UNIVERSITAS MULIA

IT Risk Management

UNIVERSITAS MULIA

Contents

1. The CIA triad
2. Identification,
3. authentication,
4. and authorization
5. Risk Classification

UNIVERSITAS MULIA

Manajemen Risiko TI

suatu proses identifikasi kerentanan dan ancaman terhadap sumber daya 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.

UNIVERSITAS MULIA

Manajemen Risiko TI

- Proses manajemen resiko yang merupakan proses berulang yang berlangsung. Ini adalah proses yang yang harus diulang tanpa batas, disebabkan lingkungan bisnis yang fleksibel atau terus berubah yang menyebabkan munculnya ancaman baru.
- Pilihan penanggulangan (kontrol)yang digunakan untuk mengelola resiko harus menjaga keseimbangan antara produktivitas, biaya, efektivitas penanggulangan, dan nilai aset informasi yang harus dilindungi.

UNIVERSITAS MULIA

Risiko tidak bisa dihilangkan.

Tetapi bisa dinimalisir

UNIVERSITAS MULIA

Kategori Manajemen Risiko TI

1. Strategi
2. Operasi/pengerjaan
3. Laporan Pengeluaran
4. Pemenuhan/Penyesuian

UNIVERSITAS MULIA

Proses Manajemen Risiko TI

1. **Mengidentifikasi Resiko**

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

2. **Menganalisis Resiko**

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

3. **Mengevaluasi Resiko**

Perusahaan mengevalusi resiko dengan menentukan besarnya resiko, yang merupakan kombinasi dari kemungkinan dan konsekuensi. Lalu Perusahaan membuat keputusan apakah resiko itu diterima atau tidak.

4. **Memantau dan Mempertimbangkan Resiko**

Ini adalah tahap dimana perusahaan memantau setiap resiko yang ada untuk menghindari resiko yang lebih besar.

UNIVERSITAS MULIA

Fungsi Manajemen Risiko TI

1. Memberikan panduan untuk membantu para eksekutif dan manajemen mengajukan pertanyaan kunci, membuat lebih baik, keputusan risiko-disesuaikan lebih banyak informasi dan membimbing perusahaan mereka sehingga risiko dikelola secara efektif
2. Membantu menghemat waktu, biaya dan tenaga dengan alat untuk mengatasi risiko bisnis
3. Mengintegrasikan manajemen TI terkait risiko bisnis menjadi manajemen risiko perusahaan secara keseluruhan
4. Membantu kepemimpinan memahami risiko perusahaan dan toleransi risiko
5. Memberikan panduan praktis didorong oleh kebutuhan kepemimpinan perusahaan di seluruh dunia

UNIVERSITAS MULIA

Rencana Kontingensi

Suatu tindakan yang dirancang untuk membantu organisasi merespon secara efektif dan cepat ketika sebuah organisasi mengalami suatu peristiwa tak terduga yang memiliki potensi untuk mempengaruhi kondisi keuangan, citra bisnis atau potensi pasar dari suatu perusahaan.

UNIVERSITAS MULIA

Sejarah Rencana Kontingensi

Selama masa krisisnya, rencana ini sering dikembangkan untuk mengeksplorasi dan mempersiapkan diri untuk kemungkinan situasi apapun. Masa Perang Dingin, banyak pemerintah membuat rencana kontingensi untuk melindungi diri mereka sendiri dan warga negara mereka dari serangan nuklir.

Contoh rencana kontinjensi yang dirancang untuk menginformasikan warga tentang bagaimana untuk bertahan hidup serangan nuklir adalah buku Survival Under Atomic Attack, Protect and Survive, and Fallout Protection, yang diterbitkan oleh pemerintah Inggris dan Amerika. Hari ini masih ada rencana kontinjensi di tempat untuk menghadapi serangan teroris atau bencana lainnya.

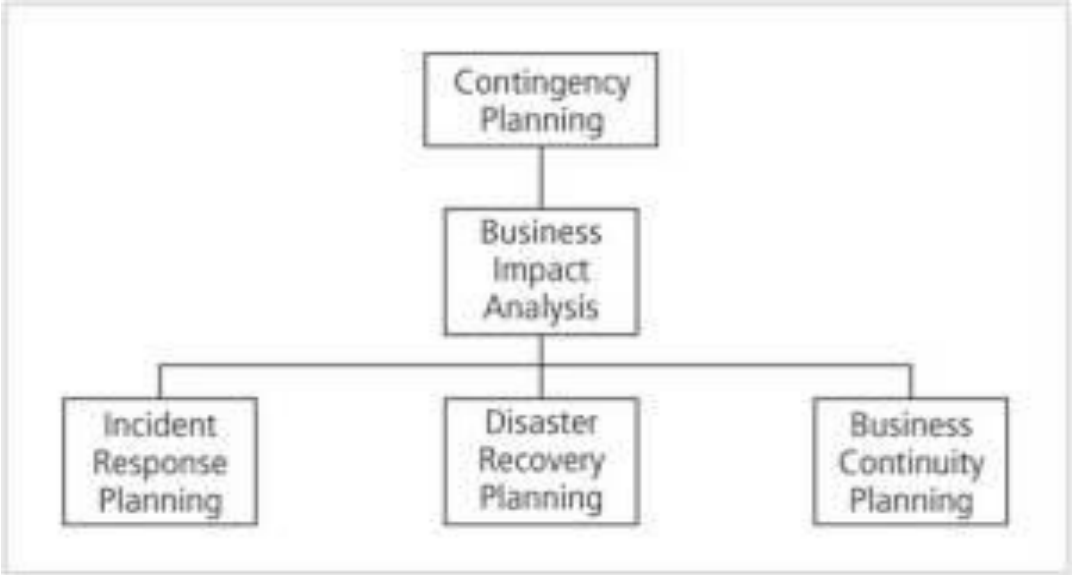
UNIVERSITAS MULIA

Manfaat Rencana Kontingensi

1. **Meminimalisir Kegagalan Rencana**
2. **Mengurangi Hubungan buruk dengan pelanggan**
3. **Menjaga Tetap Beroperasi**
4. **Meningkatkan Ketersediaan Jaminan dan Kredit**

UNIVERSITAS MULIA

Komponen Rencana Kontingensi



UNIVERSITAS MULIA

Komponen Rencana Kontingensi

– Business Impact Analysis

Pada komponen tahap ini, tim CP dilengkapi dengan informasi dan tantangan yang mereka hadapi. Setiap informasi yang diperoleh akan diidentifikasi dan dibuat perencanaan per setiap unit bisnis untuk mengembangkan skenario kesuksesan organisasi. Setelah skenario selesai, maka dilakukan tindakan lanjut untuk menanggapi kejadian tak terduga untuk selanjutnya dilakukan analisis biaya, perencanaan lanjut, serta hasil yang mungkin terjadi sebagai evaluasi organisasi di masa mendatang.

UNIVERSITAS MULIA

Komponen Rencana Kontingensi

– Incident Response Plan

Tahap ini bertujuan untuk menganalisis aktivitas sebagai deteksi dan antisipasi atas efek yang terjadi akibat dari kejadian yang tak terduga. Pada komponen tahap ini dilakukan pengukuran yang dilakukan ketika kejadian, lalu dibandingkan dengan kondisi sesudah dan sebelum kejadian. Tim juga diharapkan dapat merencanakan dan mendeteksi respon serta aksi yang harus dilakukan untuk menanggapi kejadian tersebut.

Komponen dari rencana kontinjensi ini terutama berfokus pada respon langsung yang diperlukan ketika insiden atau kejadian pertama terjadi. Rencananya dengan menguraikan lengkap serangkaian proses yang memandu orang lain dalam mengantisipasi, mendeteksi, dan mengurangi dampak kontinjensi pada aset bisnis.

UNIVERSITAS MULIA

Komponen Rencana Kontingensi

– Disaster Recovery Plan

Tahap komponen dimana perencanaan dilakukan atas antisipasi dan persiapan dari kejadian yang tak terduga. Pada tahap ini disusun skenario lanjut mulai dari proses yang paling penting bagi organisasi, serta melakukan restorasi sistem dan data penting perusahaan. Tahap ini juga menyiapkan kebijakan yang mengandung elemen-elemen seperti misalnya ruang lingkup, kebutuhan sumber daya, pelatihan, maintenance, dll.

komponen dari rencana kontinjensi ini terutama berfokus pada persiapan dan kemudian pemulihan operasi secara normal dan secepat mungkin setelah kontinjensi telah terjadi

UNIVERSITAS MULIA

Komponen Rencana Kontingensi

– Business Continuity Plan

Komponen dari rencana kontinjensi ini terutama berfokus pada memastikan bahwa fungsi bisnis yang penting bisa hilang pada saat kontingensi terjadi. mungkin saja melibatkan pada fasilitasi operasi bisnis di lokasi pengganti, sampai bisnis dapat mengembalikan operasi di lokasi asli

Tahap ini bertujuan untuk memastikan bahwa bisnis akan dapat tetap berjalan apabila terjadi kejadian yang tak diinginkan. Pada tahap ini dianalisis strategi berkelanjutan untuk masa mendatang serta manajemen resiko dan krisis atas respon (tindakan) kejadian tersebut.

UNIVERSITAS MULIA

Tahapan Rencana Kontingensi

1. **Siapkan analisis dampak bisnis** - digunakan untuk menentukan persyaratan kontingensi dan prioritas.
2. **Temukan kontrol preventif** - mencegah, mendeteksi, dan / atau mengurangi dampak terhadap organisasi kontinjensi. .
3. **Mengembangkan strategi pemulihan** - merancang untuk memulihkan atau me-restore operasi secepat dan seefektif mungkin
4. **Mengembangkan rencana kontinjensi** - memperjelas peran, tanggung jawab, tim, dan prosedur yang terkait dengan memulihkan operasi normal menyusul gangguan yang ditimbulkan oleh kontingensi.
5. **Rencana pengujian dan pelatihan** - mengidentifikasi dan mengevaluasi kemampuan tim pemulihan (Recovery Team) untuk melaksanakan rencana kontingensi dengan cepat dan efektif.

UNIVERSITAS MULIA

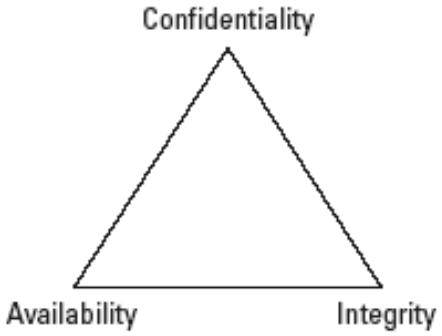
Apa yang dilindungi dari Managemen Risiko TI?

UNIVERSITAS MULIA

Informasi

UNIVERSITAS MULIA

The CIA Triad



Keamanan Informasi mempunyai 3 Goal Utama:

- Maintain the confidentiality,
- integrity, and
- availability of information resources.

UNIVERSITAS MULIA

Confidentiality

Mekanisme kerahasiaan memberlakukan kerahasiaan data Anda.

- **Mekanisme kontrol akses: Mencegah orang yang tidak berwenang mengakses sistem.**
- **Kontrol keamanan sistem file: Cegah individu yang diberi wewenang untuk menggunakan sistem agar tidak melampaui otoritas mereka dan membaca informasi rahasia yang seharusnya tidak dapat mereka akses.**
- **Kriptografi: Dapat digunakan untuk mengenkripsi konten file sensitif dan melindunginya dari pengintaian, bahkan ketika kontrol akses dan mekanisme keamanan sistem file gagal.**

UNIVERSITAS MULIA

Government Information Classification Structure

Unclassified (Tidak terklasifikasi): Informasi ini dapat dibagikan secara bebas dengan publik tanpa risiko kerusakan keamanan nasional. Informasi ini tunduk pada pengungkapan publik di bawah Freedom of Information Act (FOIA). Contoh dari jenis informasi ini adalah bagian dari Kode Peraturan Federal.

Sensitive But Unclassified (SBU): Level ini juga dikenal sebagai For Official Use Only (FOUO); informasinya mungkin tidak mempengaruhi keamanan negara, tetapi dilindungi dari pelepasan FOIA oleh satu dari sembilan pengecualian terhadap hukum. Penunjukan ini sering digunakan untuk informasi pribadi yang dimiliki pemerintah tentang seorang individu.

Info Terpercaya (Confidential): Informasi ini akan menyebabkan kerusakan keamanan nasional jika dirilis ke pihak yang tidak berwenang. Ini adalah tingkat terendah di mana informasi dianggap "diklasifikasikan" oleh pemerintah dan mengharuskan semua penerima memiliki izin keamanan formal.

Rahasia (Secret): Informasi ini akan menyebabkan kerusakan serius pada keamanan nasional jika dirilis ke pihak yang tidak berwenang.

Top Secret: Informasi ini akan menyebabkan kerusakan yang sangat parah pada keamanan nasional jika dirilis kepada pihak yang tidak berwenang.

UNIVERSITAS MULIA

Integrity

Mekanisme kontrol akses: Mencegah orang yang tidak berwenang mengakses sistem dan memodifikasi data.

Kontrol keamanan sistem file: Kontrol hak pengguna data. Mereka mungkin memberikan sejumlah besar pengguna izin untuk membaca data tetapi mencegah beberapa orang tertentu memodifikasi data.

Kriptografi: Sistem menggunakan tanda tangan digital (digital Signatures) untuk mengonfirmasi bahwa pesan tidak diubah dalam perjalanan.

UNIVERSITAS MULIA

Availability

Ketersediaan membutuhkan kompromi.

Jika mekanisme kerahasiaan dan integritas dilakukan secara ekstrem, mereka mungkin mencegah pengguna yang berwenang mengakses data dan menggunakannya secara sah.

Selain itu, peretas mungkin meluncurkan serangan yang dirancang khusus untuk mencegah individu yang berwenang mengakses sumber daya komputasi.

Jenis serangan ini, dikenal sebagai serangan penolakan layanan (DoS), cukup umum. Faktanya, serangkaian serangan DoS yang dipublikasikan pada Februari 2000 praktis menutup beberapa situs web e-commerce utama, termasuk Yahoo !, Amazon.com, dan eBay.

UNIVERSITAS MULIA

Identification, Authentication, and Authorization

the security services necessary to support the three legs of the CIA

- Izinkan pengguna mengidentifikasi diri mereka sendiri ke sumber daya yang dilindungi
- Menyediakan sarana bagi sumber daya untuk secara objektif mengkonfirmasi identitas pengguna
- Berikan administrator sumber daya suatu mekanisme untuk menentukan pengguna mana yang dapat mengakses sumber daya dan tindakan yang mungkin dilakukan pengguna tersebut

Identification

Mekanisme identifikasi memungkinkan pengguna untuk mengidentifikasi diri mereka ke sumber daya. Mereka tidak memberikan bukti identitas; mereka hanya menyediakan sarana bagi pengguna untuk menyatakan identitasnya.

Mekanisme identifikasi yang paling umum sekarang digunakan adalah nama pengguna (atau ID login), sering kali terdiri dari kombinasi huruf dari nama depan dan belakang pengguna.

Sistem harus memiliki sarana untuk mengidentifikasi pengguna individu untuk mencapai akuntabilitas.

UNIVERSITAS MULIA

Authentication

authentication mechanisms:

- **Sesuatu yang diketahui pengguna (Something The User Know):** Sepotong informasi pribadi ini hanya diketahui pengguna. Paling sering mengambil bentuk kata sandi yang disediakan untuk sistem dalam kombinasi dengan nama pengguna. Dengan memberikan nama pengguna, pengguna mengidentifikasi dirinya ke sistem. Namun, banyak orang mungkin tahu (atau dapat menebak) nama pengguna.

- **Sesuatu dari pengguna itu sendiri (Something The User is):** Karakteristik fisik ini unik bagi pengguna. Pengguna mungkin diminta untuk menyerahkan pembacaan sidik jari, pemindaian retina, atau pemindaian iris atau mungkin diminta untuk mengucapkan frasa ke dalam perangkat cetak suara. Jenis-jenis pengukuran ini, berdasarkan pada fitur biologis tubuh pengguna, dikenal sebagai pengukuran biometrik.

- **Sesuatu yang dimiliki pengguna (Something The User has):** Elemen ini bergantung pada kepemilikan fisik perangkat, seperti beberapa bentuk kunci, kartu akses, atau perangkat fisik lainnya yang entah bagaimana berinteraksi dengan sistem keamanan untuk membuktikan identitas pengguna.

UNIVERSITAS MULIA

Mother’s maiden Name

Selama bertahun-tahun, lembaga keuangan dan pihak lain yang peduli dengan keamanan menggunakan nama gadis ibu sebagai mekanisme otentikasi karena asumsi yang tidakjelas dari pengetahuan ini. Sementara itu, adopsi yang luas dari teknik ini telah mempermudah proses pemberian otentikasi.

UNIVERSITAS MULIA

Other popular Multifactor Authentication Techniques

1. A password and a biometric measurement (something the user knows and something the user is)
2. A physical key and a password (another example of something the user has and something the user knows)
3. An access card and a biometric measurement (something the user has and something the user is)

UNIVERSITAS MULIA

Authorization

Setelah pengguna mengidentifikasi dirinya dan telah memenuhi mekanisme otentikasi yang berlaku, sistem harus memiliki beberapa cara untuk memutuskan tingkat akses untuk diberikan. Proses ini dikenal sebagai **otorisasi**, dan mengontrol hak istimewa yang diberikan kepada pengguna sistem.

UNIVERSITAS MULIA

Threats

Ancaman adalah segala aktivitas potensial yang mungkin melanggar kerahasiaan, integritas, atau ketersediaan sumber daya komputasi Anda.

SANS Institute merekomendasikan agar Anda melihat tugas prioritas ancaman dari tiga perspektif berbeda:

1. **Tujuan bisnis:** Anda harus menganalisis tujuan dan sasaran organisasi Anda dan mengevaluasi ancaman berdasarkan analisis itu
2. **Data yang divalidasi:** Gagasan di balik data yang divalidasi adalah belajar dari kesalahan Anda. Ini mencakup pencatatan setiap kompromi keamanan yang terjadi pada jaringan Anda.
3. **Best Practice industri**: Perluas penggunaan data yang divalidasi dan pelajari juga kesalahan orang lain. Semua sistem harus dilindungi terhadap sejumlah ancaman keamanan komputer.

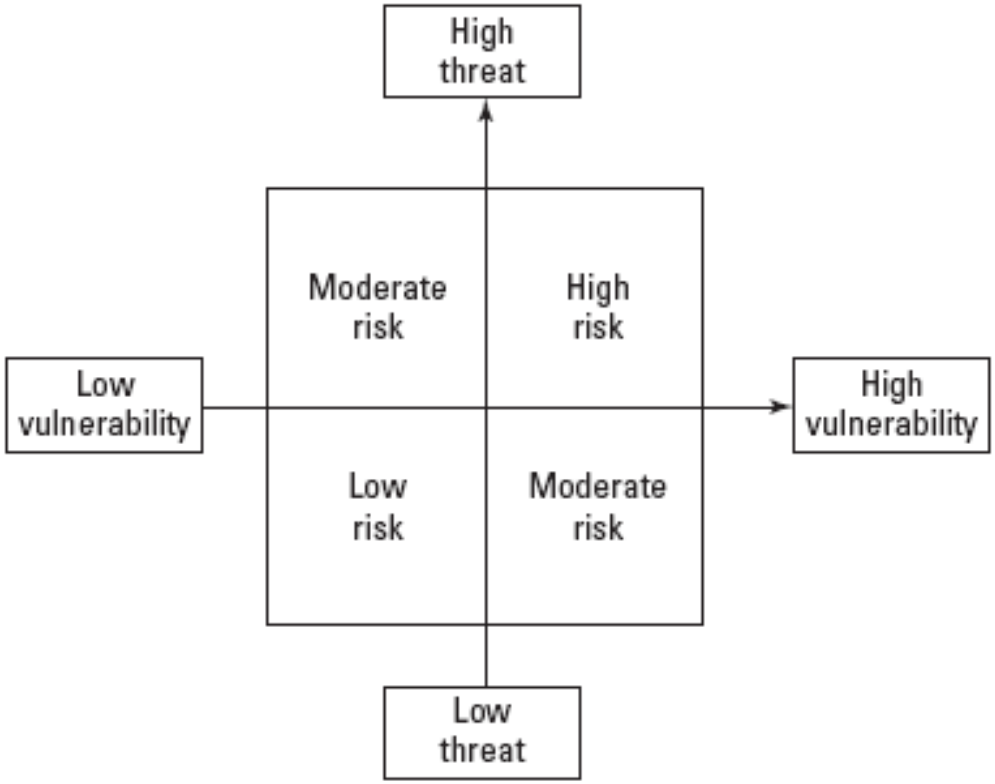
UNIVERSITAS MULIA

vulnerability

- A *vulnerability (Ke-rentan-an)*
- Hal yang ada ketika kelemahan dalam postur keamanan Anda membuka Anda terhadap potensi ancaman.
- Misalnya, jika Anda memiliki atap yang bocor, itu adalah kerentanan yang membuat Anda dalam bahaya kerusakan akibat hujan lebat.

UNIVERSITAS MULIA

Risks Classification Matrix



Tugas

Temukan Permasalahan IT dan tentukan jenis Risiko (Low/Moderate/High Risk) pada permasalahan IT tersebut dengan menggunakan Risk Classification Matrix.

- Ketahui ke-rentan-an Permasalahan tersebut
- Ketahui ancamannya
- Tentukan Jenis Risikonya
- Apa alasan anda menentukan risiko tersebut.

UNIVERSITAS MULIA

terimakasih

UNIVERSITAS MULIA