**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

**KDS – Name SME**

**Session 09**

**Incident Response Preparation, Organization and Prevention**

1. **Contingency planning proses**

Untuk memulai proses dari perencanaan kemungkinan yang akan terjadi, pertama-tama sebuah organisasi atau perusahaan harus menetapkan unit yang akan bertanggung jawab terhadap kebijakan dan rencana yang suatu saat akan muncul dari proses. Sebelum adanya perencanaan yang berarti, mereka yang ditugaskan harus menentukan ruang lingkup proyek perencanaan dan mengidentifikasi sumber daya yang digunakan. Oleh karena itu *Contingency Planning Management Team* (CPMT) dibentuk untuk tujuan tersebut. CPMT juga bertanggung jawab terhadap fungsi – fungsi tambahan lainnya, seperti:

* Mendapatkan komitmen dan dukungan dari senior management.
* Menulis dokumen rencana kemungkinan yang akan terjadi.
* Melakukan *Business Impact Analysis* (BIA), yang termasuk:
  + Membantu mengidentifikasi dan memprioritaskan ancaman dan serangan.
  + Membantu mengidentifikasi dan memprioritaskan fungsi – fungsi bisnis.
* Mengorganisir tim bawahan, seperti:
  + *Incident Response*
  + *Disaster Recovery*
  + *Business Continuity*
  + *Crisis management*

Sebuah daftar nama posisi yang umum untuk CPMT termasuk posisi – posisi berikut ini:

* *Champion:* Manager level tinggi yang memiliki pengaruh dan sumber daya yang dapat digunakan untuk membatu tim proyek, mempromosikan tujuan dari proyek CP, dan mendukung hasil dari usaha gabungan. Biasanya CIO atau CEO secara ideal.
* *Project Manager:* Manager level menengah atau mungkin CISO, harus memimpin sebuah proyek dan memastikan perencanaan proses proyek digunakan, rencana proyek yang lengkap dan berguna telah dibuat, dan sumber daya proyek diatur dengan hati-hati agar mencapai tujuan proyek.
* *Team Members:* anggota tim proyek harus menjadi manajer dari perwakilan mereka dari komunitas yang bermacam-macam, seperti bisnis, IT dan SI.
* Perwakilan dari unit bisnis: area lainnya dari bisnis, seperti *human resource, public relation, finance*, *legal,* dan / atau *physical plant operations* harus diwakilkan. Tim juga harus menambahkan perwakilan seperti:
  + Perwakilan manager bisnis yang familiar terhadap operasi area fungsional masing-masing harus menyediakan rincian kegiatan mereka dan memberikan wawasan tentang kekritisan fungsi mereka untuk kelanjutan suluruh bisnis
  + Manager IT yang familiar terhadap sistem yang beresiko dan rencana *Incident Response* (IR), *Disaster Recovery* (DR), dan rencana kelangsungan bisnis yang diperlukan untuk menyediakan konten teknikal untuk proses perancangan.
  + Manager *Information Security* untuk mengamati perencanaan keamanan dari proyek dan menyediakan informasi tentang ancaman, kelemahan, serangan, dan kebutuhan *recovery* yang dibutuhkan dalam proses perencanaan.
* Perwakilan dari tim bawahan: Tim yang bukan dari tim inti CPMT mempunyai fungsi penting yang merupakan komponen dari seluruh usaha perencanaan kemungkinan. Tim ini berbeda-beda karena fungsi individualnya sangat beda dan mungkin diaktifkan di waktu yang berbeda, atau mereka dapat aktif secara bersamaan. Tim bawahan termasuk tim-tim berikut ini:
  + *Incident Response Team*: mengatur dan menjalankan rencana *Incident* *Response* dengan mendeteksi, evaluasi, dan menanggapi kejadian.
  + *Disaster Recovery Team*: mengatur dan menjalankan rencana *Disaster* *Recovery* dengan mendeteksi, evaluasi, dan menanggapi bencana, serta membangun kembali operasi pada lokasi bisnis utama.
  + *Business Continuity Team:* mengatur dan menjalankan rencana *Business Continuity* dengan membuat dan menjalankan operasi di lokasi lain ketika terjadi bencana.
  + *Crisis Management Team:* mengatur dan meringankan dampak kehilangan pribadi dan mengurangi stress perusahaan dengen usaha meminimalisasi kehilangan jiwa, akuntabilitas personel yang cepat dan akurat, dan notifikasi personel utama yang cepat dan akurat melalui daftar peringatan.

1. **Types of threats in information security**

Mencermati kuot dari Sun Tzu “Kenalilah musuhmu,” anda dapat mulai mengkonversi daftar ancaman dari bab 1 menjadi daftar serangan yang dapat digunakan untuk membuat profil serangan.

Proses ini diawali dengan melihat masing-masing kategori ancaman dan berdasarkan informasi tambahan dari sumber-sumber tersedia termasuk pers perdagangan, pengalaman profesional, target sumber daya Web dan laporan akademik, jika hal ini memungkinkan untuk dibuatkan daftar yang paling mungkin terjadi serangan antar tiap kategori ancaman. Contohnya, dalam kategori serangan perangkat lunak yang disengaja, hal ini mungkin bisa datang dari serangan seperti:

• E-mail virus dan worm

• E-mail berdasarkan engineering sosial

• Web yang disusupi skrip berbahaya

• Denial-of-service attacks pada server

• Spyware dan adware berbahaya

Daftar serangan yang lebih spesifik umumnya cukup besar, dan dibutuhkan tingkatan pengkategorian dan mungkin ringkasan jika diperlukan.

Sangat mungkin jika kategori tersebut dapat saling tumpang tindih terhadap serangan jamak dan kebalikannya. Contohnya, hacker yang mengakses e-mail server, mencuri nomor kartu kredit dan kemudian mencoba mengirimkan blackmail ke organisasi, mungkin membutuhkan percobaan serangan yang banyak. Serangan pertama adalah untuk mengekspoitasi network atau server untuk mendapat akses sebagai aksi spionasi atau pelanggaran yang disengaja. Hacker kemudian melakukan aksi mencuri yang disengaja dengan mengambil nomor kartu kredit dan kemudian hacker melakukan aksi pemerasan informasi yagn disengaja ketika percobaan blackmail dilakukan. Setiap komponen tersebut membutuhkan masukan yang berbeda pada daftar serangan, karena masing-masing memiliki skenario serangan yang berbeda, yang dijelaskan pada seksi berikutnya.

1. **Attack success scenario development**

Berikut adalah daftar serangan yang mungkin akan terjadi.

|  |  |
| --- | --- |
| **Ancaman** | **Serangan** |
| Aksi memasuki tanpa ijin | Akses logikal ke sistem organisasi tanpa ijin  Akses fisikal ke fasilitas organisasi |
| Aksi memeras informasi | Pemerasan organisasi untuk informasi aset |
| Aksi sabotase atau vandalism | Sengaja memodifikasi atau menghancurkan aset informasi organisasi tanpa ijin  Kerusakan fisik atau hancurnya aset organisasi |
| Aksi pencurian | Mengambil aset organisasi secara ilegal |
| Aksi serangan perangkat lunak | *E-mail virus* dan *worm*, *virus* dan *worm* lainnya  *Plushing*  *Web* yang disusupi skrip berbahaya  *Denial-of-service attacks* pada *server*  *Spyware* dan *adware* berbahaya |
| Kejadian alam | Kebakaran  Banjir  Gempa bumi  Pergeseran tanah  Angin kencang atau tornado  Angin puyuh atau hurricane  Tsunami  *Electrostatic* *discharge* (ESD)  Kontaminasi debu  Paparan solar  Radiasi elektromagnetik  Kelembapan |
| Deviasi kualitas servis dari penyedia jasa servis | Koneksi jaringan putus karena putusnya kabel  Koneksi jaringan putus karen servis bermasalah  Mati listrik |
| Kegagalan perangkat keras atau eror | Kerusakan perangkat karena kesalahan manufaktur atau desain atau cacat produksi |
| Kegagalan perangkat lunak atau eror | Kegagalan perangkat lunak karena kesalahan pembuatan atau desain atau cacat seperti bug atau masalah code  Lubang atau jebakan pintu perangkat lunak yang tidak diketahui |
| Keburukan teknologi | Penggunakan perangkat atau teknologi lama atau kuno  Gagal untuk menjaga, mengantisipasi perangkat penyimpanan |

1. **Potential damage assessment**

Seperti yang sudah dilakukan dalam proses identifikasi resiko terhadap ancaman, serangan yang dihadapi organisasi harus diproritaskan berdasarkan kriteria yang dipilih oleh komite CP. Masukkan dari departemen IT dan kantor CISO sangat penting dalam menciptakan kategori dan bobot dalam serangan elektronik tradisional, tapi masukkan dari agensi lain seperti finansial dan perusahaan asuransi mungkin dibutuhkan untuk dapat mengkalkulasi probabilitas dan kerusakan secara akurat dari masalah kerusakan alam tradisional. Perusahaan asuransi secara umum mempunyai pengalaman yang besar dalam menentukan probabilitas dan kemungkinan rusaknya dari angin tornado, banjir, gempa bumi, dan lainnya sebagai basis dalam premi asuransi.

Catatan bahwa pengukuran dan penentuan prioritas ini, organisasi sering kali menggunakan skala untuk memberikan nilai pada kedua bobot dan untuk nilai serangan. Hal ini memberikan kesamaan, perbandingan yang mirip antar hal, dan menghindari untuk terlalu fokus pada nilai finansial. Beberapa hal yang perlu diperhatikan dalam menciptakan analisis bobot yang mana sebuah organisasi mungkin akan menyeleksi, berikut ini:

* Kemungkinan akan terjadinya: Tentu saja serangan yang sering terjadi lebih jarang akan mendapat perhatian kurang dibanding dengan serangan yang lebih sering terjadi. Tergantung dari negara manakan organisasi tersebut berada, Serangan petir mungkin saja lebih sering terjadi daripada gempa bumi. Serangan seperti akses yang tidak memiliki ijin atau autentikasi secara logikal (masuk ke dalam sistem) akan lebih sering terjadi daripada pencurian secara fisik.
* Kemungkinan berhasilnya: Walaupun serangan sering terjadi, jika hal tersebut memiliki kemungkinan berhasil yang rendah, maka tidak akan dilihat secara serius dibanding dengan serangan yang memiliki tingkat keberhasilan tinggi. Tingkat kesiapan organsisasi secara langsung mempengaruhi kemungkinan berhasilnya serangan. Serangan dari hacker pada server Web dalam mencoba mencuri informasi kartu kredit mungkin bisa saja tidak berhasi jika organsisasi melakukan proxy pada database server Web mereka yang asli dari intranet di dalam firewall.
* Besarnya kerusakan: Jika berhasil, seberapa besar kerusakan yang dialami oleh organisasi? Kategori ini mempunyai subkategori yang mungkin membutuhkan konsiderasi. Kerusakan bisa dalam nilai yang berbeda, bergantung apakah anda melihatnya hanya secara kerusakan finansial, kerusakan fisik, kerusakan terhadap citra perusahaan, kerusakan terhadapat pangsa pasar organisasi, dan sebagainya. Akibatnya, organisasi bisa saja menggunakan kategori ini sebagai basis dalam banyaknya sumber masuk ke dalam tabel bobot.
* Ongkos untuk mengembalikan: Berhubungan dengan kategori sebelumnya adalah ongkos organisasi untuk mengembalikan ke kondisi normal operasional setelah serangan. Kategori ini memberikan gambar pada kasus akhir skenario serangan final, di mana organisasi harus menentukan ongkos total dari kasus terbaik, kasus terburuk, dan tentunya kasus serangan. Dalam analisis ini, tabel meggunakan peringkat, dibanding menggunakan angka sesungguhnya, untuk menentukan ongkos dari segi finansial, waktu, dan sumber daya manusia yang dibutuhkan untuk mengembalikan operasional bisnis. Beberapa organisasi mungkin memilih untuk memisahkan pengelolaan waktu dengan pengelolaan finansial, karena mereka mungkin memiliki dana untuk operasi pengembalian secara cepat, namun akuisisi untuk menggantikan teknologi atau fasilitas mungkin dapat membutuhkan waktu yang cukup lama.
* Efek keberhasilan serangan di mata publik: Walaupun ongkos untuk mengembalikan dari serangan pencurian kartu kredit termasuk rendah, contohnya, namun efeknya terhadap publik akan sangat berdampak tinggi, tentunya jika hal ini tidak ditangani dengan bail.

**SIMPULAN**

Hal utama dalam IT Risk Management adalah:

1. Untuk memulai proses dari perencanaan kemungkinan yang akan terjadi atau membangun contingency plan, pertama-tama sebuah organisasi atau perusahaan harus menetapkan unit yang akan bertanggung jawab terhadap kebijakan dan rencana yang suatu saat akan muncul tersebut.
2. Perlu dibuat daftar kategori ancaman dan mencari informasi tambahan dari sumber-sumber tersedia termasuk media, industry dan dari pengalaman profesional
3. Dalam proses assessment perlu diperhatikan: Kemungkinan akan terjadinya, Kemungkinan berhasilnya, Besarnya kerusakan, dan Efek keberhasilan serangan di mata public.

**DAFTAR PUSTAKA**

1. Whitman, M.E., Mattoro, H.J. (2013). ***Principles of Incident Response and Disaster Recovery***.