkan pada sebuah perusahaan membutuhkan manajemen resiko terhadap sistem IT yang dimiliki. Tahap pertama ialah mengidentifikasi setiap resiko yang mungkin muncul dan mempengaruhi kinerja. Melakukan pengecekan terhadap setiap sistem IT yang digunakan, baik itu software, hardware, data-data critical, dsb. Kemudian mengidentifikasi sejarah kerusakan & penyerangan (*system attack*) yang pernah dialami. Identifikasi selanjutnya ialah dilakukan identifikasi kerentanan yang mungkin dapat terjadi (*vulnerability identification*). Kemudian perusahaan dapat menentukan kemungkinan dan konsekuensi dari setiap resiko tersebut, dengan mengembangkan pemahaman tentang sifat resiko dan potensi pengaruh terhadap sasaran proyek.

Selanjutnya, dilakukan kontrol terhadap sistem dan melihat resiko-resiko yang secara aktual mulai muncul dikarenakan sistem sudah berjalan. Resiko-resiko yang sudah muncul tersebut kemudian dievaluasi dan ditentukan pengaruhnya, apakah resiko tersebut dapat diterima, dapat diatasi atau tidak, dan menentukan langkah untuk menghindari resiko lebih besar yang dapat muncul kapan saja.

3. Semakin hari, sebuah teknologi baru akan semakin terkenal luas & digunakan di masyarakat. Artinya, teknologi tersebut akan banyak digunakan, baik oleh orang yang mengambil manfaat dari teknologi tersebut, termasuk juga orang yang ingin berbuat jahat dengan teknologi tersebut. Semakin lama sebuah teknologi beredar, semakin rentan ditemukan celah ancaman yang dapat dieksploitasi oleh orang-orang yang tidak bertanggung jawab. Untuk itu diperlukan update sistem & dukungan dari developer untuk menutup celah yang ditemukan.

Kemudian, cepat atau lambat, akan sampai pada suatu ketika dimana teknologi tersebut digantikan dengan teknologi yang lebih baru lagi, karena ditemukan sistem yang lebih mutakhir, lebih cepat, lebih murah, dan lebih aman. Teknologi sebelumnya akan menjadi usang dan mulai banyak ditinggalkan, baik oleh pengguna, maupun developer teknologi tersebut. Dengan tidak adanya update berkala dan dukungan dari developer lagi, akan sangat rentan terhadap ancaman dan eksploitasi bila pengguna masih menggunakan teknologi usang tersebut, sehingga diperlukan upgrade ke teknologi yang lebih baru.

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?

Nama : **Hari Febriadi**
NIM : **182420127**
Mapel : IT Risk Management

---- Selamat bekerja ----

Jawaban

1.

Ada 9 cara yang bisa dilakukan salah satunya adalah : yang pernah saya lakukan terhadap korban nya adalah "***Phishing Attack (Scamming)***" adalah teknik dimana untuk mendapatkan informasi korban seolah olah berasal dari website resmi, **contoh nya** adalah ketika saya membuat salinan web facebook yang di desain sama untuk menjebak target supaya mengisikan id dan password nya, kemudian data pribadi tersebut akan tersimpan langsung ke database saya. Biasanya jebakan seperti ini lebih cepet terjerat ke target yang sudah mengenal kita dengan baik.

2.

Pengendalian (control) adalah mekanisme yang diterapkan baik untuk melindungi perusahaan dari resiko atau untuk meminimalkan dampak resiko tersebut pada perusahaan jika resiko tersebut terjadi. Contoh **PENGENDALIAN TEKNIS** yang diambil

---

Pengendalian teknis (*technical control*) adalah pengendalian yang menjadi satu di dalam system dan dibuat oleh para penyusun system selama masa siklus penyusunan system. Didalam pengendalian teknis, jika melibatkan seorang auditor internal didalam tim proyek merupakan satu cara yang amat baik untuk menjaga agar pengendalian semacam ini menjadi bagian dari desain system. Kebanyakan pengendalian keamanan dibuat berdasarkan teknologi peranti keras dan lunak.

Contoh Dasar untuk keamanan melawan ancaman yang dilakukan oleh orang-orang yang tidak diotorisasi adalah pengendalian akses. **Alasannya sederhana:** Jika orang yang tidak diotorisasi tidak diizinkan mendapatkan akses terhadap sumber daya informasi, maka pengrusakan tidak dapat dilakukan.

3.

Selain teknologi yang usang dapat menjadi ancaman pada sistem informasi yaitu penyalahgunaan teknologi untuk kejahatan kriminal yaitu :

- 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.

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?

Nama : **Hari Febriadi**
NIM : **182420127**
Mapel : IT Risk Management

---- Selamat bekerja ----

Jawaban

1.

Ada 9 cara yang bisa dilakukan salah satunya adalah : yang pernah saya lakukan terhadap korban nya adalah "***Phishing Attack (Scamming)***" adalah teknik dimana untuk mendapatkan informasi korban seolah olah berasal dari website resmi, **contoh nya** adalah ketika saya membuat salinan web facebook yang di desain sama untuk menjebak target supaya mengisikan id dan password nya, kemudian data pribadi tersebut akan tersimpan langsung ke database saya. Biasanya jebakan seperti ini lebih cepet terjerat ke target yang sudah mengenal kita dengan baik.

2.

Pengendalian (control) adalah mekanisme yang diterapkan baik untuk melindungi perusahaan dari resiko atau untuk meminimalkan dampak resiko tersebut pada perusahaan jika resiko tersebut terjadi. Contoh **PENGENDALIAN TEKNIS** yang diambil

---

Pengendalian teknis (*technical control*) adalah pengendalian yang menjadi satu di dalam system dan dibuat oleh para penyusun system selama masa siklus penyusunan system. Didalam pengendalian teknis, jika melibatkan seorang auditor internal didalam tim proyek merupakan satu cara yang amat baik untuk menjaga agar pengendalian semacam ini menjadi bagian dari desain system. Kebanyakan pengendalian keamanan dibuat berdasarkan teknologi peranti keras dan lunak.

Contoh Dasar untuk keamanan melawan ancaman yang dilakukan oleh orang-orang yang tidak diotorisasi adalah pengendalian akses. **Alasannya sederhana:** Jika orang yang tidak diotorisasi tidak diizinkan mendapatkan akses terhadap sumber daya informasi, maka pengrusakan tidak dapat dilakukan.

3.

Selain teknologi yang usang dapat menjadi ancaman pada sistem informasi yaitu penyalahgunaan teknologi untuk kejahatan kriminal yaitu :

- 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.

Nama : **Harli Septia Fani**
NIM : **182420122**
Kelas : **MTI 20A**
Mata Kuliah : **IT Risk Management and Disaster Recovery**
Dosen : **Dedy Syamsuar, PhD.**

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?

---- Selamat bekerja ----

Jawaban :

1. *Social engineering* adalah ancaman yang bersifat non teknis. Dapat digunakan oleh banyak pihak baik internal maupun eksternal. Kebanyakan orang menyebut *social engineering* sebagai suatu aktifitas meretas informasi penting melalui psikis dan pikiran manusia. Berbeda dengan meretas sistem komputer, mendapatkan informasi berharga dari seseorang membutuhkan teknik sosial dan persuasif yang tinggi, karena objek yang akan mereka retas adalah manusia bukan mesin.
Berdasarkan data dari SANS Institute, ada 4 siklus penting yang digunakan dalam *social engineering*, yaitu :
   1) *Social engineering* akan mencari informasi terkait apa yang akan ia cari dan siapa yang bisa ia jadikan target eksplotasi.
   2) Selanjutnya, ia akan membangun hubungan dengan target yang dimaksud. Membangun hubungan tersebut dapat dilakukan dengan berbagai cara seperti bekerja pada organisasi yang ia jadikan target, membangun hubungan pertemanan ataupun persaudaraan, bahkan membangun hubungan emosional.
   3) Setelah hubungan, *social engineer* akan memanfaatkan psikis mereka untuk dieksploitasi, dengan cara yang bermacam-macam. *Social engineer* bisa menggunakan faktor psikis emosional, penyuapan, ataupun ancaman untuk

mendapatkan informasi sensitif seperti *password* ataupun akun pada bank maupun sistem keamanan

4) Fase terakhir adalah eksekusi untuk melengkapi siklus *social engineering* tersebut.

Teknik *Social Engineering* :

1. *Phising Attack*
   Adalah tindakan memperoleh informasi pribadi seperti *user ID, password* dan data-data sensitif lainnya dengan menyamar sebagai orang atau organisasi yang berwenang melalui sebuah *email.*
   Contoh kasus :
   Seperti kasus yang pernah terjadi pada Paypal. Dalam email phising tersebut tertulis untuk meng-*update* data paypal dan mengganti *password* paypal karena akun yang korban miliki disinyalir telah disalahgunakan orang dan disertakan *link* menuju *website* yang mirip 100% seperti paypal yang sebenarnya *website* tersebut adalah buatan dari si *hacker* itu sendiri. Dengan cara ini *hacker* mendapatkan semua data yang diperlukan untuk mengambil alih akun seseorang.
   Teknik ni bisa dikembangkan lebih lanjut untuk mendapatkan sasaran tetarget atau dikenal dengan *spear phising attack.* Selain *email*, teknik ini juga menggunakan media sosial seperti *facebook, instagram,* dan media sosial lainnya.
   (Sumber : http://scdc.binus.ac.id/himsisfo/2017/03/social-engineering-salah-satu-teknik-pencurian-data-yang-harus-diwaspadai/*)*
2. Pretexting
   Teknik yang digunakan *hacker* dengan berbicara layaknya para ahli.
3. Baiting
   Mirip dengan *phising*, dengan memberikan pancingan berupa hadiah atau hal-hal yang menarik korban untuk membuka situs yang dibuat *hacker.*
4. *Quid Pro Quo*
   Menjanjikan bahwa korban akan mendapatkan keuntungan yang sama jika korban menberikan informasi yang mereka butuhkan.
5. Tailgating/Piggyback
   Dengan cara mengutit seseorang yang memiliki otentikasi, seperti karyawan perusahaan untuk masuk ke area yang bisa diakses orang asing.

(Sumber : https://kumparan.com/kumparantech/5-taktik-social-engineering-salah-satunya-dilakukan-si-remaja-autis)

2. Manajemen resiko adalah suatu pendekatan terstruktur/metodologi dalam mengelola ketidakpastian yang berkaitan dengan ancaman; suatu rangkaian aktifitas manusia termasuk penilaian resiko, pengembangan strategi untuk mengelolanya dan mitigasi resiko dengan menggunakan pemberdayaan/pengelolaan sumber daya.
Strategi yang diambil antara lain adalah memindahkan resiko kepada pihak lain, menghindari resiko, mengurangi efek negatif resiko, dan menampung sebagian atau semua konsekuensi resiko tertentu. Manajemen resiko tradisional terfokus pada resiko-resiko yang timbul oleh penyebab fisik atau legal (seperti bencana alam, kebakaran, kematian, serta tuntutan hukum).
Manajemen resiko dapat diterapkan ke seluruh organisasi, pada keseluruhan area kegiatan dan pada setiap tingkatan, setiap saat, baik pada suatu fungsi khusus, proyek, proses maupun suatu kegiatan.
Adapun sasaran dan tujuan pelaksanaan manajemen resiko adalah mengurangi resiko yang mungkin akan muncul (ancaman), mengukur dampak dari potensi ancaman, menentukan berapa besar kerugian yang diderita akibat hilangnya potensi bisnis.

Ancaman ini bisa disebabkan oleh berbagai elemen seperti teknologi, *human error,* lingkungan, polotik maupun organisasi. Manajemen resiko bertujuan mengelola resiko tersebut sehingga kita dapat memperoleh hasil yang optimal.

Tahapan dalam manajemen resiko :

1) Tahapan identifikasi ancaman dan resiko yang mungkin terjadi dalam suatu aktiftas usaha. Salah satu aspek penting dalam identifikasi resiko adalah membuat *list/*daftar kemungkinan resiko yang akan terjadi.
2) Analisis resiko
   Adalah melihat potensial seberapa besar *severity* (kerusakan) dan probabilitas terjadinya resiko tersebut. Kesulitan dalam pengukuran resiko adalah menentukan kemungkinan terjadi suatu resiko karena informasi statistik tidak selalu tersedia untuk beberapa resiko tertentu. Selain itu, mengevaluasi dampak *severity* (kerusakan) seringkali cukup sulit untuk asset immaterial.
3) Evaluasi resiko
   Dengan cara membandingkan tingkat resiko terhadap standar yang telah ditentukan, target tingkat resiko dan kriteria lainnya.
   Tujuan evaluasi yaitu :
   - Mengetahui tingkat prioritas tertinggi dan terendah
   - Menentukan resiko mana yang ditindaklanjuti dengan penanganan dan resiko mana saja yang hanya perlu dipantau.
4) Pengelolaan resiko
   - Menghindari resiko *(risk avoidance)*, berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan resiko tersebut.
   - Berbagi resiko *(risk sharing/risk transfer)*, yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya resiko atau dampak resiko
   - Mitigasi *(mitigation)*, yaitu melakukan perlakuan resiko untuk mengurangi kemungkinan timbulnya resiko, atau mengurangi dampak resiko bila terjadi, atau mengurangi keduanya
   - Menerima resiko *(risk acceptance)*, yaitu tidak melakukan perlakuan apapun terhadap resiko tersebut.

3. Keamanan Teknologi Informasi atau *IT Security* mengacu pada usaha-usaha mengamankan infrastruktur teknologi informas dari gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan.

Berbeda dengan Keamanan Informasi yang fokusnya justru pada data dan informasi.

Pada konsep ini, usaha-usaha yang dilakukan adalah merencanakan, mengembangkan serta mengawasi emua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berkepentingan.

Jadi, keamanan teknologi informasi merupakan bagian dari keseluruhan aspek keamanan informasi. Karena teknologi informasi merupakan salah satu alat atau *tool* penting yang digunakan untuk mengamankan akses serta penggunaan data dan informasi perusahaan.

Dalam penggunaan teknologi informasi di setiap institusi membutuhkan suatu operasional yang optimal untuk mendukung bisnis yang berjalan. Maka banyak hal yang bisa dilibatkan mulai dari *hardware, software,* prosedur dan sumber daya manusia.

Semua itu harus selalu diperbaharui seiring dengan kemajuan teknologi dan semakin beragam dan canggihnya resiko ancaman terhadap informasi. Misalnya untuk mengantisipasi kegagalan sistem komputer, organisasi meneraapkan sistem komputer yang berbasis *fault-tolerant* (toleran terhadap kegagalan). Pada sistem ini jika komponen dalam sistem mengalami kegagalan maka komponen cadangan atau kembarannya akan segera mengambil alih peran komponen yang rusak, sehingga proses bisnis bisa tetap berjalan.

Komunikasi jaringan, toleransi kegagalan terhadap jaringan dilakukan dengan menduplikasi jalur komunikasi dan prosesor komunikasi.
Prosesor, redudansi prosesor yang akan mengambil alih prosesor yang bermasalah
Penyimpanan eksternal, terhadap kegagalan pada penyimpanan eksternal antara lain dilakukan melalui *disk memoring* atau *disk shadowing*, yang menggunakan teknik dengan menulis seluruh data ke dua disk secara paralel. Jika salah satu disk mengalami kegagalan, program aplikasi tetap berjalan dengan menggunakan disk yang masih berfungsi baik.
Catu daya, toleransi kegagalan pada catu daya diatasi melalui UPS
Transaksi, toleransi kegagalan pada level transaksi ditangani melalui basis data yang disebut *rollback*, yang akan mengembalikan ke keadaaan semula yaitu keadaan seperti sebelu transaksi dimulai sekiranya di pertengahan pemrosesan transaksi terjadi kegagalan.
Jika semua hal tersebut tidak ada, atau hanya menggunakan teknologi usang, maka data dan informasi perusahaan akan mengalami kerentanan *(vulnerability)* terhadap ancaman *(threats)* yang setiap saat bisa saja melumpuhkan bisnis perusahaan.

Nama : I Made Harya Wijaya Oka Rafflesia
NIM : 182420129
Matkul : IT RISK MANAGEMENT AND DISASTER

Pertanyaan :

1. Metode apa yang digunakan oleh seorang social enggineering hacker untuk memperoleh userid dan password dari pengguna tertentu? Jelaskan dan berikan contoh!
   Jawab:
   - ***Phishing*** adalah tindakan memperoleh informasi pribadi seperti user ID, **password**, dan data-data sensitif lainnya **dengan menyamar** sebagai orang atau organisasi yang berwenang melalui sebuah jalur komunikasi digital, *Phising* bisa dikatakan mencuri informasi penting dengan mengambil alih akun korban untuk maksud tertentu. 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, 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

     Contoh : : Hacker akan menggunakan email yang berisi pesan palsu dan link berbahaya untuk memancing korban agar memberikan informasi penting. Agar korban percaya, 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.

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:
   Berikut beberapa strategi untuk melakukan manajemen risiko secara efektif dan efisien untuk perusahaan yang sedang berkembang saat ini :
   - **Melakukan perencanaan manajemen risiko**, Langkah awal yang dilakukan adalah melakukan perencanaan manajemen risiko. Dengan melakukan perencanaan kita dapat memutuskan bagaimana manajemen risiko yang baik dan sesuai untuk proyek yang akan dilakukan. Perencanaan manajemen risiko

mempertimbangkan lingkup proyek, rencana manajemen proyek, faktor lingkungan perusahaan, maka tim proyek dapat mendiskusikan dan menganalisis aktivitas manajemen risiko untuk proyek-proyek tertentu. Untuk membuat perencanaan risiko ada hal –hal yang pendukung perencanaan seperti project charter, kebijakan manajemen risiko, susunan peran dan tanggung jawab, toleransi stackholder terhadap risiko, template untuk rencana manajemen risiko.

- **Melakukan pengidentifikasian risiko**, Setelah kita merancang bagaimana manajemen risiko yang akan diterapkan di perusahaan, langkah selanjutnya adalah melakukan pengidentifikasian risiko dengan memahami terlebih dahulu risiko yang akan terjadi pada proyek yang dijalankan. Identifikasi risiko dapat dilakukan dengan analisis sumber risiko dan analisis masalah Analisis sumber risiko yaitu analisis risiko dengan melihat darimana risiko berasal. Ada tiga sumber risiko yang sudah banyak dikenal yakni Risiko internal yakni risiko yang bersumber dari internal organisasi yang dapat dikategorikan dalam non technical risk (manusia, material, keuangan) dan technical risk (disain, konstruksi dan operasi).
- **Mengevaluasi risiko**, Setelah risiko potensial teridentifikasi, tim proyek kemudian mengevaluasi setiap risiko berdasarkan probabilitas kejadian risiko akan terjadi dan potensi kerugian yang terkait dengannya. Tidak semua risikonya sama. Beberapa kejadian berisiko lebih mungkin terjadi daripada yang lain, dan biaya risiko bisa sangat bervariasi. Mengevaluasi kemungkinan terjadinya risiko dan tingkat keparahan atau potensi kerugian proyek adalah langkah selanjutnya dalam proses manajemen risiko.
- **Melakukan rencana mitigasi**, Setelah risiko diidentifikasi dan dievaluasi, tim proyek mengembangkan rencana mitigasi risiko, yang merupakan rencana untuk mengurangi dampak kejadian tak terduga. Tim proyek mengurangi risiko dengan berbagai cara yaitu risk avoidance, risk sharing, risk reduction dan risk transfer. Masing-masing teknik mitigasi ini bisa menjadi alat yang efektif dalam mengurangi risiko individu dan profil risiko proyek. Rencana mitigasi risiko akan melakukan pendekatan mitigasi untuk setiap kejadian risiko yang teridentifikasi dan tindakan yang akan diambil oleh tim manajemen proyek untuk mengurangi atau menghilangkan risiko tersebut.
- **Memindahkan Risiko**, Jika risiko tidak bisa ditangani oleh perusahaan secara internal, maka risiko tersebut bisa dipindahkan kepada pihak-pihak yang bisa membantu untuk menangani risiko tersbut. Maksud pihak yang bisa membantu menangani risiko yang ada adalah perusahaan asuransi. Jika risiko yang terjadi adalah hal-hal yang berhubungan dengan kejadian tak terduga seperti kebakaran, pencurian atau kerusakan, maka jasa perusahaan asuransi akan meringankan beban perusahaan dalam menangani risikonya.

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

   Dalam rencana sistem keamanan untuk menganalisis risiko-risiko yang mungkin ada, diingat ancaman keamanan sistem tak hanya bisa ditemukan dari luar sistem. Kemungkinan ancaman dari dalam sistem pun banyak ditemukan. Untuk minimalisir hal tersebut perlu dibuat pemetaan atau rencana penanggulangan risiko TI, baik dari dalam maupun dari luar, Teknologi yang telah using juga ikut berkontribusi ancaman bagi keamanan teknologi yang mendorong tingkat dan sifat kerugian. Misalnya, potensi hilangnya produktivitas akibat aset yang dihancurkan atau dicuri tergantung pada seberapa penting aset itu bagi produktivitas organisasi. Jika aset penting diakses secara tidak sah, tidak ada kerugian produktivitas langsung. Demikian pula, penghancuran aset yang sangat sensitif yang tidak memainkan peran penting dalam produktivitas tidak akan secara langsung mengakibatkan hilangnya produktivitas yang signifikan. Namun, aset yang sama itu, jika diungkapkan, dapat mengakibatkan hilangnya keunggulan kompetitif atau reputasi secara signifikan, dan menghasilkan biaya hukum. Intinya adalah kombinasi aset dan jenis tindakan terhadap aset yang menentukan sifat dasar dan tingkat kerugian.

Terima kasih.

NAMA	: IBNU FAJARIADI
NIM	: 182420109
MATKUL	: IT RISK MANAGEMENT AND DISASTER RECOVERY
KELAS	: MTI2A1

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

   Brute Force
   Brute Force berfokus pada kombinasi karakter yang digunakan dalam password. Keyword yang dipakai biasanya sesuai dengan algoritma yang dimiliki password manager, misalnya kombinasi antara beberapa huruf besar, huruf kecil, angka-angka, dan beberapa karakter simbol.
   Serangan brute force ini akan mencoba beberapa kombinasi dari karakter alfanumerik yang paling banyak dipakai, misalnya seperti 1q2w3e4r5t, zxcvbnm, dan qwertyuiop. Nah, apakah kalian termasuk yang menggunakan password seperti itu?
   Kelebihan cara ini adalah dapat menambah variasi serangan daripada hanya menggunakan kamus password saja. Jika akun kalian ingin aman dari serangan brute force, maka gunakan kombinasi karakter yang lebih bervariasi. Bila memungkinkan gunakan juga simbol-simbol ekstra untuk meningkatkan kompleksitas kata sandi.

   Phising
   Phising adalah salah satu cara yang paling populer untuk mendapatkan akun milik korban sampai saat ini. Jadi, phising adalah usaha untuk mengelabui target supaya mereka tidak menyadari jika mereka sedang ditipu.
   Saat ini email phising menjadi salah satu cara populer untuk mendapatkan akun milik korban, dan juga setiap harinya terdapat miliaran email palsu yang dikirim ke semua pengguna internet di seluruh dunia. Modusnya adalah korban akan menerima email palsu yang mengaku bahwa mereka berasal dari organisasi atau bisnis yang terpercaya. Biasanya isi email ini mengharuskan korban untuk melakukan sesuatu seperti menyerahkan informasi pribadi dan lain-lain.
   Selain itu, email palsu juga terkadang berisi informasi yang mengarahkan target untuk mengklik tautan situs tertentu, yang bisa berupa malware atau situs web palsu yang dibuat mirip dengan web aslinya. Sehingga dalam kasus ini korban tidak menyadari jika mereka sedang diarahkan untuk menyerahkan informasi pribadi yang penting.

   Social Engineering
   Social engireening mirip dengan teknik phising, namun teknik ini lebih dipakai dalam kehidupan nyata. Misalnya kasus mama minta pulsa juga menggunakan teknik ini, si korban yang tidak menyadari bisa dengan mudah langsung percaya dengan isi pesan tersebut dan langsung mengikuti arahan yang diberikan si penipu.
   Teknik social engireening ini sudah ada sejak dulu dan hal ini malah disalahkangunakan sebagai metode untuk menipu korban secara tidak langsung, seperti meminta password atau meminta sejumlah uang.

   Rainbow Table
   Rainbow table adalah bentuk serangan dengan memanfaatkan database akun dan password yang sudah didapat. Dalam kasus ini penyerang sudah mengantongi daftar username target dan kata sandi, tetapi dalam bentuk enkripsi. Kata sandi yang terenkripsi

ini memiliki tampilan yang sangat berbeda dengan aslinya, misalnya kata sandi yang didapat adalah 'BinaDarmaOke , maka bentuk enkripsi hash MD5 nya berbentuk 8f4047e3233b39e4444e1aef240e80aa , rumit bukan?
Namun dalam kasus tertentu, penyerang hanya menjalankan daftar password plaintext lewat algoritma *hashing*, lalu kemudian membandingkan hasilnya dengan data password yang masih berbentuk enkripsi. Ya, bisa dibilang algoritma enkripsi tidak seratus persen aman serta sebagian besar password yang terenkripsi pun ternyata masih mudah dibobol.
Inilah mengapa metode rainbow table paling relevan saat ini, alih-alih penyerang harus memproses jutaan password dan mencocokkan nilai hash yang dihasilkannya, rainbow table sendiri sudah merupakan daftar nilai hash dari algoritma yang telah dihitung sebelumnya.
Metode ini dapat mengurangi waktu yang dibutuhkan untuk memecahkan kata sandi target. Nah, hacker sendiri dapat membeli rainbow table yang telah terisi penuh oleh jutaan kombinasi password yang potensial dan banyak dipakai. Jadi, hindari situs yang masih menggunakan metode enkripsi SHA1 atau MD5 sebagai algoritma hashing password karena metode ini telah ditemukan celah keamanannya.

Malware/Keylogger
Cara lain yang bisa membahayakan akun dan informasi penting di internet adalah karena adanya malware atau program jahat. Malware ini telah tersebar di seluruh jaringan internet dan berpotensi untuk terus berkembang. Bahayanya lagi jika kita sampai terkena malware dalam bentuk keylogger, maka secara tak sadar setiap aktivitas kita di komputer bisa diketahui oleh penyerang.
Program malware ini sendiri secara khusus dapat menargetkan data pribadi, lalu penyerang bisa dengan mudah mengendalikan komputer korban dari jarak jauh untuk mencuri setiap informasi yang berharga.
Bagi kalian yang tidak ingin terkena malware, maka jangan pernah menggunakan aplikasi bajakan. Lalu jangan malas untuk memperbarui software antivirus dan antimalware yang ada. Selain itu selalu berhati-hati saat *browsing* internet dan jangan asal downlad file dari sumber yang tidak jelas.

2. Mengingat seriusnya resiko keamanan akan aset teknologi 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 merek;;a dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan. Sehubungan dengf,an hal ini bagaimana strategi yang dapat diterapkan untuk memanajemen resiko ini? (Jelaskan dengan contoh)

   Dalam Resiko Managemen IT dikenal dengan Strategi Kontrol. Strategi ini berguna untuk merespon setiap resiko terhadap penggunaan IT. Ada 4 strategi yang dikenal untuk mengatasi resiko IT. Seperti Avoidance, Mitigation, Transference dan Acceptance.

   Dari wacana diatas dapat kita ambil solusi Strategi kontrol yaitu Avoidance.
   Avoidance adalah Mengambil tindakan untuk menghentikan kegiatan yang dapat menyebabkan risiko terjadi. Strategi kontrol yang dilakukan dengan tujuan untuk

mencegah terjadinya serangan kepada aset organisasi baik dilakukan dengan penerapan kebijakan, pelatihan yang memadai ataupun menggunakan teknologi yang mumpuni.
Contohnya adalah Sebuah perusahaan menerepkan sistem keamanan IT dengan Melaksanakan program pelatihan kesadaran keamanan perusahaan yang mencakup informasi tentang proses manajemen keamanan perusahaan. Pelatihan ini disediakan untuk semua karyawan (tidak hanya karyawan baru) dalam kurun waktu tertentu. Pelatihan ini disediakan untuk semua karyawan (tidak hanya karyawan baru) dalam kurun waktu tertentu dan mendokumentasikan tugas dan tanggung jawab keamanan informasi untuk semua karyawan dalam perusahaan.

3. Jelaskan mengapa dan bagaimana teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi?
   Karena teknologi yang usang sorcecode keamanannya sudah dipahami para hacker dan teknologi yang usang tanpa update keamanan maka akan sangat mudah diretas oleh para hacker.
   Teknologi yang sudah usang sistem keamanannya tidak didukung lagi oleh developer. Tak hanya perusahaan developer menghentikan dukungan keamanan tetapi juga para pembuat antivirus pun sudah tidak akan lagi memproduksi produk keamanan pada teknologi yang sudah usang. Sehingga para komunitas hacker telah mengetahui berbagai celah keamanan yang ada pada teknologi yang sudah usang. Itulah mengapa teknologi yang usang berkontribusi menjadi ancaman bagi keamanan teknologi.