MID

Petunjuk:

1. Silakan jawab pertanyaan berikut
2. Jawaban akan dinilai berdasarkan pemahaman yang anda miliki terhadap masing2 soalnya
3. Jawaban yang terindikasi hasil kolaborasi, maka hanya si 'penjawab' pertama yang dinilai, selebihnya tidak akan dinilai ...alias urung dapet A

Soal:

1. Jelaskan apa yang dimaksud dengan IT Risk Manajemen? Dan mengapa hal ini penting?
2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya
3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

----- oOOo -----

MID

Nama: Mustakim

Nim: 202420028

Petunjuk:

1. Silakan jawab pertanyaan berikut
2. Jawaban akan dinilai berdasarkan pemahaman yang anda miliki terhadap masing2 soalnya
3. Jawaban yang terindikasi hasil kolaborasi, maka hanya si 'penjawab' pertama yang dinilai, selebihnya tidak akan dinilai ...alias urung dapet A

Soal & Jawaban :

1. Jelaskan apa yang dimaksud dengan IT Risk Manajemen? Dan mengapa ini penting?

Jawaban: IT Risk Management adalah suatu proses dalam penerapan prinsip manajemen risiko untuk melindungi suatu organisasi/perusahaan yang memanfaatkan teknologi informasi dalam mencegah kerentanan dan ancaman informasi yang dapat mempengaruhi tujuan/bisnis dari organisasi/perusahaan tersebut. Risiko-risiko yang dari teknologi informasi yang digunakan pada sebuah perusahaan/organisasi yaitu kerusakan perangkat lunak dan keras, virus computer, malware, spam, scam, phishing dan human error. Selain risiko itu IT Risk Management juga dapat mengelola hambatan criminal yang berkaitan dengan teknologi informasi pada organisasi/perusahaan yaitu antara lain seperti hacker yang dapat menerobos system computer dengan cara yg salah, kemudian ada fraud yaitu orang memanipulasi data untuk kepentingan melanggar hukum. Jadi dapat disimpulkan bahwa sebegus dan sebaik apapun sebuah system pada perusahaan/organisasi dalam pemanfaatan teknologi informasi tetap harus menerapkan IT risk management dalam upaya mencegah dan membuat nyaman dalam penggunaan teknologi dalam mencapai tujuan perusahaan/organisasi.

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya

Jawaban:

1. Hacker: orang yang dapat menerobos system computer dengan cara yg salah/ tidak sah,
2. Fraud: yaitu orang memanipulasi data untuk kepentingan melanggar hukum dan merugikan Organisasi/perusahaan.
3. Malware/Virus computer: sebuah program computer yg masuk kedalam system untuk mempengaruhi kinerja/merusak sebuah system/computer.
4. Spam, scams, and phishing: Penipuan melalui media teknologi informasi yaitu contohnya email yang dapat mencuri informasi seperti nomor rekening bank, kata sandi, dan nomor kartu kredit baik pribadi, organisasi maupun perusahaan.
5. Human Error: yaitu sebuah kesalahan atau yang dapat terjadi yang diakibatkan minimnya pengetahuan tentang IT pada sebuah organisasi/perusahaan.

Contoh: <https://www.cnbcindonesia.com/tech/20210609131452-37-251746/ngeri-miliaran-password-bocor-di-forum-hacker>

Kumpulan miliaran kata sandi diduga bocor di forum peretas populer. Hal ini diketahui dari pengguna forum yang menggugah file TXT 100GB berisi 8,4 miliar entri password.

Jumlah itu nampaknya telah digabungkan dari kebocoran data dan pelanggaran yang telah terjadi di masa lalu. Menurut orang yang mengunggah, seluruh password memiliki panjang 6-20 karakter, dengan karakter non-ASCII dan tanpa spasi.

Menurut saya dalam contoh kasus diatas tetap akan terjadi karna semakin canggihnya sebuah system pasti tetap akan ada celah. Maka dari itu pentingnya update password berjangka seperti password email yg dapat diganti agar tidak mudah dikases dan menghindari hal-hal diatas.

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

Jawaban: yang akan saya lakukan adalah menerapkan IT Risk Management pada perusahaan dan mencari pihak yang dapat menjamin keamanan IT perusahaan berjalan dengan baik. Dengan kemudian akan mengamankan jaringan untuh mencegah cyber crime, lalu memperhatikan phishing yang dapat mencuri informasi yg digunakan hacker dalam menjalankan aksi kriminalnya, dan membackup data atau file penting/ yg berkaitan dengan perusahaan secara berkala.

----- oOOo -----

MID

Petunjuk:

1. Silakan jawab pertanyaan berikut
2. Jawaban akan dinilai berdasarkan pemahaman yang anda miliki terhadap masing2 soalnya
3. Jawaban yang terindikasi hasil kolaborasi, maka hanya si 'penjawab' pertama yang dinilai, selebihnya tidak akan dinilai ...alias urung dapet A

Soal:

1. Jelaskan apa yang dimaksud dengan IT Risk Manajemen? Dan mengapa hal ini penting?
2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya
3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

Jawaban:

1. IT Risk Manajemen adalah keamanan informasi yang didefinisikan sebagai seperangkat mekanisme, teknik, tindakan, dan proses administratif yang digunakan untuk melindungi aset TI dari pihak yang tidak berwenang akses, manipulasi, modifikasi, kehilangan, dan dari pengungkapan data dan informasi yang tidak disengaja yang tertanam dalam aset ini.

IT Risk Manajemen penting dikarenakan pada setiap organisasi memiliki misi. Di era digital ini, karena organisasi menggunakan otomatis teknologi informasi (TI) sistem untuk memproses informasi mereka untuk dukungan yang lebih baik dari misi mereka, manajemen risiko memainkan peran penting dalam melindungi aset informasi, dan karena itu misinya, dari risiko terkait TI.

2. Dalam IT Risk Management pastinya ada ancaman terhadap sistem yang mungkin terjadi. Sumber ancaman meliputi bencana alam, kegagalan sistem, kerusakan hardware dan software, malware, virus komputer, dan human error.

Contoh gangguan pada teknologi sistem informasi yaitu:

- a) Kesalahan teknis (*technical errors*)

Kesalahan perangkat keras (*hardware problems*)

Kesalahan di dalam penulisan sintak perangkat lunak (*syntax errors*)

Kesalahan logika (*logical errors*)

- b) Gangguan lingkungan (*environmental hazards*)

Kegagalan arus listrik karena petir

- c) Kesalahan manusia (*human errors*)

3. Mengamankan asset IT yang saya kelola jika saya menjadi CIO (Chief Information Officer) dengan cara selalu mengidentifikasi area potensial yang rentan terhadap pelanggaran keamanan siber dan harus mempraktikkan metode pencegahan untuk memastikan bahwa intranet perusahaan tetap aman.

Nama : Nurul Amalina Setyorini
NIM : 202420005
Jurusan : MTI Regular B

MID

Petunjuk:

1. Silakan jawab pertanyaan berikut
2. Jawaban akan dinilai berdasarkan pemahaman yang anda miliki terhadap masing2 soalnya
3. Jawaban yang terindikasi hasil kolaborasi, maka hanya si 'penjawab' pertama yang dinilai, selebihnya tidak akan dinilai ...alias urung dapet A

Soal:

1. Jelaskan apa yang dimaksud dengan IT Risk Manajemen? Dan mengapa hal ini penting?
2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya
3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

----- oOOo -----

1. IT Risk Manajemen merupakan usaha untuk mengelola resiko bisnis menggunakan kerangka IT sehingga kerentanan dan ancaman dapat diidentifikasi. Hal ini penting untuk menciptakan lingkungan kerja yang aman dan terjamin untuk semua staff dan pelanggan, meningkatkan stabilitas operasional serta melindungi perusahaan dari resiko yang merugikan.
2. Sumber ancaman yang mungkin terjadi terhadap sistem :
 1. Human error : terjadinya kelalaian.
Contoh : kesalahan penginputan dan penghapusan data, serta kesalahan pengoperasian sistem.
 2. Bencana alam : merupakan faktor yang tak terduga yang bisa mengancam sistem informasi.
Contoh : gangguan listrik, kegagalan peralatan dan fungsi perangkat lunak dapat menyebabkan data tidak konsisten , transaksi tidak lengkap atau bahkan data rusak. Selain itu variasi tegangan listrik yang terlalu tajam dapat membuat peralatan-peralatan terbakar.
 3. Hacker : orang-orang yang dapat dikategorikan sebagai programmer yang pandai dan senang mengutak-utik sesuatu yang dirasakan sebagai penghalang terhadap apa yang ingin dicapainya. Hacker akan mencari cara bagaimana bisa menembus password, firewall, access-key dan sebagainya.
Contoh teknik yang digunakan untuk melakukan hacking :
 - Back Door : suatu serangan (biasanya bersumber dari suatu software yang baru di install) yang dengan sengaja membuka suatu "pintu belakang" bagi pengunjung tertentu, tanpa

disadari oleh orang yang menginstall software, sehingga mereka dengan mudah masuk ke dalam sistem jaringan.

- Sniffer : Teknik ini diimplementasikan dengan membuat program yang dapat melacak paket data seseorang. Ketika paket tersebut melintas internet, menangkap password atau isinya.
 - Spoofing : suatu usaha dari orang yang tidak berhak misalnya dengan memalsukan identitas, untuk masuk ke suatu sistem jaringan, seakan-akan dia adalah user yang berhak.
 - DNS Poisoning : hacker merubah atau merusak isi DNS sehingga semua akses yang memakai DNS ini akan disalurkan ke alamat yang salah atau alamat yang dituju tidak bisa diakses.
4. Virus : program computer yang masuk ke dalam sistem untuk melakukan sesuatu, misalnya meng-interrupt proses yang sedang berjalan di CPU, memperlambat kinerja computer, memenuhi memory computer sehingga kegiatan CPU berhenti, memenuhi hard disk, menghapus file-file, merusak sistem operasi dan sebagainya.
3. Jika saya seorang CIO, ada tiga cara mengamankan asset IT yaitu :
1. Mengamankan jaringan : selalu beri password dalam seluruh jaringan data computer serta hidden seluruh sistem adalah cara untuk mencegah cyber crime serta mempersulit hacker memperoleh akses menuju jaringan.
 2. Memperhatikan phishing : selalu berhati-hati dalam memberikan informasi.
 3. Membackup data : melakukan backup berkala untuk jaga-jaga seandainya suatu waktu terjadi kehilangan data. Sehingga data masih tersimpan aman.

MID IT RISK MANAGEMENT

NAMA : OKTARIANSYAH

NIM : 202420006

KELAS : MTI2B

1. Untuk mencapai tujuan bisnis, seringkali perusahaan-perusahaan menggunakan teknologi informasi atau *information technology* (IT) sebagai basis dalam menciptakan layanan yang berkualitas ataupun dalam mengoptimalkan proses bisnisnya. Namun pada penerapannya, teknologi informasi memerlukan perencanaan yang strategis agar penerapannya dapat selaras dengan tujuan bisnisnya. Jika penerapan teknologi informasi tidak sesuai dengan arah bisnis perusahaan, maka hal inilah yang akan menimbulkan risiko. Risiko yang timbul akibat penerapan teknologi informasi yang salah dapat menyebabkan proses bisnis yang berjalan tidak optimal, timbul pula kerugian financial, dan berbagai hal yang dapat merugikan perusahaan.

Oleh karena itu diperlukan suatu pengukuran terhadap risiko penerapan teknologi informasi bagi perusahaan. Penerapan ini berguna untuk mengetahui profil risiko teknologi informasi, analisa terhadap risiko, kemudian mengambil tindakan terhadap risiko tersebut sehingga tidak terjadi dampak-dampak yang nantinya akan timbul oleh risiko tersebut. Manajemen risiko teknologi informasi, merupakan suatu proses identifikasi kerentanan dan ancaman terhadap sumber daya informasi yang digunakan oleh sebuah perusahaan atau organisasi, yang dilakukan oleh manajer IT untuk mencapai tujuan bisnis, mengurangi risiko, dan menyeimbangkan pengeluaran dalam mencapai keuntungan dan melindungi teknologi informasi perusahaan tersebut. Namun dalam pelaksanaannya, terdapat beberapa macam hambatan umum terhadap data dan sistem teknologi informasi yang meliputi :

- Kerusakan perangkat keras dan perangkat lunak
- *Malware (Malicious Software)*
- Virus komputer
- *Spam, scams, and phishing*
- Kesalahan manusia (*human error*)

Selain hambatan umum tersebut, dalam IT RISK MANAGEMENT juga mengelola hambatan kriminal terhadap teknologi informasi suatu perusahaan, antara lain yaitu :

- *Hackers*, yaitu orang-orang yang secara tidak sah menerobos masuk ke dalam sistem komputer.
- *Fraud*, yaitu penggunaan komputer untuk memanipulasi data untuk kepentingan yang melanggar hukum.
- *Denial of service*, yaitu serangan *online* yang membuat pengguna tidak dapat mengakses situs tertentu.

- *Staff dishonesty*, yaitu pencurian data atau informasi penting oleh karyawan internal perusahaan.

Jika manajemen risiko diatur dengan baik, proses akan terus menerus mengidentifikasi masalah dan resolusi, maka sistem akan mudah melengkapinya sistem lain. Ini termasuk organisasi, perencanaan dan penganggaran, dan kontrol biaya. Hal-hal yang tidak terduga akan berkurang karena penekanan akan menjadi manajemen yang proaktif dan bukan reaktif.

Adapun proses dari manajemen risiko IT yaitu :

1. Mengidentifikasi Risiko

Perusahaan mengungkap, mengenali dan menggambarkan risiko yang mungkin mempengaruhi proyek.

2. Menganalisis Risiko

Ketika risiko sudah diidentifikasi, perusahaan menentukan kemungkinan dan konsekuensi dari setiap risiko yang ada. Perusahaan lalu mengembangkan sebuah pemahaman tentang sifat risiko dan potensi untuk mempengaruhi tujuan dan sasaran proyek .

3. Mengevaluasi Risiko

Perusahaan mengevaluasi risiko dengan menentukan besarnya risiko, yang merupakan kombinasi dari kemungkinan dan konsekuensi. Lalu perusahaan membuat keputusan apakah risiko itu dapat diterima atau tidak.

4. Memantau dan Mempertimbangkan Risiko

Ini adalah proses dimana perusahaan memantau setiap risiko yang ada untuk menghindari risiko yang lebih besar.

Alasan utama mengapa pentingnya suatu perusahaan perlu untuk menerapkan proses manajemen risiko adalah untuk mendukung misi perusahaan dan melindungi aset dari perusahaan tersebut. Pada IT RISK MANAGEMENT, erat kaitannya dengan bagaimana implementasi *security* pada suatu perusahaan sehingga diperlukan pemahaman tentang proses bisnis organisasi dan kemungkinan risiko yang berdampak pada proses bisnis tersebut. *Risk management* akan sangat membantu manajemen perusahaan untuk menyeimbangkan antara dampak dari *risk* dan *cost* yang dibutuhkan untuk meminimalisir risiko tersebut.

2. Ancaman Keamanan Informasi (Information Security Threat) merupakan orang, organisasi, mekanisme, atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan. Pada kenyataannya, ancaman dapat bersifat internal serta eksternal dan bersifat disengaja dan tidak disengaja.

Ancaman Internal dan Eksternal

Ancaman internal bukan hanya mencakup karyawan perusahaan, tetapi juga pekerja temporer, konsultan, kontraktor, bahkan mitra bisnis perusahaan tersebut. Ancaman internal diperkirakan menghasilkan kerusakan yang secara potensi lebih serius jika dibandingkan dengan ancaman eksternal, dikarenakan pengetahuan ancaman internal yang lebih mendalam akan sistem tersebut. Ancaman eksternal misalnya perusahaan lain yang memiliki produk yang sama dengan produk perusahaan atau disebut juga pesaing usaha.

Tindakan Kecelakaan dan disengaja

Tidak semua ancaman merupakan tindakan disengaja yang dilakukan dengan tujuan mencelakai. Beberapa merupakan kecelakaan yang disebabkan oleh orang-orang di dalam ataupun diluar perusahaan. sama halnya

Jenis- Jenis Ancaman:

Malicious software, atau malware terdiri atas program-program lengkap atau segmen-segmen kode yang dapat menyerang suatu system dan melakukan fungsi-fungsi yang tidak diharapkan oleh pemilik system. Fungsi-fungsi tersebut dapat menghapus file, atau menyebabkan sistem tersebut berhenti. Terdapat beberapa jenis peranti lunak yang berbahaya, yakni:

1. Virus. Adalah program komputer yang dapat mereplikasi dirinya sendiri tanpa dapat diamati oleh si pengguna dan menempelkan salinan dirinya pada program-program dan boot sector lain
2. Worm. Program yang tidak dapat mereplikasikan dirinya sendiri di dalam sistem, tetapi dapat menyebarkan salinannya melalui e-mail
3. Trojan Horse. Program yang tidak dapat mereplikasi atau mendistribusikan dirinya sendiri, namun disebarkan sebagai perangkat
4. Adware. Program yang memunculkan pesan-pesan iklan yang mengganggu
5. Spyware. Program yang mengumpulkan data dari mesin pengguna

RISIKO

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 Informasi yang tidak terotorisasi 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.

PERSOALAN E-COMMERCE

E-Commerce memperkenalkan suatu permasalahan keamanan baru. Masalah ini bukanlah perlindungan data, informasi, dan piranti lunak, tetapi perlindungan dari pemalsuan kartu kredit.

Kartu Kredit "Sekali pakai" Kartu sekali pakai ini bekerja dengan cara berikut: saat pemegang kartu ingin membeli sesuatu secara online, ia akan memperoleh angka yang acak dari situs web perusahaan kartu kredit tersebut. Angka inilah, dan bukannya nomor kartu kredit pelanggan tersebut, yang diberikan kepada pedagang e-commerce, yang kemudian melaporkannya ke perusahaan kartu kredit untuk pembayaran.

Praktik keamanan yang diwajibkan oleh Visa

Visa mengumumkan 10 praktik terkait keamanan yang diharapkan perusahaan ini untuk diikuti oleh peritelnya. Peritel yang memilih untuk tidak mengikuti praktik ini akan menghadapi denda, kehilangan keanggotaan dalam program visa, atau pembatasan penjualan dengan visa. Peritel harus :

1. Memasang dan memelihara firewall
2. Memperbaharui keamanan
3. Melakukan enkripsi data yang disimpan
4. Melakukan enkripsi pada data yang dikirim
5. Menggunakan dan memperbaharui peranti lunak anti virus
6. Membatasi akses data kepada orang-orang yang ingin tahu
7. Memberikan id unik kepada setiap orang yang memiliki kemudahan mengakses data
8. Memantau akses data dengan id unik
9. Tidak menggunakan kata sandi default yang disediakan oleh vendor
10. Secara teratur menguji sistem keamanan

Selain itu, visa mengidentifikasi 3 praktik umum yang harus diikuti oleh peritel dalam mendapatkan keamanan informasi untuk semua aktivitas bukan hanya yang berhubungan dengan e-commerce:

1. Menyaring karyawan yang memiliki akses terhadap data
2. Tidak meninggalkan data atau komputer dalam keadaan tidak aman
3. Menghancurkan data jika tidak dibutuhkan lagi.

3. MANAJEMEN RISIKO (MANAGEMENT RISK)

Manajemen Risiko merupakan satu dari dua strategi untuk mencapai keamanan informasi. Risiko dapat dikelola dengan cara mengendalikan atau menghilangkan risiko atau mengurangi dampaknya. Pendefinisian risiko terdiri atas empat langkah :

1. Identifikasi aset-aset bisnis yang harus dilindungi dari risiko
2. Menyadari risikonya
3. Menentukan tingkatan dampak pada perusahaan jika risiko benar-benar terjadi
4. Menganalisis kelemahan perusahaan tersebut

Tingkat keparahan dampak dapat diklasifikasikan menjadi:

1. dampak yang parah (severe impact) yang membuat perusahaan bangkrut atau sangat membatasi kemampuan perusahaan tersebut untuk berfungsi
2. dampak signifikan (significant impact) yang menyebabkan kerusakan dan biaya yang signifikan, tetapi perusahaan tersebut tetap selamat
3. dampak minor (minor impact) yang menyebabkan kerusakan yang mirip dengan yang terjadi dalam operasional sehari-hari.

Setelah analisis risiko diselesaikan, hasil temuan sebaiknya didokumentasikan dalam laporan analisis risiko. Isi dari laporan ini sebaiknya mencakup informasi berikut ini, mengenai tiap-tiap risiko:

1. diskripsi risiko
2. sumber risiko
3. tingginya tingkat risiko
4. pengendalian yang diterapkan pada risiko tersebut
5. para pemilik risiko tersebut
6. tindakan yang direkomendasikan untuk mengatasi risiko
7. jangka waktu yang direkomendasikan untuk mengatasi risiko

Jika perusahaan telah mengatasi risiko tersebut, laporan harus diselesaikan dengan cara menambahkan bagian akhir :

KEBIJAKAN KEAMANAN INFORMASI

Suatu kebijakan keamanan harus diterapkan untuk mengarahkan keseluruhan program. CIO Perusahaan dapat menerapkan keamanan dengan pendekatan yang bertahap, diantaranya:

1. Fase 1, Inisiasi Proyek. Membentuk sebuah tim untuk mengawas proyek kebijakan keamanan tersebut.
2. Fase 2, Penyusunan Kebijakan. Berkonsultasi dengan semua pihak yang berminat dan terpengaruh.
3. Fase 3, Konsultasi dan persetujuan. Berkonsultasi dengan manajemen untuk mendapatkan pandangan mengenai berbagai persyaratan kebijakan.
4. Fase 4, Kesadaran dan edukasi. Melaksanakan program pelatihan kesadaran dan edukasi dalam unit-unit organisasi.
5. Fase 5, Penyebarluasan Kebijakan. Kebijakan ini disebarluaskan ke seluruh unit organisasi dimana kebijakan tersebut dapat diterapkan.

Kebijakan Keamanan yang Terpisah dikembangkan untuk

1. Keamanan Sistem Informasi
2. Pengendalian Akses Sistem
3. Keamanan Personel
4. Keamanan Lingkungan Fisik
5. Keamanan Komunikasi data
6. Klasifikasi Informasi
7. Perencanaan Kelangsungan Usaha
8. Akuntabilitas Manajemen

Kebijakan terpisah ini diberitahukan kepada karyawan, biasanya dalam bentuk tulisan, dan melalui program pelatihan dan edukasi. Setelah kebijakan ini ditetapkan, pengendalian dapat diimplementasikan, *Management Keamanan Informasi Perusahaan* untuk menjadi lebih baik.

NAMA : RACHMAD IQBAL

NIM : 202420002

MID

Petunjuk:

1. Silakan jawab pertanyaan berikut
2. Jawaban akan dinilai berdasarkan pemahaman yang anda miliki terhadap masing2 soalnya
3. Jawaban yang terindikasi hasil kolaborasi, maka hanya si 'penjawab' pertama yang dinilai, selebihnya tidak akan dinilai alias urung dapet A

Soal:

1. Jelaskan apa yang dimaksud dengan IT Risk Manajemen? Dan mengapa hal ini penting?
2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya
3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

Jawaban:

1. Manajemen risiko adalah segala proses kegiatan yang dilakukan semata untuk meminimalkan bahkan mencegah terjadinya risiko perusahaan. Di dalamnya ada kegiatan identifikasi, perencanaan, strategi, tindakan, pengawasan dan evaluasi terhadap hal-hal negatif yang kemungkinan akan menimpa usaha.

Penerapan manajemen risiko dan prediksi risiko dapat membantu perusahaan menghemat pengeluaran sekaligus melindungi masa depan. Sebab rencana manajemen risiko yang tepat akan membantu perusahaan menetapkan prosedur untuk menghindari ancaman, meminimalkan dampak negatif, serta mengatasi ancaman tersebut.

Kemampuan memahami dan mengendalikan risiko membuat perusahaan lebih percaya diri dalam menentukan keputusan bisnis. Selain itu, prinsip tata kelola perusahaan yang kuat dan berfokus pada manajemen risiko dapat membantu mencapai tujuan perusahaan.

Manajemen risiko juga memiliki manfaat lain sebagai berikut:

- Menciptakan lingkungan kerja yang aman dan terjamin untuk semua staf dan pelanggan.
- Meningkatkan stabilitas operasional bisnis sekaligus mengatur tanggung jawab hukum.

- Melindungi perusahaan maupun lingkungan sekitarnya dari risiko kejadian yang merugikan.
- Memberikan proteksi untuk semua orang dan aset yang terlibat dalam risiko berbahaya.
- Membantu menetapkan kebutuhan asuransi perusahaan sehingga bisa meminimalkan premi yang tidak penting.

Implementasi manajemen risiko harus bisa menjawab beberapa pertanyaan krusial, yaitu:

- Apa yang salah dengan perusahaan? Pihak yang bertanggung jawab terhadap manajemen risiko wajib mencermati pekerjaan individu maupun lingkungan tempat kerja secara keseluruhan.
- Bagaimana pengaruh suatu kejadian terhadap perusahaan? Segala kemungkinan kejadian yang berdampak besar atau kecil wajib dipertimbangkan secara rinci.
- Apa yang bisa perusahaan lakukan untuk mencegah kerugian atau memulihkan keadaan jika sudah terjadi kerugian?
- Bagaimana perusahaan membayar suatu risiko yang sudah terjadi?

2. Dalam IT Risk Management pastinya ada ancaman terhadap sistem yang mungkin terjadi. Sumber ancaman meliputi bencana alam, kegagalan sistem, kerusakan hardware dan software, malware, virus komputer, dan human error.

Contoh gangguan pada teknologi sistem informasi yaitu:

a) Kesalahan teknis (*technical errors*)

Kesalahan perangkat keras (*hardware problems*)

Kesalahan di dalam penulisan sintak perangkat lunak (*syntax errors*)

Kesalahan logika (*logical errors*)

b) Gangguan lingkungan (*environmental hazards*)

Kegagalan arus listrik karena petir

c) Kesalahan manusia (*human errors*)

3. Karena itulah diperlukan penjagaan ekstra ketat dari pihak jaringan teknologi Apabila perusahaan Anda memakai sistem jaringan nirkabel, maka pastikan Anda memiliki teknisi yang mampu mengamankan jaringan Apalagi *hacker* yang berpengalaman pasti bisa

memperoleh berbagai akses menuju jaringan dalam jangka waktu yang cepat. Semakin canggih *hacker*, maka data perusahaan Anda akan langsung terbuka bahkan tanpa Anda sadari. Pastikan perusahaan selalu mengunci *router* dan juga mengenkripsi seluruh informasi dari mata-mata. Bila perlu, selalu beri password dalam seluruh jaringan data komputer dan bila perlu cobalah untuk hidden seluruh system dengan menyembunyikan data, maka setidaknya Anda telah mencegah kejahatan dalam perusahaan Anda. Bila perlu, jangan ada orang lain yang mengakses komputer orang lain dengan sembarangan meskipun dalam satu perusahaan.

Nama : Ribhan Mandala

NIM : 202420035

MID

Petunjuk:

1. Silakan jawab pertanyaan berikut
2. Jawaban akan dinilai berdasarkan pemahaman yang anda miliki terhadap masing2 soalnya
3. Jawaban yang terindikasi hasil kolaborasi, maka hanya si 'penjawab' pertama yang dinilai, selebihnya tidak akan dinilai alias urung dapet A

Soal:

1. Jelaskan apa yang dimaksud dengan IT Risk Manajemen? Dan mengapa hal ini penting?
2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya
3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

Jawaban:

1. IT Risk Manajemen adalah keamanan informasi yang didefinisikan sebagai seperangkat mekanisme, teknik, tindakan, dan proses administratif yang digunakan untuk melindungi aset TI dari pihak yang tidak berwenang akses, manipulasi, modifikasi, kehilangan, dan dari pengungkapan data dan informasi yang tidak disengaja yang tertanam dalam aset ini.

IT Risk Manajemen penting dikarenakan pada setiap organisasi memiliki misi. Di era digital ini, karena organisasi menggunakan otomatis teknologi informasi (TI) sistem untuk memproses informasi mereka untuk dukungan yang lebih baik dari misi mereka, manajemen risiko memainkan peran penting dalam melindungi aset informasi, dan karena itu misinya, dari risiko terkait TI.

2. Dalam IT Risk Management pastinya ada ancaman terhadap sistem yang mungkin terjadi. Sumber ancaman meliputi bencana alam, kegagalan sistem, kerusakan hardware dan software, malware, virus komputer, dan human error.

Contoh gangguan pada teknologi sistem informasi yaitu:

- a) Kesalahan teknis (*technical errors*)

Kesalahan perangkat keras (*hardware problems*)

Kesalahan di dalam penulisan sintak perangkat lunak (*syntax errors*)

Kesalahan logika (*logical errors*)

b) Gangguan lingkungan (*environmental hazards*)

Kegagalan arus listrik karena petir

c) Kesalahan manusia (*human errors*)

3. Mengamankan asset IT yang saya kelola jika saya menjadi CIO (Chief Information Officer) dengan cara selalu mengidentifikasi area potensial yang rentan terhadap pelanggaran keamanan cyber dan harus mempraktikkan metode pencegahan untuk memastikan bahwa intranet perusahaan tetap aman.

Nama : Yusria Lenitasari
NIM : 202420003
Jurusan : Program Pasca Sarjana Teknologi Informatika Reguler B
MID : *IT Risk Management and Disaster Recovery*

1. Jelaskan apa yang dimaksud dengan IT Risk Manajemen? Dan mengapa hal ini penting?
2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya
3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

Jawab :

1. IT Risk Manajemen adalah suatu proses identifikasi kerentanan dan ancaman terhadap informasi yang digunakan oleh sebuah organisasi dan dilakukan oleh manajer IT untuk mencapai tujuan bisnis, mengurangi resiko, dan menyeimbangkan pengeluaran dalam mencapai keuntungan dan melindungi IT.

Mengapa penting, karena manajemen resiko adalah proses yang berlanjut dengan mengidentifikasi semua resiko yang akan terjadi dapat menghambat kesuksesan proyek maka perusahaan harus membuat keputusan berdasarkan pengalaman mengenai kemungkinan yang akan terjadi. Jika manajemen resiko diatur dengan baik, proses akan terus menerus mengidentifikasi masalah dan resolusi, maka sistem akan mudah melengkapi sistem lain. Ini termasuk organisasi, perencanaan dan penganggaran, dan kontrol biaya. Hal – hal yang tidak terduga akan berkurang karena penekanan akan menjadi manajemen yang proaktif dan bukan reaktif. Selain itu dengan menerapkan IT Risk Management dapat mengukur resiko dan memprediksi dampak dari resiko pada proyek. Hasilnya adalah resiko yang dapat diterima atau tidak dapat diterima. Persetujuan atau tidak dari suatu resiko biasanya tergantung pada tingkat toleransi manajer proyek Dengan menerapkan tiga proses IT risk manajemen yaitu *risk assessment*, *risk mitigation*, dan *evaluation and assessment* sehingga resiko IT dapat ditanggulangi.

2. Ancaman terhadap system terbagi menjadi dua yaitu ancaman aktif dan pasif.

1. Ancaman aktif

2. Ancaman pasif

Ancaman aktif

Merupakan ancaman yang sengaja dilakukan oleh manusia

Contoh :

I. Pencurian data

Jika informasi penting yang terdapat dalam database dapat diakses oleh orang yang tidak berwenang maka hasilnya dapat kehilangan informasi atau harta. Misalnya mata-mata industry yang memperoleh informasi persaingan berharga, penjahat computer yang dapat mencuri uang di bank.

II. Penggunaan system secara illegal

Orang yang tidak berhak mengakses informasi pada suatu system yang bukan menjadi haknya dapat mengakses system tersebut. Contohnya hacker yang menembus system keamanan dengan tujuan mendapatkan data atau informasi penting yang diperlukan, memperoleh akses ke system telepon, dan membuat sambungan telepon jarak jauh.

III. Penghacuran data secara illegal

Orang yang dapat merusak atau menghancurkan data atau informasi dan membuat berhentinya suatu system computer. Penjahat dengan cara ini tidak perlu berada ditempat kejadian. Ia dapat masuk ke jaringan computer suatu terminal dan menyebabkan kerusakan pada semua system dan hilangnya data atau informasi penting. Penjahat seperti ini biasa disebut cracker yaitu penjelol system computer yang bertujuan melakukan pencurian data atau merusak system.

IV. Modifikasi secara illegal

Perubahan data informasi dan perangkat lunak secara tidak disadari. Perubahan tersebut disebabkan oleh program aplikasi yang merusak (*malicious software*).

Ancaman Pasif

Merupakan suatu ancaman yang diakibatkan ketidaksengajaan

Contoh

I.Kegagalan Sistem

Kegagalan system yang menyebabkan data tidak konsisten, transaksi tidak berjalan lancar sehingga data menjadi tidak lengkap atau bahkan menjadi rusak atau hal lain seperti tegangan listrik yang tidak stabil.

II.Kesalahan Manusia

Kesalahan dalam hal penginputan data atau informasi yang dapat mengancam integritas system dan data.

III.Bencana Alam

Seperti gempa bumi, banjir, kebakaran, hujan, badai yang merupakan factor yang tidak terduga.

3. Cara mengamankan asset IT

1. Physical security adalah perlindungan terhadap personel, hardware, software, jaringan komputer dan data/informasi dari aneka keadaan/lingkungan fisik dan berbagai peristiwa yang dapat menyebabkan kerugian serius dan kerusakan bagi institusi/lembaga. Perlindungan ini meliputi perlindungan dari gangguan alam seperti gempa, badai, tsunami, banjir, longsor, salju, panas dan sebagainya, dan gangguan dari manusia seperti pencurian, perampokan, vandalisme, terorisme, pemogokan, dan sabotase.

2. Mengunci dan mengamankan ruang server dengan baik.

Ruang server biasanya penuh dengan peralatan penting perusahaan seperti hardware, software, firewall, router, switch, tape backup, distribution cable, sensor-sensor, dan masih banyak lagi. Ancaman yang dapat terjadi di ruang server adalah kehilangan hardware, software di dalam hardware tersebut, peralatan jaringan dirusak/ sabotase, temperatur ruangan tidak memenuhi syarat sehingga suhu naik dan dapat menimbulkan kebakaran atau shutdown, ruang server terlalu lembab akan dihuni oleh hama seperti, jamur, karatan, tikus, kutu dan binatang yang lain, yang tentu akan mengganggu kinerja server tersebut. Melakukan Countermeasure: setiap kali setup ruang server, harus dipastikan lingkungan pendukung ruang tersebut aman dan sehat. Kebijakan keamanan harus ditegakkan dengan benar, ruangan server harus terus menerus terkunci. Ruang server harus

menaati kebijakan tertutup rapat dan terkunci, dan siapa saja yang dapat keluar masuk ruangan server. Membatasi akses orang yang masuk keruang server.

3. Pasang peralatan surveillance

Membuat Catatan log orang masuk dan keluar ruang server sebaiknya dilakukan dengan akses elektronik, sehingga bila mereka melakukan akses ke pintu ang server akan selalu tercatat dengan baik. Masuk dan luar kapan saja tercatat dalam log. access code ke pintu-pintu mangan server dan catatan log elektronik sangat sulit untuk dikelabui karena menggunakan peralatan berbasis authentication yang kuat seperti smart card, pemindai iometric (seperti sidik jari), retina dan iris, pengenalan wajah, pengenalan suara bahkan sampai dengan pengenalan bentuk dan ukuran tubuh. Meletakkan Kamera dan beberapa sensor yang diletakkan di ruang dan sudut-sudut server akan mempersulit gerakan orang asing tersebut untuk melakukan akses yang tidak diinginkan. Kamera dan hard disk akan merekam segala perbuatan detik per detik (terus-menerus) tanpa terlewatkan

4. Memastikan tidak ada celah di peralatan yang sudah terkunci

segala peralatan yang dapat terhubung ke luar ruang server. Sebaiknya tutup port USB dan port ke storage server seperti NAS (network access server), termasuk SAN (storage area network), Wi-Fi, Bluetooth, cable modem fiber optic, satellite, dan lainnya. Paling tidak, lakukan pengawasan traffic yang keluar dari segala macam peralatan tersebut.

5. Melakukan pencatatan/ register terhadap asset IT

6. Pemasangan antivirus yang terpercaya disetiap computer

7. Pemblokiran instal aplikasi diluar ketentuan perusahaan

8. Melakukan penghindaran terhadap penggunaan flashdisk, harddisk yang dapat menyebabkan virus pada computer

9. Pemblokiran akses internet kepada pegawai

10. Dilarang membuka spam dari yang pengirim yang tidak dikenal

MID

Petunjuk:

1. Silakan jawab pertanyaan berikut
2. Jawaban akan dinilai berdasarkan pemahaman yang anda miliki terhadap masing2 soalnya
3. Jawaban yang terindikasi hasil kolaborasi, maka hanya si 'penjawab' pertama yang dinilai, selebihnya tidak akan dinilai ...alias urung dapet A

Soal:

1. Jelaskan apa yang dimaksud dengan IT Risk Manajemen? Dan mengapa hal ini penting?
2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya
3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

----- oOOo -----

Aldo Fajarino

202420004

MTI 23 Reg B

1. Menurut pendapat saya, IT Risk Manajemen merupakan suatu cara organisasi atau perusahaan untuk mengatur dan mengendalikan resiko yang mungkin terjadi dalam teknologi informasi yang ada di perusahaannya, mulai dari operasional, pencegahan, penanggulangan dampak resiko, recovery atau pemulihan kerusakan data, dan kemudian mengevaluasi resiko yang ada. Hal ini menjadi penting karena dapat meminimalisir dampak yang mungkin terjadi pada suatu komponen IT di perusahaan, IT risk manajemen juga perlu sebagai dasar fundamental pengambilan keputusan yang sifatnya menyeimbangkan antara operational cost dan economic cost.
2. Ancaman terhadap sistem yang biasa terjadi yaitu kerusakan perangkat, baik itu perangkat keras komputer maupun perangkat lunak, contohnya kerusakan pada harddisk yang dapat mengakibatkan kehilangan data-data penting di suatu perusahaan, karena seperti yang kita tahu, bahwa harddisk itu memiliki rentang usia, semakin tua usia harddisk, maka semakin besar resiko kerusakan pada harddisk tersebut. Ada ancaman human error atau kesalahan manusia maupun serangan secara fisik ke perangkat, untuk human error biasanya terjadi pada operator yang salah memasukkan kode inputan ke dalam komputer ataupun lalai dalam mengoperasikan komputer. Kemudian ada ancaman lain yang sering kita temui di internet contohnya berupa virus, malware, phishing, scam, dan fraud atau manipulasi data untuk kepentingan yang melanggar hukum, beberapa pihak dengan sengaja membuat suatu program yang sifatnya merusak ataupun mencuri data pada komputer yang terinfeksi. Ada juga ancaman dari dalam

atau internal perusahaan dimana terjadi pencurian data oleh karyawan dari perusahaan itu sendiri.

3. Menurut saya, dalam mengamankan aset IT yang dikelola, seorang CIO bertanggung jawab merencanakan teknologi informasi secara matang, perencanaan infrastruktur yang baik adalah kunci penting dalam dunia IT, pengelolaan dan perhitungan budget yang tepat juga harus dilakukan, dengan tetap memperhatikan performa dari komponen keamanan informasi. Keputusan yang diambil oleh seorang CIO harus berdasarkan Risk Management Program.

1. IT Risk manajemen adalah proses untuk mengidentifikasi kerentanan dan ancaman pada sumber daya informasi yang digunakan oleh sebuah organisasi dalam mencapai tujuan bisnis, dan menentukan tindakan pencegahan dalam meminimalisir resiko ke level yang dapat diterima, berdasarkan nilai dari sumber daya informasi untuk organisasi.

Hal ini penting karena informasi perlu dilindungi dari segala ancaman yang ada berupa: akses tidak sah, penyalahgunaan, manipulasi, modifikasi, dan kebocoran data. Oleh karena itu, organisasi/perusahaan diwajibkan untuk memiliki tindakan pencegahan andai-andai ancaman yang dimaksud menyerang organisasi/perusahaan.

2. Beberapa dari ancaman yang dimaksud adalah:

1. Properti yang bocor

- Pembajakan

Pembajakan adalah kegiatan penyalinan atau distribusi suatu perangkat lunak yang dilakukan secara illegal atau tidak sah.

- Pelanggaran Hak Cipta

Pelanggaran hak cipta adalah penggunaan suatu materi yang masih dilindungi hukum hak cipta tanpa seizin pencipta atau pemegang haknya.

2. Serangan Software

- Virus

Virus adalah sebuah program komputer perusak yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinannya ke dalam program atau dokumen lain pada sebuah system.

- Worm

Worm adalah sebuah program computer perusak yang dapat menggandakan dirinya dengan memanfaatkan suatu jaringan tanpa perlu campur tangan dari user itu sendiri. Tidak seperti virus, worm memanfaatkan vulnerability dari suatu sistem untuk menyisipkan dirinya.

- Macro

Macro adalah sebuah fungsi yang memungkinkan penggunaannya untuk melakukan banyak hal dalam waktu yang singkat. Dalam game, macro ini sangat merugikan pemain lain yang tidak menggunakan macro, dikarenakan pengguna macro akan mendapat kemenangan dalam waktu yang sangat singkat tanpa harus bersusah payah seperti pemain yang tidak menggunakan macro.

- DoS

Denial of Services atau DoS adalah jenis serangan cyber yang menyerang suatu sistem dengan memanfaatkan jaringan internet dengan cara menghabiskan resource yang dimiliki oleh suatu sistem sehingga sistem tersebut tidak dapat menjalankan fungsinya dengan benar, sehingga pengguna dari sistem tersebut tidak akan dapat mengakses sistem yang terkena serangan DoS.

3. Bencana Alam

Bencana alam dapat merusak perangkat keras secara fatal, seperti kabel terbakar, kehancuran server, server terpenggang, listrik arus pendek, dan kehancuran infrastruktur lain yang Sebagian besar bersifat tidak dapat diperbaiki. Selain itu bencana alam dapat berpotensi membunuh individual yang penting pada keberlangsungan suatu sistem.

4. Sabotase atau Vandalisme

Sabotase atau Vandalisme adalah sebuah kegiatan yang dilakukan dengan tujuan untuk merubah data dari sebuah sistem. Misalnya seorang hacker/peretas yang mengubah desain grafis dari suatu sistem sehingga tampilan dari sistem tersebut tidak sesuai/menyimpang dari yang seharusnya.

3. Dengan cara membuat kerja sama secara hukum dengan pihak ke-3 yang terpercaya terkait keamanan informasi sistem, berupa keamanan server dan jaringan nirkabel. Selain itu saya juga akan membentuk sebuah tim khusus agar dapat terus memonitor pihak ke-3 agar tidak terjadi pelanggaran kerja sama.

MID

Petunjuk:

1. Silakan jawab pertanyaan berikut
2. Jawaban akan dinilai berdasarkan pemahaman yang anda miliki terhadap masing2 soalnya
3. Jawaban yang terindikasi hasil kolaborasi, maka hanya si 'penjawab' pertama yang dinilai, selebihnya tidak akan dinilai ...alias urung dapet A

Soal:

1. Jelaskan apa yang dimaksud dengan IT Risk Manajemen? Dan mengapa hal ini penting?
2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya
3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

----- oOOo -----

Jawaban

1. IT risk Manajemen adalah sebuah strategi atau langkah yang dilakukan untuk mengamankan sebuah data perusahaan yang sangat penting dengan menerapkan manajemen resiko dengan membudayakan sebuah penggunaan fasilitas IT untuk menanggulangi resiko yang dihadapi oleh perusahaan tersebut. Mengapa hal ini penting sekali karena yang terutama adalah kita akan tahu bagaimana kedepannya serangan ataupun pencurian data perusahaan oleh orang asing atau virus dapat diantisipasi dan diatasi dengan melakukan langkah-langkah pengamanan yang efisien dan efektif menggunakan sebuah perangkat atau firewall.
2. Sumber ancaman yang dapat terjadi banyak sekali contohnya : pertama dari manusia internal perusahaan yaitu sebuah perilaku yang dilakukan oleh manusia yang dilakukan secara fisik seperti menghancurkan, membakar, bahkan merusak komponen perangkat sebuah server. Kedua ancaman berasal dari virus yaitu merupakan sebuah aplikasi atau program yang dapat merusak sebuah perangkat lunak atau software dengan cara menyebarkan virus kedalam sebuah sistem sehingga merusak semua file yang ada pada sebuah sistem tersebut seperti dokumen, aplikasi, bahkan sistem tersebut. Ketiga hackers adalah orang yang masuk dengan sengaja kedalam sebuah sistem komputer yang orang lain tidak ketahui yang merugikan karena mengambil atau mencuri data bahkan dapat merusak sistem komputer tersebut.

3. CIO merupakan sebuah jabatan yang bertanggung jawab untuk menjamin keakuratan data, ketepatan waktu, dan keamanan teknologi dan informasi yang dibutuhkan perusahaan untuk mencapai tujuan. Jika ini menjadi posisi saya yang akan dilakukan adalah :
 - a. Akan bertanggung jawab dalam mengamankan sebuah data atau aplikasi dalam perusahaan.
 - b. Akan bertanggung jawab dalam mengantisipasi berbagai macam serangan baik itu secara nyata maupun dunia maya
 - c. Akan bertanggung jawab dalam melakukan analisa dan perubahan teknologi yang sesuai dengan perkembangan zaman teknologi
 - d. Akan bertanggung jawab dalam melakukan strategi keamanan dan peluang bisnis dalam upaya meningkatkan infrastruktur teknologi.
 - e. Menjalin kerjasama tim dan melakukan pelayanan berbasis IT.

MID

Nama	: KhadijahThahira
NIM/ Kelas	:202420027/ MTI 232

Petunjuk:

1. Silakan jawab pertanyaan berikut
2. Jawaban akan dinilai berdasarkan pemahaman yang anda miliki terhadap masing2 soalnya
3. Jawaban yang terindikasi hasil kolaborasi, maka hanya si 'penjawab' pertama yang dinilai, selebihnya tidak akan dinilai ...alias urung dapet A

Soal:

1. Jelaskan apa yang dimaksud dengan IT Risk Manajemen? Dan mengapa hal ini penting?
2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya
3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

----- oOOo -----

1. IT Risk Management merupakan proses yang dilakukan oleh manager IT untuk mengelola resiko bisnis (seperti: ancaman, bencana, human error) menggunakan kerangka kerja IT Risk Management terhadap asset- asset system IT yang dimiliki oleh perusahaan tersebut (seperti: data customer) agar dapat mencapai tujuan dari visi&misi perusahaan tersebut.

Mengapa IT Risk Management di butuhkan ?

- Untuk memperkecil kemungkinan terjadinya resiko yang akan akan merugikan perusahaan
 - Untuk melindungi asset perusahaan, seperti : kehilangan data
 - Security itu seperti rantai terlihat kuat karena saling bertautan tapi kelemahannya juga ada pada sambungan rantai yang saling terkait
 - Untuk mencapai tujuan dari visi & misi perusahaan
 - Security bukan hanya sebuah status tetapi ada proses yang terus berjalan di dalamnya, proses yang berjalan ini harus mengikuti perkembangan dunia IT yang terbaru, karena semakin ketinggalan akses security yang di terapkan maka semakin besar resiko yang akan di timbulkan
 - Untuk menghandle human error yang menjadi factor pemicu utama terjadinya resiko di dalam asset IT, karena karyawan merupakan ancaman yang paling besar terhadap keamanan informasi.
2. Sumber – sumber ancaman :
 - Maksud dan tujuan dari metode yang digunakan adalah untuk mengeksploitasi kerentanan resiko yang akan datang
 - Terjadinya resiko dari kesalahan Situasi dan method yang di gunakan, contoh: perusahaan mengeluarkan banyak biaya menggunakan pihak ketiga (outsourcing) untuk mengamankan asset IT tetapi hasilnya ancaman dan resiko yang terjadi semakin banyak sehingga pemilihan pihak ketiga ini bukannya menguntungkan tapi malah merugikan perusahaan.

- Serangan dari pihak musuh atau diserang secara fisik oleh pihak lawan (rival) bisnis yang ada, contohnya: Ketika bulan Mei 2021 Palestina kembali perang dengan Israel, cyber Indonesia dan Malaysia membantu dengan cara meretas beberapa situs, CCTV, dan 300 nomor WhatsApp warga Israel, menurut komunitas cyber ini merupakan cara mereka untuk membantu warga Palestina
- Kesalahan manusia karena kelalaiannya, contoh : kasus pembobolan rekening Ilham Bintang yang dilakukan oleh karyawan bank bekerja sama dengan hacker untuk mengambil uang di rekening Ilham Bintang. Hacker tersebut mendapatkan data pribadi Ilham Bintang melalui karyawan bank, karyawan bank mendapatkan data pribadi Ilham Bintang melalui Sistem Laporan Informasi Keuangan (SLIK).
- Kegagalan struktural dari sumberdaya yang dikelola oleh organisasi contoh: perangkat lunak dan perangkat keras yang digunakan sudah ketinggalan zaman sehingga keamanan aset IT yang dimiliki oleh perusahaan sangat minim
- Bencana alam, contoh: banjir/ gempa bumi/ kebakaran yang mengakibatkan rusak atau lenyapnya aset IT yang dimiliki oleh perusahaan
- Ancaman risiko di luar dari organisasi IT, contoh: serangan hacker.

3. Langkah- Langkah yang akan saya lakukan untuk mengamankan aset IT:

- *Assessment*, merujuk pada pencarian risiko dan penilaian tingkat keparahan risiko.
- *Mitigation*, yaitu penanggulangan yang dilakukan untuk mengurangi dampak risiko.
- *Evaluation and Assessment*, merujuk pada evaluasi terhadap penanggulangan yang sudah dilakukan.

Mid Semester IT Risk Management

Mirza Eka Putra

202420034

MTI23B

1. Jelaskan apa yang dimaksud dengan IT Risk Manajemen? Dan mengapa hal ini penting?
2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya
3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

Jawab

1. IT Risk Manajemen adalah suatu cara untuk mengelola segala hal yang berkaitan dengan kerentanan di system IT baik hardware maupun software. Sehingga jika terjadi suatu ancaman maupun serangan terhadap sistem IT pada suatu tempat, pengelola IT pada tempat tersebut dapat menangani masalah tersebut. Dan Jika sistem tersebut mati dikarenakan serangan terhadap sistem IT, maka dengan Pengelolaan resiko IT maka system dengan cepat bangkit kemabali sehingga layanan IT bisa berjalan dengan baik.
2. Serangan terhadap sistem IT di era sekarang ini banyak sekali, baik langsung maupun tidak langsung.
 - A. Sumber Ancaman langsung yaitu misal Sumber ancaman dari serangan serangan terhadap sistem IT bisa dilakukakan dengan langsung misalnya merubah tampilan website (defeace website), mencoba dengan serangan brute force dalam upaya masuk ke suatu akun, merusak sistem sistem dengan masuk ke database dengan sql injection.
Contoh

- Gangguan yang muncul dengan dihapusnya database sistem,
- pengerusakan perangkat keras jaringan seperti kabel
- mengganti gambar di website

B. Sumber Ancaman tidak langsung misal

Sumber ancaman tidak langsung seperti beberapa komputer bisa dijadikan juga sebagai komputer yang secara tidak langsung menyerang suatu sistem (computer zombie), pengguna komputer yang dijadikan transit data untuk membanjiri sistem dengan harapan sistem tersebut down.

Sumber ancaman tidak langsung juga bisa didapat dengan bantuan seseorang (pihak internal) dengan cara menyogok agar orang bisa memberi password akun sistem.

3. Hal yang akan saya lakukan untuk mengamankan asset IT saya yaitu
 1. Backup File secara rutin
 2. Menjaga selalu Sistem Jaringan dengan memasang Firewall
 3. monitoring jaringan dengan berbagai aplikasi seperti the dude, cacti dsb
 4. selalu rutin mengecek akses Log Pada setiap perangkat jaringan, database, maupun aplikasi yang digunakan
 5. Menyediakan lokasi server yang tahan akan bencana alam(banjir dan gempa bumi)
 6. Monitoring Hardware jaringan seperti kabel yang bagus, switch yang terjaga, dan router yang selalu berada dalam kondisi prima.
 7. Menyediakan Sumber Listrik yang baik, tidak hanya listrik dari PLN tetapi juga backup listrik dari UPS untuk menjaga semua sistem tahan terhadap kerusakan

8. Pelatihan secara rutin terhadap staf IT untuk mengupdate ilmunya baik itu mengikuti
 1. Pelatihan jaringan seperti CCNA, CCNP, MTCRA, MTCRE, CCDA, CCNA Security
 2. Pelatihan security seperti CEH, mengikuti pelatihan dari ID-SIRTII, dan sebagainya
 3. Pelatihan pengamanan Aplikasi dan database

4. Bekerja sama dengan vendor untuk mengajari staf dalam keadaan real di lapangan (sharing ilmu) .

NAMA : Muhamad Yamin Achiruddin

NPM : 202420031

Soal:

1. Jelaskan apa yang dimaksud dengan IT Risk Manajemen? Dan mengapa hal ini penting?
2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya
3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

----- oOOo -----

Jawab :

1. IT Risk Management merupakan sebuah prinsip-prinsip risiko terhadap Instansi/Lembaga/Perusahaan yang menggunakan teknologi informasi untuk tujuan mengelola risiko yang berhubungan dengan Instansi/Lembaga/Perusahaan tersebut.
Mengapa hal ini penting, agar dapat mengidentifikasi kerentanan dan risiko-risiko yang berhubungan dengan berlangsungnya perusahaan.
2. Pada era pertumbuhan sistem informasi yang sangat cepat saat ini keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan, karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan. Pada dasarnya suatu sistem yang aman akan melindungi data didalamnya seperti identifikasi pemakai (user identification), pembuktian keaslian pemakai (user authentication), otorisasi pemakai (user authorization). Beberapa kemungkinan serangan (Hacking) yang dapat dilakukan, seperti Intrusion, denial of services, joyrider, vandal, hijacking, sniffing, spoofing dan lain-lain. Ancaman terhadap sistem informasi banyak macamnya, antara lain: pencurian data, penggunaan sistem secara ilegal, penghancuran data secara ilegal, modifikasi data secara ilegal, kegagalan pada sistem, kesalahan manusia (SDM-sumber daya manusia), bencana alam. Tujuan dari keamanan informasi yaitu mencegah ancaman terhadap sistem serta mendeteksi dan memperbaiki kerusakan yang terjadi pada sistem.
3. **A. Dalam Hal Jaringan**
Selalu mengunci router dan juga mengenkripsi seluruh informasi dari mata-mata. Memberi password dalam seluruh jaringan data komputer dan menghidden seluruh sistem.

B. Memperhatikan Phising

Memberi tahu pada karyawan untuk tetap berhati-hati pada situs yang meminta informasi dalam bentuk apapun. Pastikan untuk tetap membuat karyawan waspada selama mereka mengakses internet.

C. Backup Data

Selalu backup data atau file perusahaan sesering mungkin. Sebagai contoh apabila di kantor terjadi pemadaman listrik mendadak ataupun koneksi internet yang hilang seringkali membuat tugas maupun data informasi menjadi hilang.