**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

**KDS – Name SME**

**Session 10**

**Incident Response Reaction, Recovery and Maintenance**

Perlindungan untuk kemungkinan perencanaan semua dilakukan oleh sebuah organisasi/perusahaan untuk mempersiapkan hal-hal yang tidak terduga. Penanganan Insiden (Incident Response/IR) adalah salah satu kemungkinan perencanaan yang berfokus pada mendeteksi atau mencoba untuk menganalisis dan mengevaluasi tingkat ancaman dari hal-hal yang tidak terduga. Bila memungkinkan, proses IR seharusnya memuat dan menyelesaikan insiden tersebut berdasarkan rencana IR. Ketika insiden yang tidak dapat diselesaikan muncul, element lain dari kemungkinan proses perencanaan diaktifkan, dengan menggunakan proses eskalasi yang didokumentasikan seperti yang tercantum dalam seluruh rencana. Proses penanganan insiden (IR process) dibuat dalam beberapa tahap :

1. Persiapan (Preparation)
2. Mendeteksi dan menganalisis (Detection and analysis)
3. Penahanan (containment)
4. Pemberantasan (eradication)
5. Pemulihan atau pembaruan (recovery)
6. Kegiatan pasca insiden (Postincident activity)

Karena proses penanganan insiden begitu kompleks, pada dokumen ini hanya akan membahas mengenai tahap persiapan awal dari penanganan insiden dengan tujuan agar suatu organisasi/perusahaan dapat membuat suatu perencanaan penanganan insiden yang dapat dilakukan secara efektif untuk menangani suatu insiden atau masalah.

1. **Preparing for incident response**

Setelah CPMT (Contingency Planning Management Team) menyelesaikan setiap komponen dari analisis dampak bisnis (BIA), kita dapat memulai untuk mentransfer informasi yang diambil dari suatu organisasi/perusahaan ke berbagai subordinat komite. Untuk membantu perencanaan subordinat, setiap komite penanganan insiden, komite pemulihan bencana, dan komite kelanjutan bisnis mendapatkan informasi mengenai serangan yang akan mereka hadapi, prioritas dari serangan, dan skenario penyelesaian serangan. Setelah anggota komite mempunyai informasi ini, mereka mulai dengan menuliskan rencana. Pada pembuatan dokumen incident response plan atau penanganan insiden, langkah langkah nya terbagi menjadi beberapa tingkatan, yaitu :

1. Membentuk komite perencanaan penanganan insiden

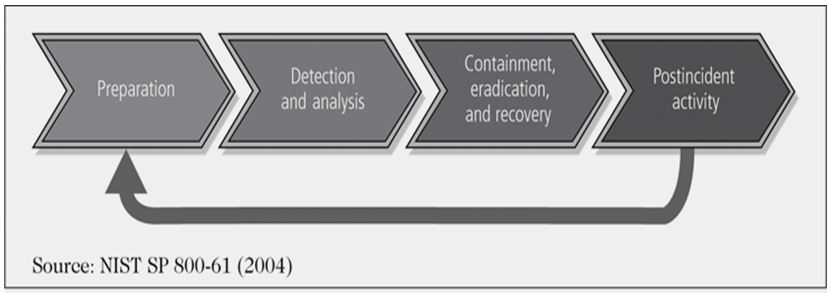
2. Membuat kebijakan penanganan insiden

3. Mengatur SIRT

4. Membuat perencanaan penanganan insiden

5. Membuat prosedur penanganan insiden

Pada dasarnya langkah langkah ini juga sesuai dengan NIST (National Institute of Standards & Technology) dan CERT (Computer Emergency Response Team). Untuk memperoleh gambaran dari cara perencanaan penanganan insiden yang ditunjukkan pada organisasi/perusahaan lain, dua contoh dari IR planning life cycle ditunjukkan pada gambar dibawah ini. Gambar tersebut menunjukkan bagaimana U.S. National Institute of Standards and Technology (NIST) mendefinisikan proses perencanaan penanganan insiden. Seperti yang dapat dilihat dari gambar, dokumen ini mengikuti pendekatan NIST secara lebih dekat. Gambar tersebut juga menyediakan perspektif yang lebih luas, menunjukkan bagaimana pendekatan Computer Emergency Response Team Coordinating Center (CERT/CC) pada perencanaan penanganan insiden sesuai dengan model penanganan insiden secara keseluruhan.



1. **Security incident response team**

Pengaturan proses perencanaan penanganan insiden dimulai dengan menentukan orang-orang (staf) untuk pembentukan komite perencanaan penanganan insiden. Banyak upaya pengorganisasian awal dilakukan oleh tim CP, tetapi tim penanganan insiden perlu ditata sebagai entitas yang terpisah, dan proses dimulai dengan mengidentifikasi dan melibatkan kumpulan pemegang kepentingan yang berarti mewakili individu di setiap departemen atau operasi pada organisasi.

Pemegang kepentingan ini digunakan untuk mengumpulkan informasi penting tentang peran dan tanggung jawab dari tim SIRT. Tipe-tipe pemegang kepentingan pada umumnya adalah:

1. Communities of interest :

* General management : kelompok ini perlu memahami apa itu SIRT dan apa yang dilakukannya. Kelompok ini juga perlu melakukan pra-otorisasi interaksi antara SIRT dan fungsi bisnis utama, dan tindakan tertentu yang diperlukan untuk menangkap penyebaran dan dampak dari insiden.
* IT Management : kelompok ini perlu untuk mengerti detail permintaan SIRT yang akan ditempatkan pada IT, dan akses dan sumber daya apa yang mereka butuhkan untuk merespon insiden secara baik dan berhasil. Kelompok ini butuh untuk menyetujui aksi SIRT ketika beberapa aksi berdampak pada sistem, fungsi network, dan koneksi yang sedang berjalan dalam suatu organisasi/perusahaan.
* InfoSec Management : kelompok ini perlu mengerti kebutuhan sumber daya yang dibutuhkan SIRT atau kemudahan akses yang mereka butuhkan dalam waktu yang singkat.

1. Organizational Departments, seperti :

* Departemen hukum (The Legal Department) butuh untuk mereview prosedur SIRT dan mengerti langkah-langkah yang akan dilakukan SIRT untuk memastikan mereka berada dalam pedoman hukum dan etika dari kota, negara, dan yurisdiksi federal Anda. Departemen Hukum dapat memberikan panduan pada pengembangan kontrak dan perjanjian tingkat layanan untuk layanan tambahan dan berulang, perjanjian yang tidak diungkapkan untuk mitra bisnis dan asosiasi non-karyawan lainnya, dan dalam meninjau kebijakan dan dokumen rencana untuk masalah pertanggungjawaban.
* Departemen HR (The Human Resources Department) membantu InfoSec memperoleh personil untuk melengkapi tim SIRT. Individu dengan pengalaman penanganan insiden mungkin saat ini tidak dipekerjakan oleh organisasi. Pengembangan deksripsi pekerjaan dan wawancara dan akhirnya memperkerjakan kandidat akan menguntungkan dari koordinator dekat dengan HR.
* Departemen PR (The Public Relations Department) perlu diberitahu tentang informasi apa yang dapat dan harus diungkapkan kepada publik jika dan ketika suatu insiden terjadi. Pemberitahuan publik yang telah ditetapkan dapat disusun dan ditinjau oleh Public Relation untuk memastikan jumlah yang tepat dari informasi yang tersedia ke lembaga yang tepat, penegak hukum, dan media ketika diperlukan.
* Bergantung pada pengaturan dari suatu organisasi/perusahaan, beberapa kelompok dengan keamanan informasi yang tumpang tindih akan membutuhkan konsultasi, misalnya :
* Physical security
* Audit dan manajemen resiko
* Asuransi

1. Other interest groups, seperti :

* Pengguna akhir umum perlu mengetahui apa yang terjadi ketika SIRT dilakukan dan bagaimana menanggapi pertolongan terbaik dalam pengembangan dan pengujian prosedur dan kebijakan. Pemegang kepentingan atau saham yang paling familiar dengan fungsi bisnis, dapat memberikan wawasan tambahan ke area-area tersebut.
* Pemegang kepentingan atau pemegang saham lain, termasuk rekan bisnis utama, kontraktor, agensi karyawan sementara, dan dalam beberapa kasus konsultan.
* Department PR perlu memberitahu informasi yang dapat dan harus diungkap ke public ketika insiden terjadi, informasi public dapat di susun dan di review oleh PR untuk memastikan informasi di berikan ke lembaga penegak hukum dan media sesuai kebutuhan.

Catatan: Pada beberapa struktur perusahaan, ada tumpang tindih informasi keamanan yang perlu di konsultasikan, termasuk :

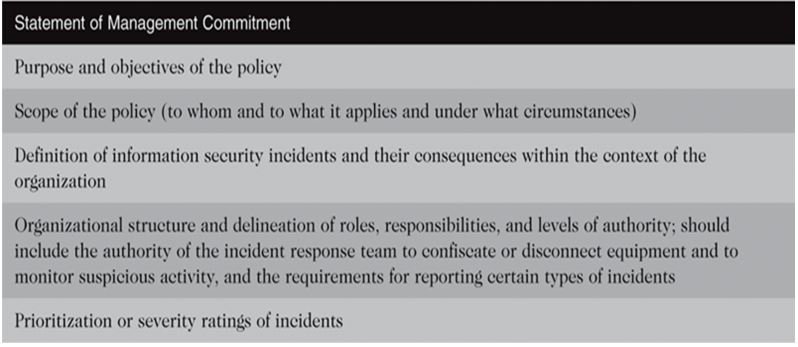
* 1. Phisical security (keamanan fisik)
  2. Auditing and risk management (audit dan resiko managemen)
  3. Insurances (Asuransi / Jaminan )

1. **Incident response planning**

Hal utama yang harus dilakukan oleh komite perencanaan IT (CPMT) adalah harus membuat kebijakan respon insiden (incident response policy). Komite perencanaan membentuk tim SIRT, perwakilan SIRT bergabung dengan komite IR merencanakan pengembangan kebijakan untuk menentukan operasi dari tim dan mengartikan respon organisasi untuk berbagai jenis insiden, serta meyarankan ke end user untuk ikut berkontribusi pada organisasi dengan efektif, dengan memberikan kontribusi terhadap masalah.

Kebijakan (policy) untuk insiden response plan ini mirip dengan struktur kebijakan lain yang digunakan oleh organisasi. Sama seperti perusahaan kebijakan keamanan informasi mendefinisikan peran dan tanggung jawab untuk keamanan informasi untuk seluruh perusahaan, kebijakan penanganan insiden mendefinisikan peran dan tanggung jawab untuk penanganan insiden untuk SIRT dan lain-lain yang dapat dijabarkan dalam aktivasi. Tabel dibawah memberikan gambaran tentang struktur kebijakan IR.

Kebijakan IR, seperti kebijakan lain yang tertulis, harus mendapatkan dukungan penuh dari top manajemen dan dipahami dengan jelas oleh semua pihak yang terkena dampak. Hal itu sangat penting untuk mendapatkan dukungan dari komunitas-komunitas yang akan diperlukan untuk mengevaluasi bisnis atau membuat perubahan pada infrastruktur teknologi informasi mereka. misalnya, jika SIRT menentukan satu-satunya cara untuk menghentikan serangan denial-of-service yaitu serangan besar-besaran adalah untuk memutuskan hubungan organisasi ke internet, mereka harus memiliki dokumen tersebut dalam lemari arsip yang sesuai dengan pra-otorisasi tindakan tersebut. ini mencegah setiap persepsi anggota tim SIRT dan organisasi dari kesalahpahaman. Seperti misi perusahaan, kebijakan tidak bisa ditegakkan apabila tidak didukung oleh manajemen senior.

Contoh isi dari kebijakan (policy) dari incident responsediambil dari Whitman, M.E., Mattoro, H.J. (2013). ***Principles of Incident Response and Disaster Recovery***.

Setiap anggota tim, baik teknis, manajemen, atau administrasi, harus dapat dengan mudah memahami kebijakan yang diberikan. Hindari jargon yang tidak perlu, jangan ambigu, dan menggunakan kalimat yang sangat singkat. Jika mungkin (sesuai dengan pembatasan pengungkapan Anda), meminta seseorang yang tidak tercantum dalam keamanan atau TI untuk membaca kebijakan Anda. Jika ia tidak dapat memahaminya, tulis ulang kebijakan tersebut.

Kebijakan yang baik adalah kebijakan yang singkat. Sebuah kebijakan yang panjang adalah salah satu kebijakan yang buruk (atau menggunakan terlalu banyak kata-kata) atau yang sebenarnya mencakup banyak prosedur. Sayangnya, kebijakan keamanan dalam prakteknya sering cenderung tidak singkat, membingungkan pencampuran aspek manajemen (kebijakan) dengan aspek operasional (prosedur), sehingga campuran yang tak benar-benar peduli untuk. Upayakan untuk menghindari kondisi ini. Hindari pernyataan yang terdengar bagus tapi tidak berguna karena mereka terbuka untuk interpretasi, seperti "state-of-art-keamanan akan disediakan." Laporan Akal sehat seperti "memperlakukan pelanggan Anda dengan hormat"

**SIMPULAN**

Hal utama dalam IT Risk Management adalah:

1. Proses pembuatan dokumen incident response plan (penanganan insiden - IR process) dibuat dalam beberapa tahap, yaitu:
   1. Persiapan (Preparation)
   2. Mendeteksi dan menganalisis (Detection and analysis)
   3. Penahanan (containment)
   4. Pemberantasan (eradication)
   5. Pemulihan atau pembaruan (recovery)
   6. Kegiatan pasca insiden (Postincident activity)
2. Anggota dari Incident Response harus mewakili setiap department di perusahaan
3. Hal pertama yang harus dilakukan oleh komite perencanaan IT (CPMT) adalah harus membuat kebijakan respon insiden (incident response policy).

**DAFTAR PUSTAKA**

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