MATERI PERTEMUAN

MINGGU KE IX

MENGAMANKAN SISTEM

SIKLUS HIDUP SISTEM KEAMANAN INFORMASI

Sistem keamanan komputer dikembangkan dengan menerapkan metoda-metoda yang telah mapan yang terdiri dari : analisis sistem; desain; implementasi; dan operasi, evaluasi serta kendali, seperti di bawah ini:

FASE SIKLUS HIDUP	SASARAN
Analisis Sistem	Analisis kerentanan sistem informasi terutama yang berhubungan dengan hambatan dan kerugian yang mungkin timbul.
Perancangan Sistem	Perancangan pengukuran keamanan dan rencana kontigensi untuk mengatasi kerugian.
Implementasi Sistem	Implementasi ukuran keamanan seperti rancangan.
Operasi, evaluasi, dan pengendalian sistem	Operasi sistem dan penilaian efektifitas dan efisiensinya. Perubahan sesuai dengan kondisi yang dibutuhkan.

SISTEM KEAMANAN INFORMASI DI DALAM ORGANISASI

Sistem keamanan informasi harus diatur oleh seorang **kepala petugas keamanan (*Chief Security Officer*).** Yang mana untuk menjaga independensinya, CSO harus bertanggungjawab secara langsung kepada dewan direktur. Laporan-laporan CSO harus meliputi semua tahap siklus daur hidup yang telah disebutkan sebelumnya. Ada dua pendekatan dasar yang dipakai untuk meneliti kerentanan dan ancaman-ancaman sistem informasi, yaitu:

- **PENDEKATAN KUANTITATIF.** Di dalam pendekatan kwantitatif untuk penaksiran risiko, setiap kemungkinan kerugian dihitung sesuai hasil biaya kerugian perorangan dikalikan dengan kemungkinan munculnya. Ada beberapa kesulitan di dalam menerapkan pendekatan kwantitatif untuk menaksir kerugian, adalah sebagai berikut:

- Kesulitan mengidentifikasi biaya relevan per kerugian dan kemungkinan-kemungkinan yang terkait.
- Kesulitan menaksir kemungkinan dari suatu kegagalan yang memerlukan peramalan masa depan.

- **PENDEKATAN KWALITATIF.** Pendekatan kwalitatif untuk penaksiran risiko dilakukan dengan mengurutkan kerentanan dan ancaman sistem, dan menyusun secara subyektif menurut sumbangan mereka terhadap kemungkinan total kerugian perusahaan. Terlepas metoda yang digunakan, setiap analisa harus mencakup kemungkinan kerugian untuk masalah berikut ini:

  - Gangguan Bisnis
  - Kehilangan Perangkat Lunak (*Software*) dan Kehilangan Perangkat Keras (*Hardware*)
  - Kehilangan Data
  - Kehilangan Fasilitas-Fasilitas dan Kehilangan Layanan Pegawai

KERENTANAN DAN ANCAMAN

Kerentanan adalah suatu kelemahan di suatu sistem. Sedangkan, **Ancaman** adalah suatu eksploitasi potensial kerentanan sistem. Ada 2 (dua) kategori yang menjadi ancaman sistem, yaitu:

- **ANCAMAN AKTIF.** Yang menjadi ancaman aktif adalah seperti upaya penipuan komputer dan juga kasus sabotase komputer. Terdapat metoda-metoda yang biasa dipakai untuk melakukan penipuan sistem informasi:

  - **Manipulasi masukan.** Dalam banyak kasus penipuan komputer, manipulasi masukan adalah metoda yang paling banyak digunakan yang merupakan metoda yang memerlukan paling sedikit kecapakan teknis.

- **Gangguan program.** Gangguan program barangkali adalah metoda yang paling sedikit digunakan untuk melakukan penipuan komputer. Hal dikarenakan metoda ini memerlukan keterampilan programming yang mumpuni yang mana hanya dikuasi oleh beberapa orang saja. Dimana ada istilah **Trapdoor** yang merupakan Titik masuk tak terdokumentasi rahasia di satu program untuk memberikan akses tanpa metode-metode otentifikasi normal. **Trapdoor** telah dipakai secara benar selama bertahun-tahun oleh pemogram untuk mencari kesalahan program.
- **Gangguan file secara langsung.** Gangguan file secara langsung terjadi ketika seseorang menemukan jalan untuk membypass proses normal untuk memasukkan data ke program komputer.
- **Pencurian data.** Pencurian data adalah masalah yang serius di dalam bisnis sekarang ini.
- **Sabotase.** Sabotase komputer adalah suatu bajaya yang sangat serius bagi semua sistem informasi. Kasus sabotase komputer bisa saja terjadi dikarenakan adanya pihak yang tidak puas terkait suatu keputusan, seperti seorang karyawan. Ada beberapa metoda dari sabotase yang digunakan, antara lain:

- **Logic Bomb.** Logic bomb merupakan metode tertua yang digunakan untuk tujuan sabotase. Logic Bomb akan ditempatkaan atau dikirmkan secara diam-diam pada suatu sistem komputer yang menjadi target dan akan meledak bila pemicunya diaktifkan.
- **Trojan Horse.** Virus trojan horse merupakan perangkat lunak yang fungsinya untuk merusak. Virus ini merupakan sejenis malware yang berpura-pura untuk menjadi perangkat lunak lain. Trojan horse hadir seperti perangkat lunak biasa dan virus ini akan meminta izin akses perangkat. Trojan horse biasa digunakan untuk mengambil data-data penting dari korban.
- **Virus Program.** Salah satu jenis dari virus program yang menyebar dengan sendirinya di atas suatu jaringan komputer adalah worm.

- **Penggelapan atau pencurian sumber daya informasi.** Salah satu jenis penggelapan sumber daya komputer adalah ketika penggunaan sumber daya komputer-komputer perusahaan digunakan karyawan untuk urusan bisnis mereka sendiri.

Cara utama untuk mencegah penggelapan dan sabotase adalah menerapkan jenjang memadai pada pengendalian akses. Ada 3 (tiga) jenjang pengendalian akses, antara lain:

SITE-ACCESS CONTROLS

Site access controls atau pengendalian akses situs merupakan serangkaian prosedur dan kebijakan yang dirancang untuk mengelola akses ke situs atau area fisik di mana sistem informasi disimpan atau dioperasikan. Tujuan pengendalian akses fisik adalah untuk memisahkan secara fisik, individu yang tidak memiliki otorisasi dari sumberdaya komputer yang ada. Pemisahan fisik ini harus diterapkan pada perangkat keras, area masukan, keluaran dan librari data, dan kabel kabel komunikasi. Beberapa contoh dari site access controls dalam mengamankan sistem informasi antara lain:

- **Identifikasi dan autentikasi pengguna.** Organisasi harus memastikan bahwa pengguna yang mengakses situs atau area fisik memiliki identitas yang valid dan diotentikasi sebelum diberikan

akses. Ini dapat mencakup penggunaan kartu akses, kode akses, atau penggunaan biometrik seperti sidik jari atau wajah.

- **Pengendalian akses fisik.** Organisasi harus memastikan bahwa area fisik di mana sistem informasi disimpan atau dioperasikan dilindungi dengan baik dan hanya dapat diakses oleh orang yang berwenang. Ini dapat mencakup penggunaan gembok, pengamanan dengan sistem keamanan elektronik, atau pengamanan dengan personel keamanan.
- **Pembatasan akses logis.** Organisasi harus memastikan bahwa pengguna hanya memiliki akses ke sistem informasi dan data yang diperlukan untuk melakukan tugas mereka. Ini dapat dicapai melalui hak akses yang ditetapkan, pengendalian akses jaringan, dan penggunaan perangkat lunak pengamanan seperti firewall.
- **Pemantauan akses.** Organisasi harus memantau akses ke situs atau area fisik di mana sistem informasi disimpan atau dioperasikan, termasuk pencatatan waktu dan kegiatan yang dilakukan oleh pengguna. Ini dapat membantu mengidentifikasi kegiatan yang mencurigakan atau pengguna yang berlaku tidak wajar.

- Pelatihan dan kesadaran. Organisasi harus memberikan pelatihan kepada pengguna tentang pengendalian akses situs dan memastikan bahwa mereka memahami pentingnya pengendalian akses untuk menjaga keamanan sistem informasi.

SYSTEM-ACCESS CONTROLS

Pengendalian akses sistem adalah pengendalian yang berbentuk perangkat lunak, yang dirancang untuk mencegah pemanfaatan sistem oleh orang yang tidak berhak. Pengendali ini membuktikan keaslian pemakai dengan ID pemakai, kata sandi, alamat protokol internet, dan alat-alat perangkat keras

FILE-ACCESS CONTROLS

Pengendalian akses file mencegah akses yang tidak sah ke file data dan file-file program. Pengendalian akses file paling pokok adalah penetapan petunjuk otorisasi dan prosedurprosedur untuk mengakses dan mengubah file-file.

- **ANCAMAN PASIF.** Ancaman-ancaman pasif termasuk permasalahan kegagalan tenaga dan perangkat keras. Contoh dari ancaman pasif adalah seperti sistem yang bermasalah, dan juga dampak dari adanya bencana alam. Sistem yang bermasalah juga dapat terjadi dikarenakan adanya kegagalan-kegagalan peralatan dan komponen. Pengendalian untuk ancaman pasif dapat bersifat **preventive atau korektif.**

PENGENDALIAN PREVENTIVE

Pengendalian preventif dalam ancaman sistem informasi adalah serangkaian langkah atau kebijakan yang dirancang untuk mencegah atau mengurangi kemungkinan terjadinya ancaman terhadap sistem informasi sebelum terjadi. Pengendalian preventif bertujuan untuk meminimalkan risiko keamanan informasi dengan mengidentifikasi potensi ancaman dan mengambil tindakan yang tepat untuk mencegahnya. Beberapa contoh pengendalian preventif dalam ancaman sistem informasi antara lain:

- **Menerapkan kebijakan keamanan yang ketat.** Organisasi harus memiliki kebijakan keamanan yang jelas dan ketat, yang mencakup prosedur keamanan, aturan akses, dan pengawasan yang ketat terhadap akses ke sistem.
- **Menggunakan teknologi keamanan yang canggih.** Organisasi harus menggunakan teknologi keamanan yang canggih seperti firewall, antivirus, dan enkripsi data untuk mencegah ancaman dari luar atau dari dalam.

- **Pelatihan dan kesadaran karyawan.** Organisasi harus memberikan pelatihan dan kesadaran kepada karyawan tentang keamanan informasi, serta menjelaskan risiko dan ancaman yang mungkin timbul dari tindakan yang tidak aman.
- **Pemantauan dan penilaian risiko secara teratur.** Organisasi harus melakukan pemantauan dan penilaian risiko secara teratur untuk mengidentifikasi potensi ancaman dan mengambil tindakan preventif yang sesuai.
- **Melakukan pembaruan sistem secara rutin.** Organisasi harus melakukan pembaruan sistem secara rutin untuk memperbaiki kerentanan dan menghindari serangan yang mungkin timbul dari kerentanan tersebut.

PENGENDALIAN KOREKTIF

Pengendalian korektif dalam ancaman sistem informasi adalah serangkaian langkah atau kebijakan yang dirancang untuk mengatasi ancaman yang telah terjadi atau merespon serangan terhadap sistem informasi. Pengendalian korektif bertujuan untuk mengurangi dampak dari ancaman dan memulihkan sistem informasi kembali ke kondisi normal setelah terjadi serangan. Beberapa contoh pengendalian korektif dalam ancaman sistem informasi antara lain:

- **Pemulihan system.** Organisasi harus memiliki prosedur pemulihan sistem yang tepat untuk memulihkan sistem informasi ke kondisi normal setelah terjadi serangan.
- **Investigasi keamanan.** Organisasi harus melakukan investigasi keamanan setelah terjadi serangan untuk mengidentifikasi penyebab serangan dan mengambil tindakan preventif yang sesuai.

- **Pemulihan data.** Organisasi harus memiliki cadangan data yang cukup untuk memulihkan data yang hilang akibat serangan.
- **Perbaikan kelemahan.** Organisasi harus melakukan perbaikan pada kelemahan sistem yang telah dieksploitasi oleh serangan.
- **Pelaporan kejadian.** Organisasi harus melaporkan kejadian keamanan yang signifikan kepada pihak berwenang dan pelanggan yang terpengaruh.

Selain pengendalian preventive dan korektif terdapat juga **manajemen risiko bencana** dalam menghindari ancaman keamanan sistem informasi adalah suatu pendekatan yang dirancang untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengelola risiko yang terkait dengan bencana terhadap sistem informasi. Manajemen risiko bencana bertujuan untuk meminimalkan dampak dari bencana dan memastikan kelangsungan bisnis setelah terjadi bencana.

Beberapa contoh manajemen risiko bencana dalam menghindari ancaman keamanan sistem informasi antara lain:

- **Identifikasi Risiko.** Organisasi harus mengidentifikasi semua potensi risiko bencana terhadap sistem informasi, termasuk risiko dari bencana alam, serangan siber, dan kegagalan sistem. Hasil penelitian menunjukkan frekwensi bencana dari berbagai sebab:

  - Bencana alam 30%
  - Tindakan yang disengaja 45%
  - Kesalahan manusia 25%

- **Penilaian Risiko.** Organisasi harus mengevaluasi dampak dari setiap risiko yang teridentifikasi terhadap sistem informasi dan menentukan prioritas untuk tindakan pencegahan yang diperlukan.

- **Perencanaan mitigasi.** Organisasi harus mengembangkan rencana mitigasi untuk setiap risiko bencana terhadap sistem informasi, termasuk strategi untuk mengurangi dampak dan waktu pemulihan setelah terjadi bencana. Perancangan rencana pemulihan bencana meliputi tiga komponen utama:

  - Menilai kebutuhan-kebutuhan penting perusahaan.
  - Membuat daftar prioritas daftar pemulihan.
  - Menetetapkan strategi dan prosedur pemulihan. Rancangan strategi pemulihan perlu mempertimbangkan hal-hal:

    - pusat respons darurat
    - prosedur-prosedur ekskalasi dan perubahan pelaksanaan pemrosesan
    - rencana relokasi dan penggantian pegawai
    - rencana penyediaan cadangan, dan rencana pengujian dan pemeliharaan sistim

- **Pelatihan dan Latihan.** Organisasi harus melatih karyawan tentang rencana mitigasi bencana dan melakukan latihan simulasi untuk memastikan kesiapan dalam menghadapi bencana.
- **Evaluasi dan perbaikan.** Organisasi harus mengevaluasi rencana mitigasi bencana secara teratur dan melakukan perbaikan yang diperlukan untuk memastikan bahwa sistem informasi mereka tetap aman dari ancaman bencana.

INDIVIDU YANG DAPAT MENIMBULKAN ANCAMAN SISTEM INFORMASI

Suatu serangan yang sukses di suatu sistem informasi, pada umumnya memerlukan akses ke perangkat keras, file data yang bersifat penting/sensitive, atau juga program kritis. Ada 3 (tiga) kategori indivisu yang bisa menimbulkan serangan ke sistem informasi antara lain:

- **KARYAWAN SISTEM INFORMASI.** Yang disebut sebagai karyawan sistem informasi, meliputi:

- Karyawan pemeliharaan komputer
- Programmer
- Operator komputer dan jaringan
- Karyawan administrasi sistem informasi
- Karyawan pengendalian data

- **PARA PEMAKAI.** Yang disebut sebagai para pemakai terdiri dari kelompok orang yang beragam dan satu sama lain dapat dibedakan berdasarkan kegiatan fungsional mereka tanpa memandang pengolahan data.
- **PENGGANGGU.** Pengganggu adalah setiap orang yang mengakses peralatan, data elektronik, atau memfile tanpa otorisasi yang tepat. Diantara individu pengganggu ada juga yang disebut dengan Hacker. Hacker adalah seorang pengganggu yang menyerang suatu sistem untuk ke-isengan dan tantangan dan serangan yang ditimbulkan merusak sistem tersebut.