APTIKOM
ASOSIASI PERGURUAN TINGGI INFORMATIKA DAN KOMPUTER

MODUL PJJ

Mata Ajar

MANAJEMEN KEAMANAN INFORMASI DAN INTERNET

Topik Bahasan

PROSEDUR PENANGANAN INSIDEN KEMANAN DUNIA SIBER

Versi

2013/1.0

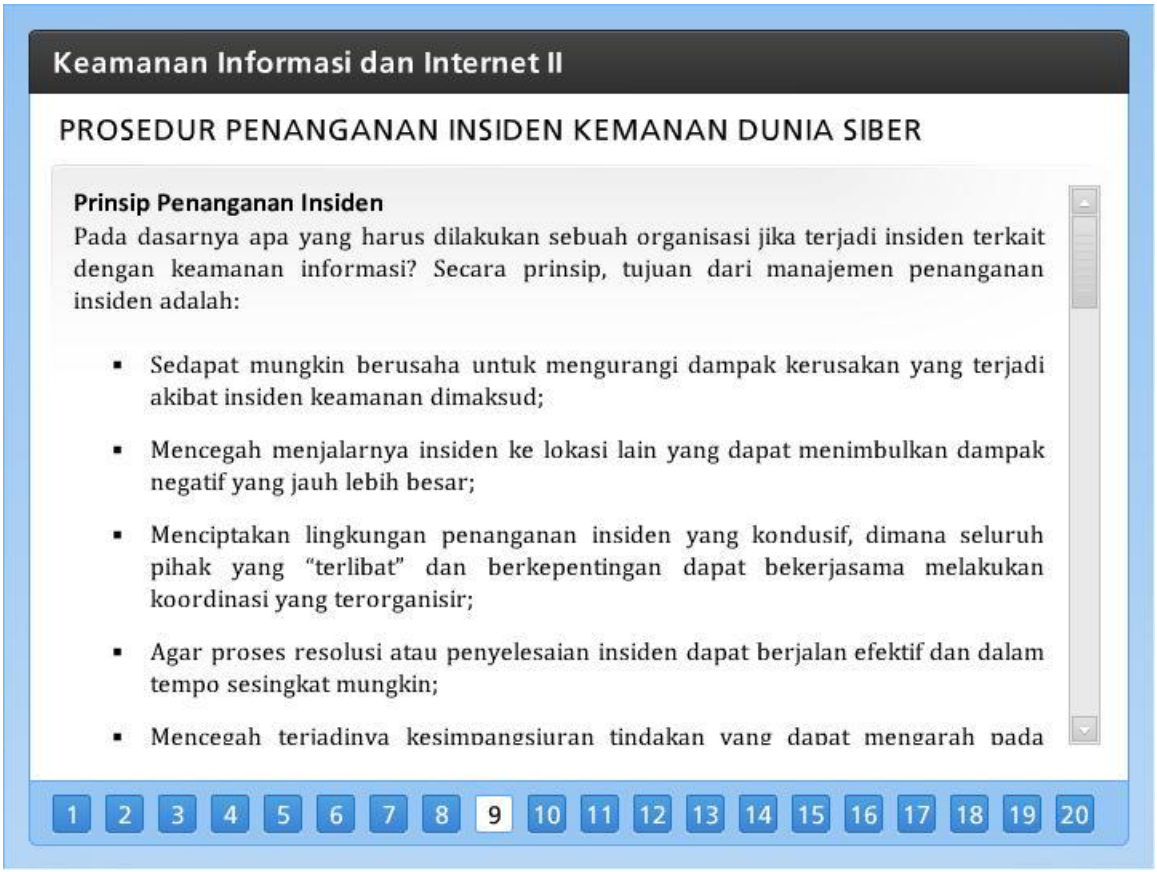
Nama File

MKIDI-8A-ProsedurPenanganan.pdf

Referensi Pembelajaran

8-A

PROSEDUR PENANGANAN INSIDEN KEMANAN DUNIA SIBER



Prinsip Penanganan Insiden

Pada dasarnya apa yang harus dilakukan sebuah organisasi jika terjadi insiden terkait dengan keamanan informasi? Secara prinsip, tujuan dari manajemen penanganan insiden adalah:

- Sedapat mungkin berusaha untuk mengurangi dampak kerusakan yang terjadi akibat insiden keamanan dimaksud;
- Mencegah menjalarnya insiden ke lokasi lain yang dapat menimbulkan dampak negatif yang jauh lebih besar;
- Menciptakan lingkungan penanganan insiden yang kondusif, dimana seluruh pihak yang "terlibat" dan berkepentingan dapat bekerjasama melakukan koordinasi yang terorganisir;
- Agar proses resolusi atau penyelesaian insiden dapat berjalan efektif dan dalam tempo sesingkat mungkin;
- Mencegah terjadinya kesimpangsiuran tindakan yang dapat mengarah pada dampak negatif yang lebih besar lagi; dan

- Memperkaya referensi jenis insiden serta prosedur penanganannya sehingga dapat dipergunakan di lain kesempatan pada peristiwa insiden yang sama oleh berbagai kalangan terkait.

Dalam prakteknya, mendefinisikan dan menjalankan mekanisme "incident handling" merupakan tantangan bagi organisasi yang perduli akan pentingnya mengurangi dampak resiko dari peristiwa yang tidak diinginkan ini.

Kerangka Dasar Fungsi Penanganan Insiden

CERT/CC melalui publikasinya "Handbook for CSIRTs" menggambarkan kerangka fungsi penanganan insiden yang terdiri dari sejumlah entitas atau komponen seperti yang diperlihatkan dalam gambar berikut.

Triage Function

"Triage" merupakan fungsi yang bertugas menjadi "a single point of contact" atau sebuah entitas/unit yang menjadi pintu gerbang komunikasi antara organisasi dengan pihak luar atau eksternal. Seluruh informasi yang berasal dari luar menuju dalam maupun dari dalam menuju luar harus melalui unit "pintu gerbang" ini - karena di sinilah pihak yang akan menerima, menyusun, mengorganisasikan, memprioritasikan, dan menyebarluaskan data atau informasi apa pun kepada pihak yang berkepentingan. Fungsi "triage" ini sangatlah penting agar koordinasi dalam situasi kritis karena insiden berjalan secara lancar dan efektif (baca: satu pintu). Dengan kata lain, laporan adanya insiden baik yang diterima secara lisan maupun melalui sensor teknologi, pertama kali akan masuk melalui fungsi "triage" ini.

Handling Function

"Handling" merupakan fungsi pendukung yang bertugas untuk mendalami serta mengkaji berbagai insiden, ancaman, atau serangan terhadap keamanan informasi yang terjadi. Fungsi ini memiliki tanggung jawab utama dalam meneliti mengenai laporan insiden yang diterima, mengumpulkan bukti-bukti terkait dengan insiden yang ada, menganalisa penyebab dan dampak yang ditimbulkan, mencari tahu siapa saja pemangku kepentingan yang peru dihubungi, melakukan komunikasi dengan pihak-pihak yang terkait dengan penanganan insiden, dan memastikan terjadinya usaha untuk mengatasi insiden.

Announcement Function

"Announcement" merupakan fungsi yang bertugas mempersiapkan beragam informasi yang akan disampaikan ke seluruh tipe konstituen atau pemangku kepentingan yang terkait langsung maupun tidak langsung dengan insiden yang terjadi. Tujuan disebarkannya informasi kepada masing-masing pihak adalah agar seluruh pemangku kepentingan segera mengambil langkah-langkah yang penting untuk mengatasi insiden dan mengurangi dampak negatif yang ditimbulkannya. Aktivitas pemberitahuan ini merupakan hal yang sangat penting untuk dilakukan agar seluruh pihak yang berkepentingan dapat saling berpartisipasi dan berkoordinasi secara efektif sesuai dengan porsi tugas dan tanggung jawabnya masing-masing.

Feedback Function

"Feedback" merupakan fungsi tambahan yang tidak secara langsung berhubungan dengan insiden yang terjadi. Fungsi ini bertanggung jawab terhadap berbagai aktivitas rutin yang menjembatani organisasi dengan pihak eksternal seperti media, lembaga swadaya masyarakat, institusi publik, dan organisasi lainnya dalam hal diseminasi informasi terkait dengan keamanan informasi. Termasuk di dalamnya jika ada permintaan khusus untuk wawancara atau dengar pendapat atau permohonan

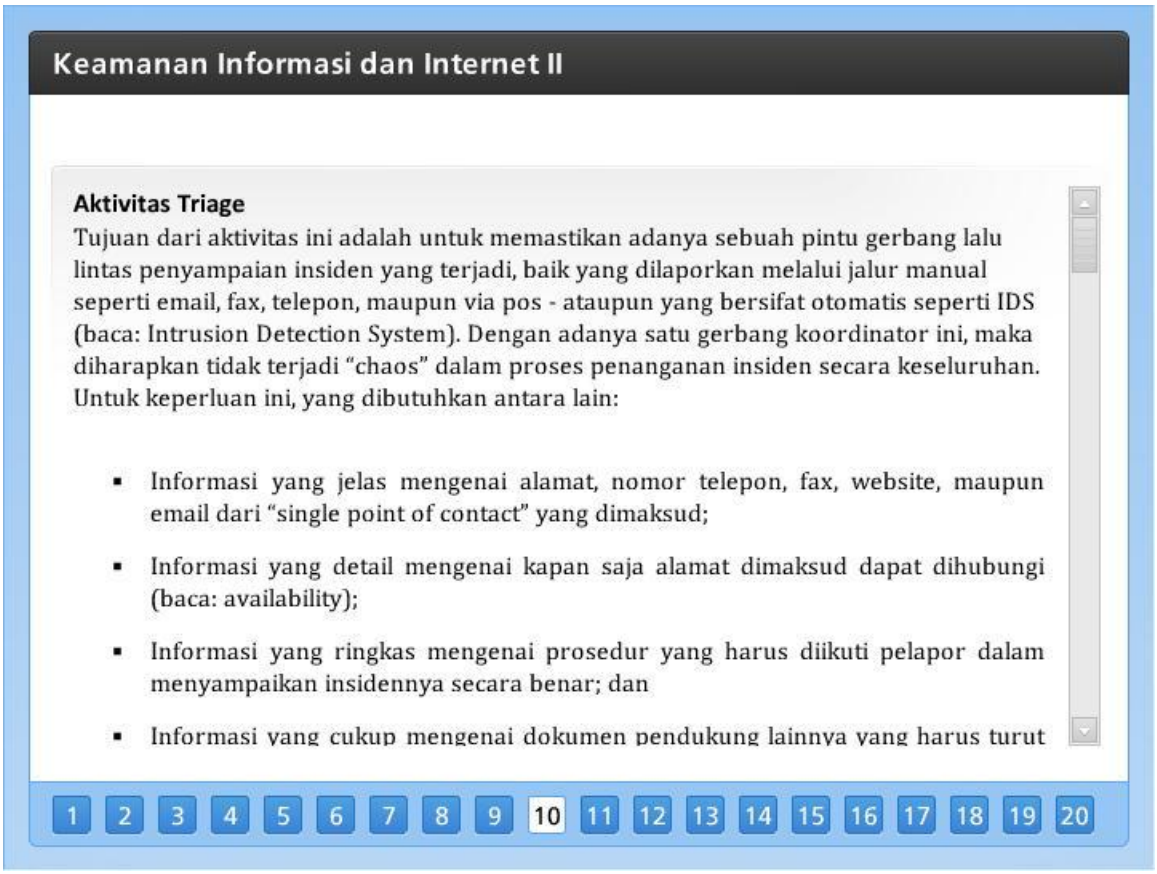
rekomendasi terkait dengan berbagai fenomena keamanan informasi yang terjadi di dalam masyarakat.

Siklus dan Prosedur Baku Penanganan Insiden

Berdasarkan kerangka dasar penanganan insiden yang telah dibahas sebelumnya, maka dapat disusun tahap-tahap atau prosedur atau siklus aktivitas penanganan insiden dalam sebuah organisasi seperti yang direkomendasikan oleh CERT/CC berikut ini.

- Setiap harinya, secara berkala dan rutin unit "Triage" akan mendapatkan sinyal ada atau tidak adanya peristiwa yang mencurigakan (misalnya: penyusupan, insiden, serangan, dan lain sebagainya) melalui berbagai kanal, seperti: email, IDS (Intrusion Detection System), telepon, dan lain sebagainya.
- Sesuai dengan standar dan kesepakatan yang ada, berdasarkan masukan aktivitas rutin tersebut, organisasi melalui fungsi unit "Announcement" dan "Feedback" akan memberikan informasi dan laporan kepada pihak-pihak yang berkepentingan dengan keamanan informasi yang dimaksud - misalnya ISP, internet exchange point, para pengguna sistem, manajemen dan pemilik, dan lain sebagainya.
- Setelah "Triage" menyatakan bahwa memang telah terjadi "insiden" yang harus ditangani, maka fungsi "Handling" mulai menjalankan peranannya, yang secara prinsip dibagi menjadi empat, yaitu: (i) analisa mengenai karakteristik insiden; (ii) mencari informasi dari pihak lain terkait dengan insiden yang ada; (iii) kerja teknis mitigasi resiko insiden; dan (iv) koordinasi untuk implementasi penanganan insiden.

Agar mendapatkan gambaran yang jelas mengenai apa yang dilakukan oleh masing-masing tahap, berikut ini akan dijelaskan secara lebih rinci mengenai aktivitas yang dilakukan pada setiap tahap proseduralnya.



Aktivitas Triage

Tujuan dari aktivitas ini adalah untuk memastikan adanya sebuah pintu gerbang lalu lintas penyampaian insiden yang terjadi, baik yang dilaporkan melalui jalur manual seperti email, fax, telepon, maupun via pos - ataupun yang bersifat otomatis seperti IDS (baca: Intrusion Detection System). Dengan adanya satu gerbang koordinator ini, maka diharapkan tidak terjadi "chaos" dalam proses penanganan insiden secara keseluruhan. Untuk keperluan ini, yang dibutuhkan antara lain:

- Informasi yang jelas mengenai alamat, nomor telepon, fax, website, maupun email dari "single point of contact" yang dimaksud;
- Informasi yang detail mengenai kapan saja alamat dimaksud dapat dihubungi (baca: availability);
- Informasi yang ringkas mengenai prosedur yang harus diikuti pelapor dalam menyampaikan insidennya secara benar; dan
- Informasi yang cukup mengenai dokumen pendukung lainnya yang harus turut disampaikan ketika laporan disampaikan.

Biasanya proses pelaporan insiden ini dilakukan secara semi-otomatis, dalam arti kata ada sebagian yang dilakukan secara manual dan sejumlah hal lainnya dengan memanfaatkan teknologi. Contohnya adalah sang korban melaporkan dengan

menggunakan telepon genggam dimana sang penerima laporan menggunakan aplikasi tertentu untuk mencatatnya.

Mengingat bahwa dalam satu hari kerap dilaporkan lebih dari satu insiden, maka ada baiknya setiap laporan kejadian diberikan nomor lacak atau "tracking number" yang unik, agar dapat menjadi kode referensi yang efektif. Hal ini menjadi semakin terlihat manfaatnya jika insiden yang terjadi melibatkan pihak internasional (baca: lintas negara).

Hal lain yang tidak kalah pentingnya - apakah dilakukan secara manual maupun berbasis aplikasi - adalah membuat formulir pengaduan dan laporan yang akan dipergunakan untuk merekam interaksi, dimana di dalamnya terdapat informasi seperti: (i) data lengkap pelapor; (ii) alamat jaringan yang terlibat atau ingin dilaporkan; (iii) karakteristik dari insiden; (iv) dukungan data/informasi terkait dengan insiden; (v) nomor lacak yang berhubungan dengan insiden; dan lain-lain.
Setelah itu barulah dilakukan apa yang dinamakan sebagai "pre-registration of contact information" yaitu penentuan media dan kanal komunikasi selama aktivitas penanganan insiden berlangsung, terutama berkaitan dengan: (i) pihak yang diserahkan tanggung jawab dan dapat dipercaya untuk berkoordinasi (baca: Person In Charge); (ii) perjanjian kerahasiaan data dan informasi (baca: Non Disclosure Agreement); dan (iii) kunci publik dan tanda tangan digital untuk kebutuhan verifikasi.

Aktivitas Handling

Tujuan dari aktivitas ini adalah untuk mempersiapkan "response" atau langkah-langkah efektif yang perlu dipersiapkan untuk menangani insiden, dimana paling tidak harus ada sejumlah fungsi, yaitu:

- Reporting Point: mempelajari detail pengaduan dan laporan mengenai insiden yang terjadi untuk selanjutnya melakukan kajian mendalam terkait dengan berbagai hal seperti: analisa dampak, pihak yang perlu diperingatkan, asal atau sumber insiden, dan lain sebagainya;
- Analysis: melakukan kajian teknis secara mendalam mengenai karakteristik insiden, seperti: menganalisa "log file", mengidentifikasikan domain korban dan penyerang, mencari referensi teknis, menemukan penyebab dan solusi pemecahan insiden, mempersiapkan kebutuhan memperbaiki sistem, menunjuk pihak yang akan menerapkan prosedur perbaikan, dan memperbaiki sistem yang diserang; dan
- Notification: memberikan notifikasi atau berita kepada semua pihak yang terlibat langsung maupun tidak langsung dengan insiden untuk mengambil langkah-langkah yang dianggap perlu agar proses penanganan insiden dapat berlangsung dengan baik.

Nampak terlihat jelas dalam aktivitas ini sejumlah kegiatan teknis yang membutuhkan sumber daya tidak sedikit. Pertama, sumber daya manusia yang memiliki kompetensi dan keahlian khusus dalam hal-hal semacam: malware analysis, log files analysis, traffic analysis, incident handling, computer forensics, dan lain sebagainya - haruslah dimiliki oleh organisasi yang bersangkutan. Jika tidak ada, maka ada baiknya dilakukan kerjasama dengan pihak ketiga, seperti perguruan tinggi, konsultan, atau pihak-pihak berkompeten lainnya. Kedua, fasilitas laboratorium teknis yang lumayan lengkap untuk

melakukan berbagai kegiatan kajian forensik dan analisa juga mutlak dibutuhkan keberadaannya. Jika tidak memiliki, maka ada baiknya menjalin kerjasama dengan pihak seperti lembaga riset, laboratorium kepolisian, vendor keamanan informasi, dan lain-lain. Ketiga, adanya referensi dan SOP yang memadai terkait dengan proses penanganan insiden agar berjalan secara efektif dan dapat dipertanggung-jawabkan hasilnya. Untuk yang ketiga ini, telah banyak dokumen yang tersedia secara terbuka untuk dipergunakan bagi pihak-pihak yang berkepentingan.

Aktivitas Announcement

Seperti telah dijelaskan sebelumya, sesuai dengan namanya, aktivitas ini memiliki tujuan utama untuk menyusun dan mengembangkan sejumlah laporan untuk masing-masing pihak terkait dengan insiden. Perlu dicatat, bahwa setiap pihak memerlukan laporan yang berbeda dengan pihak lainnya (baca: tailor-made), karena harus disesuaikan dengan wewenang, peranan, serta tugas dan tanggung jawabnya. Berdasarkan sifat dan karakteristiknya, ada sejumlah tipe berita yang biasa disampaikan:

- Heads-Up: merupakan suatu pesan pendek yang disampaikan terlebih dahulu sambil menunggu informasi detail lebih lanjut. Pesan pendek ini bertujuan untuk memberikan peringatan awal terhadap hal-hal yang mungkin saja akan terjadi dalam waktu dekat. Dengan cara preventif ini, maka diharapkan pihak penerima pesan dapat mempersiapkan dirinya dalam menghadapi insiden yang akan terjadi.
- Alert: merupakan suatu pesan peringatan yang disampaikan karena telah terjadi sebuah serangan atau ditemukannya sejumlah kerawanan pada sistem yang akan segera mempengaruhi pihak yang berkepentingan dalam waktu dekat (baca: critical time). Jika pesan "alarm" ini telah sampai, maka penerima pesan harus segera mengambil langkah-langkah teknis yang diperlukan untuk menghindari atau mengurangi dampak negatif yang disebabkannya.
- Advisory: merupakan pesan rekomendasi atau "nasehat" untuk keperluan jangka menengah atau panjang terhadap pemilik sistem agar dapat menghindari diri dari serangan atau insiden tertentu di kemudian hari, baik melalui langkah-langkah yang bersifat strategis manajerial maupun teknis operasional. Rekomendasi yang diberikan biasanya terkait dengan sejumlah kerawanan sistem yang sewaktu-waktu dapat dieksploitasi oleh pihak-pihak yang tidak berwenang.
- For Your Information: merupakan pesan untuk keperluan jangka menengah ke panjang seperti halnya "Advisory", hanya saja bedanya tidak terlampau berbau teknis. Pesan ini disampaikan untuk menambah keperdulian penerima terhadap fenomena yang belakangan ini terjadi di dalam dunia keamanan informasi. Pesan singkat ini dapat dikonsumsi oleh siapa saja, baik awam maupun praktisi teknologi informasi.
- Guideline: merupakan sebuah petunjuk yang berisi serangkaian langkah-langkah yang harus dilakukan agar sebuah sistem dapat terhindar dari sasaran serangan atau terlindungi dari insiden yang mungkin terjadi. Dengan mengikuti panduan ini, maka nischaya sistem yang dimaksud akan terhindar dari kerusakan pada saat insiden terjadi.
- Technical Procedure: merupakan petunjuk sebagaimana "Guideline", tetapi lebih bernuansa teknis, karena ditujukan bagi mereka yang bekerja di bagian

operasional teknologi untuk melakukan langkah-langkah teknis tertentu terhadap sistem yang ingin dijaga.

Pemilihan pesan mana yang hendak disampaikan tidak saja ditentukan oleh tipe audines atau target penerima pesan, tetapi juga berdasarkan kategori dari kriteria pesan yang ingin disampaikan. Misalnya ada sebuah insiden sederhana yang sebenarnya bukan tanggung jawab unit penanganan insiden - seperti seseorang yang kehilangan "password" dan membuat pengaduan - maka perlu diberikan pesan mengenai kemana seharusnya yang bersangkutan melaporkan diri.

Hal lain yang perlu pula diperhatikan adalah mengenai asas prioritas penanganan insiden. Dengan mempertimbangkan "magnitude" dampak negatif dari insiden yang terjadi, maka dipilihlah jenis pesan yang tepat dan efektif. Semakin tinggi prioritasnya, semakin formal dan resmi pesan yang harus disampaikan.

Metode atau media penyampaian pesan perlu pula dipersiapkan dan diperhatikan dengan sungguh-sungguh, karena sejumlah alasan, seperti: sensitivitas informasi, target penerima pesan, kecepatan pengiriman, alokasi biaya transmisi, dan lain sebagainya.

Aktivitas Feedback

Salah satu hal yang paling sulit untuk dikelola oleh sebuah unit penanganan insiden adalah ekspektasi atau harapan dari publik. Terlepas dari ada atau tidaknya insiden serius terjadi, adalah merupakan suatu kenyataan bahwa banyak sekali pihak yang dalam perjalanannya mengharapkan bantuan dari unit yang bersangkutan. Misalnya adalah diperlukannya sejumlah informasi mengenai serangan tertentu, dibutuhkannya pihak yang bisa membantu sosialisasi keamanan informasi, diinginkannya keterlibatan unit terkait dengan pihak-pihak eksternal lainnya, dipertanyakannya sejumlah hal oleh media, dan lain sebagainya. Untuk menanggapi dan mengelola berbagai permintaan di luar tugas utama ini, diperlukan sebuah aktivitas rutin yang bernama "Feedback". Bahkan terkadang tidak jarang dijumpai permintaan yang terkesan mengada-ngada, karena jauh di luar ruang lingkup unit penanganan insiden, seperti: laporan seseorang yang mengaku lupa akan passwordnya, atau permohonan bantuan untuk memasukkan data kartu kredit pada transaksi e-commerce, permintaan mengecek kebenaran pesan sebuah email, dan lain sebagainya. Namun "response" haruslah diberikan terhadap berbagai jenis permintaan yang ada. Kalau tidak dijawab, publik atau pihak pelapor dapat memberikan asumsi atau persepsi negatif yang beraneka ragam, seperti: tim tidak memiliki niat untuk membantu, tim tidak memiliki kompetensi untuk menolong, tim tidak perduli akan kesulitan seseorang, dan lain sebagainya. Jika hal ini sampai ke media dan disebarkan ke publik, akan menimbulkan keadaan krisis yang tidak diharapkan.