APTIKOM
ASOSIASI PERGURUAN TINGGI INFORMATIKA DAN KOMPUTER

MODUL PJJ

Mata Ajar

MANAJEMEN KEAMANAN INFORMASI DAN INTERNET

Topik Bahasan

CSIRT/CERT: TIM PENGAWAS KEAMANAN INTERNET

Versi

2013/1.0

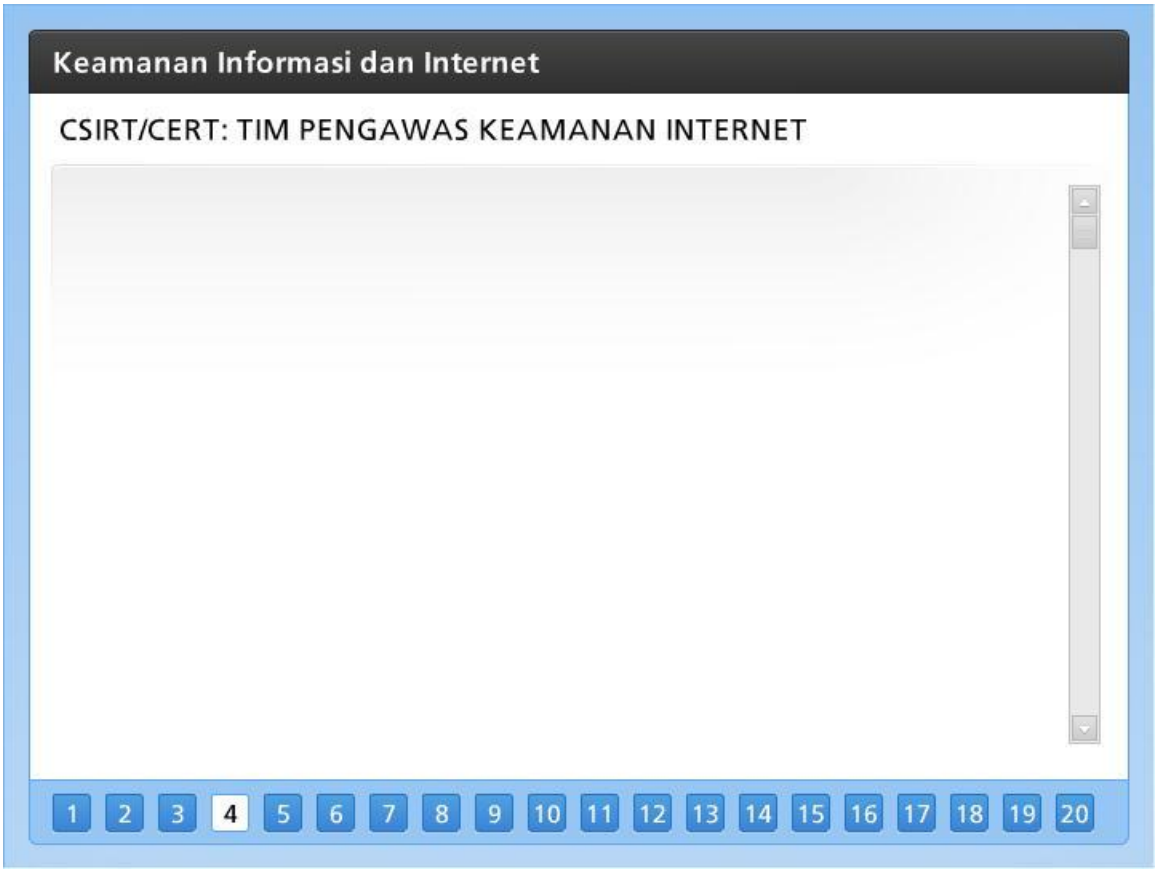
Nama File

MKIDI-1B-TimPengawas.pdf

Referensi Pembelajaran

1-B

CSIRT/CERT: TIM PENGAWAS KEAMANAN INTERNET



Masyarakat Dunia Maya

Tidak banyak orang yang menyangka sebelumnya bahwa internet yang tadinya hanya merupakan jejaring komunikasi antara lembaga riset perguruan tinggi di Amerika Serikat akan menjadi dunia tersendiri tempat berkumpulnya masyarakat dunia untuk melakukan transaksi, interaksi, dan koordinasi secara global seperti sekarang ini. Bahkan keberadaannya telah mampu menciptakan suatu revolusi tersendiri di sektor pemerintahan, industri swasta, komunitas akademik, dan aspek-aspek kehidupan lainnya. Masyarakat internet ini semakin lama semakin meningkat jumlahnya. Bahkan statistik terakhir tahun 2008 memperlihatkan bahwa satu dari lima penduduk dunia telah menjadi pengguna internet dewasa ini. Bukanlah suatu hal yang mustahil bahwa dalam waku yang tidal lama lagi, seluruh penduduk dunia akan menjadi *internet user* yang aktif.

Masalah Internet dan Lembaga Pengaman

Memperhatikan bahwa internet adalah suatu wahana "dari, oleh, dan untuk" masyarakat dunia maya, maka salah satu isu utama yang mengemuka adalah permasalahan keamanan atau

security - baik dalam hal keamanan informasi (konten), infrastruktur, dan interaksi; karena dalam konteks arsitektur internet yang demokratis ini akan meningkatkan faktor resiko terjadinya *incident*keamanan yang tidak diinginkan - baik yang dilakukan secara sengaja maupun tidak. Apalagi sangat banyak hasil riset yang memperlihatkan bahwa dari hari ke hari, jumlah serangan dan potensi ancaman di dunia maya secara kualitas maupun kuantitas meningkat secara signifikan. Karena internet merupakan suatu "rimba tak bertuan", maka masing-masing pihak yang terhubung di dalamnya harus memperhatikan dan menjamin keamanannya masing-masing. Selain melengkapi sistem teknologi informasinya dengan perangkat lunak dan perangkat keras pengamanan (seperti *firewalls*dan *anti virus* misalnya), beberapa institusi besar seperti ABN AMRO, MIT, General Electric, dan lain-lain membentuk sebuah tim khusus yang siap dan sigap untuk menghadapi berbagai *incident* yang mungkin terjadi dan dapat merugikan organisasi. Tim ini biasa disebut sebagai CERT atau Computer Emergency Response Team. Tim CERT dari ABN AMRO misalnya, akan bertanggung jawab penuh untuk memonitor dan mengelola berbagai isu-isu terkait dengan keamanan internet untuk menjaga aset informasi dan komunikasi dari seluruh unit-unit bisnis ABN AMRO yang ada di dunia ini.

Dalam dunia keamanan internet dikenal prinsip *"your security is my security"* atau yang dalam praktek manajemen sering dianalogikan dengan contoh sebuah rantai, dimana *"the strenght of a chain depends on its weakest link"* (kekuatan sebuah rantai terletak pada sambungannya yang terlemah). Artinya adalah bahwa sebaik-baiknya sebuah organisasi mengelola keamanan sistem teknologi informasinya, kondisi sistem keamanan pihak-pihak lain yang terhubung di internet akan secara signifikan mempengaruhinya. Hal inilah yang kemudian menimbulkan pertanyaan utama: terlepas dari adanya sejumlah CERT yang telah beroperasi, bagaimana mereka dapat bersama-sama menjaga keamanan internet yang sedemikian besar dan luas jangkauannya? Dalam kaitan inilah maka sebuah perguruan tinggi terkemuka di Amerika Serikat yaitu Carnegie Mellon University, melalui lembaga risetnya Software Engineering Institute, memperkenalkan konsep CERT/CC yaitu singkatan dari Computer Emergency Response Team (Coordination Center) - yaitu sebuah pusat koordinasi sejumlah CERT yang tertarik untuk bergabung dalam forum atau komunitas ini. Dengan adanya pusat koordinasi ini, maka para praktisi CERT dapat bertemu secara virtual maupun fisik untuk membahas berbagai isu terkait dengan keamanan dan pengamanan internet. Untuk membedekannya dengan CERT, maka dikembangkanlah sebuah istilah khusus untuk merepresentasikan CERT/CC yaitu CSIRT. Di Jepang contohnya, banyak sekali tumbuh lembaga-lembaga CERT independen yang dikelola oleh pihak swasta. Untuk itulah maka dibentuk sebuah CSIRT dengan nama JPCERT/CC sebagai sebuah forum

berkumpulnya dan bekerjasamanya pengelolaan keamanan internet melalui sebuah atap koordinasi secara nasional.

Pendirian ID-SIRTII

Kasus atau *incident* yang menimpa sistem informasi dan teknologi pendukung pemilu 2004 di Indonesia membuka mata masyarakat akan besarnya ancaman keamanan yang dapat menimpa berbagai sistem berskala nasional apapun yang ada di tanah air. Bisa dibayangkan apa jadinya jika eksploitasi tersebut terjadi pada obyek vital yang ada di Indonesia, seperti pada sistem pembayaran nasional, sistem distribusi listrik, sistem persenjataan militer, sistem pelabuhan udara, dan lain sebagainya. Oleh karena itulah maka segenap komunitas di tanah air yang perduli akan keamanan komputer dan internet - yang terdiri dari APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), Mastel (Masyarakat Telematika), AWARI (Asosiasi Warung Internet Indonesia), Kepolisian Republik Indonesia, dan Direktorat Jenderal Post dan Telekomunikasi Departemen Komunikasi dan Informatika Republik Indonesia - berjuang keras untuk membentuk lembaga CSIRT untuk tingkat nasional Indonesia. Akhirnya pada tahun 2007, melalui Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jarinan Telekomunikasi berbasis Protokol Internet, lahirlah sebuah institusi yang bernama ID-SIRTII, singkatan dari "Indonesia Security Incident Response Team on Internet Infrastructure". Menurut Permen 26 tersebut, tugas utama ID-SIRTII adalah sebagai berikut:

1. Mensosialisasikan kepada seluruh pihak yang terkait untuk melakukan kegaitan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;
2. Melakukan pemaantauan, pendeteksian dini, dan peringatan dini terhadap ancaman dan gangguan pada jaringan telekomunikasi berbasis protokol internet di Indonesia;
3. Membangun dan atau menyediakan, mengoperasikan, memelihara, dan mengembangkan sistem *database* pemantauan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet sekurang-kurangnya untuk:

    a. Mendukung kegiatan sebagaimana dimaksud dalam butir 2 di atas;
    b. Menyimpan rekaman transaksi *(log file)*; dan
    c. Mendukung proses penegakan hukum.

4. Melaksanakan fungsi layanan informasi atas ancaman dan gangguan keamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;
5. Menyediakan laboratorium simulasi dan pelatihan kegaitan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;
6. Melakukan pelayanan konsultasi dan bantuan teknis; dan
7. Menjadi *contact point* dengan lembaga terkait tentang pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet baik dalam negeri maupun luar negeri.

Memperhatikan ketujuh tugas dan fungsi utama yang cukup luas tersebut, maka jelas terlihat bahwa dalam melaksanakan pekerjaannya, ID-SIRTII harus bekerjasama dengan banyak pihak terkait yang berkepentingan (baca: *stakeholders*). Artinya adalah, bahwa untuk negara kepulauan semacam Indonesia, dimana karakteristiknya sangat beragam (baca: *heterogeneous*), diharapkan akan terbentuk di kemudian hari sejumlah CERT pada komunitas-komunitas tertentu.

Dilihat dari karakteristik dan anggotanya, ada 4 (empat) jenis CERT yang dikenal, yaitu:

- *Sector CERT* - institusi yang dibentuk untuk mengelola keamanan komputer/internet untuk lingkungan komunitas tertentu seperti militer, rumah sakit, universitas, dan lain sebagainya;
- *Internal CERT* - institusi yang dibentuk sebuah perusahaan yang memiliki ruang lingkup geografis tersebar di seluruh nusantara sehingga dibutuhkan koordinasi dalam hal mengelola keamanan komputer, seperti milik Pertamina, LippoBank, PLN, Telkom, dan lain sebagainya;
- *Vendor CERT* - institusi pengelola keamanan yang dimiliki oleh vendor teknologi untuk melindungi kepentingan pemakai teknologi terkait, seperti Yahoo, Cisco, Microsoft, Oracle, dan lain sebagainya; dan
- *Commercial CERT* - institusi yang biasanya dibentuk oleh sejumlah praktisi dan ahli keamanan komputer/internet yang banyak menawarkan beragam produk/jasa kepada

pihak lain terkait dengan tawaran membantu proses pengamanan teknologi informasi secara komersial.

Masyarakat Dunia Maya

Tidak banyak orang yang menyangka sebelumnya bahwa internet yang tadinya hanya merupakan jejaring komunikasi antara lembaga riset perguruan tinggi di Amerika Serikat akan menjadi dunia tersendiri tempat berkumpulnya masyarakat dunia untuk melakukan transaksi, interaksi, dan koordinasi secara global seperti sekarang ini. Bahkan keberadaannya telah mampu menciptakan suatu revolusi tersendiri di sektor pemerintahan, industri swasta, komunitas akademik, dan aspek-aspek kehidupan lainnya. Masyarakat internet ini semakin lama semakin meningkat jumlahnya. Bahkan statistik terakhir tahun 2008 memperlihatkan bahwa satu dari lima penduduk dunia telah menjadi pengguna internet dewasa ini. Bukanlah suatu hal yang mustahil bahwa dalam waku yang tidal lama lagi, seluruh penduduk dunia akan menjadi *internet user* yang aktif.

Masalah Internet dan Lembaga Pengaman

Memperhatikan bahwa internet adalah suatu wahana "dari, oleh, dan untuk" masyarakat dunia maya, maka salah satu isu utama yang mengemuka adalah permasalahan keamanan atau *security* - baik dalam hal keamanan informasi (konten), infrastruktur, dan interaksi; karena dalam konteks arsitektur internet yang demokratis ini akan meningkatkan faktor resiko terjadinya *incident*keamanan yang tidak diinginkan - baik yang dilakukan secara sengaja maupun tidak. Apalagi sangat banyak hasil riset yang memperlihatkan bahwa dari hari ke hari, jumlah serangan dan potensi ancaman di dunia maya secara kualitas maupun kuantitas meningkat secara signifikan. Karena internet merupakan suatu "rimba tak bertuan", maka masing-masing pihak yang terhubung di dalamnya harus memperhatikan dan menjamin keamanannya masing-masing. Selain melengkapi sistem teknologi informasinya dengan perangkat lunak dan perangkat keras pengamanan (seperti *firewalls*dan *anti virus* misalnya), beberapa institusi besar seperti ABN AMRO, MIT, General Electric, dan lain-lain membentuk sebuah tim khusus yang siap dan sigap untuk menghadapi berbagai *incident* yang mungkin terjadi dan dapat merugikan organisasi. Tim ini biasa disebut sebagai CERT atau Computer Emergency Response Team. Tim CERT dari ABN AMRO misalnya, akan bertanggung jawab penuh untuk memonitor dan mengelola berbagai isu-isu terkait dengan keamanan internet untuk menjaga aset informasi dan komunikasi dari seluruh unit-unit bisnis ABN AMRO yang ada di dunia ini.

Dalam dunia keamanan internet dikenal prinsip *"your security is my security"* atau yang dalam praktek manajemen sering dianalogikan dengan contoh sebuah rantai, dimana *"the strenght of a chain depends on its weakest link"* (kekuatan sebuah rantai terletak pada sambungannya yang terlemah). Artinya adalah bahwa sebaik-baiknya sebuah organisasi mengelola keamanan sistem teknologi informasinya, kondisi sistem keamanan pihak-pihak lain yang terhubung di internet akan secara signifikan mempengaruhinya. Hal inilah yang kemudian menimbulkan pertanyaan utama: terlepas dari adanya sejumlah CERT yang telah beroperasi, bagaimana mereka dapat bersama-sama menjaga keamanan internet yang sedemikian besar dan luas jangkauannya? Dalam kaitan inilah maka sebuah perguruan tinggi terkemuka di Amerika Serikat yaitu Carnegie Mellon University, melalui lembaga risetnya Software Engineering Institute, memperkenalkan konsep CERT/CC yaitu singkatan dari Computer Emergency Response Team (Coordination Center) - yaitu sebuah pusat koordinasi sejumlah CERT yang tertarik untuk bergabung dalam forum atau komunitas ini. Dengan adanya pusat koordinasi ini, maka para praktisi CERT dapat bertemu secara virtual maupun fisik untuk membahas berbagai isu terkait dengan keamanan dan pengamanan internet. Untuk membedekannya dengan CERT, maka dikembangkanlah sebuah istilah khusus untuk merepresentasikan CERT/CC yaitu CSIRT. Di Jepang contohnya, banyak sekali tumbuh lembaga-lembaga CERT independen yang dikelola oleh pihak swasta. Untuk itulah maka dibentuk sebuah CSIRT dengan nama JPCERT/CC sebagai sebuah forum berkumpulnya dan bekerjasamanya pengelolaan keamanan internet melalui sebuah atap koordinasi secara nasional.

Pendirian ID-SIRTII

Kasus atau *incident* yang menimpa sistem informasi dan teknologi pendukung pemilu 2004 di Indonesia membuka mata masyarakat akan besarnya ancaman keamanan yang dapat menimpa berbagai sistem berskala nasional apapun yang ada di tanah air. Bisa dibayangkan apa jadinya jika eksploitasi tersebut terjadi pada obyek vital yang ada di Indonesia, seperti pada sistem pembayaran nasional, sistem distribusi listrik, sistem persenjataan militer, sistem pelabuhan udara, dan lain sebagainya. Oleh karena itulah maka segenap komunitas di tanah air yang perduli akan keamanan komputer dan internet - yang terdiri dari APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), Mastel (Masyarakat Telematika), AWARI (Asosiasi Warung Internet Indonesia), Kepolisian Republik Indonesia, dan Direktorat Jenderal Post dan Telekomunikasi Departemen Komunikasi dan Informatika Republik Indonesia - berjuang keras untuk membentuk lembaga CSIRT untuk tingkat nasional Indonesia. Akhirnya pada tahun 2007, melalui Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor

26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jarinan Telekomunikasi berbasis Protokol Internet, lahirlah sebuah institusi yang bernama ID-SIRTII, singkatan dari "Indonesia Security Incident Response Team on Internet Infrastructure". Menurut Permen 26 tersebut, tugas utama ID-SIRTII adalah sebagai berikut:

1. Mensosialisasikan kepada seluruh pihak yang terkait untuk melakukan kegaitan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;
2. Melakukan pemaantauan, pendeteksian dini, dan peringatan dini terhadap ancaman dan gangguan pada jaringan telekomunikasi berbasis protokol internet di Indonesia;
3. Membangun dan atau menyediakan, mengoperasikan, memelihara, dan mengembangkan sistem *database* pemantauan dan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet sekurang-kurangnya untuk:

    a. Mendukung kegiatan sebagaimana dimaksud dalam butir 2 di atas;
    b. Menyimpan rekaman transaksi *(log file)*; dan
    c. Mendukung proses penegakan hukum.

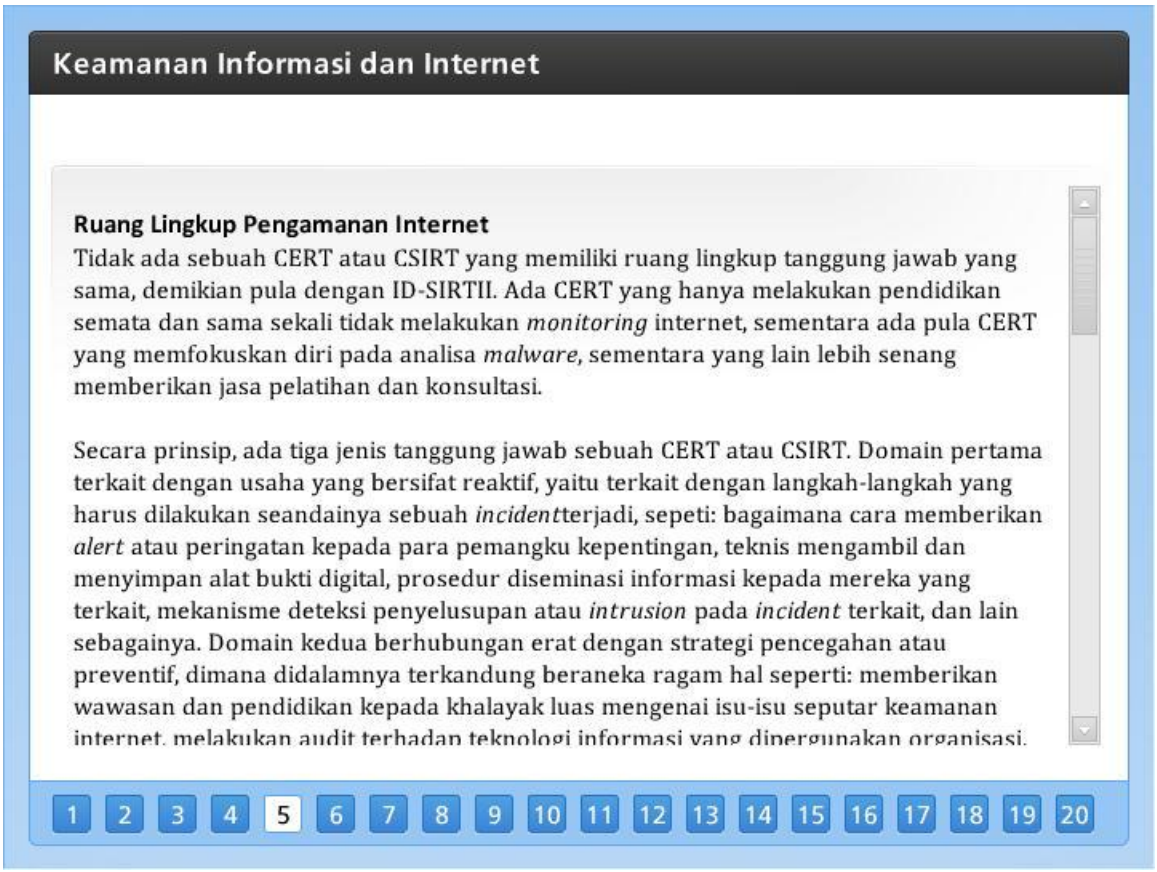
4. Melaksanakan fungsi layanan informasi atas ancaman dan gangguan keamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;
5. Menyediakan laboratorium simulasi dan pelatihan kegaitan pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet;
6. Melakukan pelayanan konsultasi dan bantuan teknis; dan
7. Menjadi *contact point* dengan lembaga terkait tentang pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet baik dalam negeri maupun luar negeri.

Memperhatikan ketujuh tugas dan fungsi utama yang cukup luas tersebut, maka jelas terlihat bahwa dalam melaksanakan pekerjaannya, ID-SIRTII harus bekerjasama dengan banyak pihak terkait yang berkepentingan (baca: *stakeholders*). Artinya adalah, bahwa untuk negara kepulauan semacam Indonesia, dimana karakteristiknya sangat beragam (baca: *heterogeneous*),

diharapkan akan terbentuk di kemudian hari sejumlah CERT pada komunitas-komunitas tertentu.

Dilihat dari karakteristik dan anggotanya, ada 4 (empat) jenis CERT yang dikenal, yaitu:

- *Sector CERT* - institusi yang dibentuk untuk mengelola keamanan komputer/internet untuk lingkungan komunitas tertentu seperti militer, rumah sakit, universitas, dan lain sebagainya;
- *Internal CERT* - institusi yang dibentuk sebuah perusahaan yang memiliki ruang lingkup geografis tersebar di seluruh nusantara sehingga dibutuhkan koordinasi dalam hal mengelola keamanan komputer, seperti milik Pertamina, LippoBank, PLN, Telkom, dan lain sebagainya;
- *Vendor CERT* - institusi pengelola keamanan yang dimiliki oleh vendor teknologi untuk melindungi kepentingan pemakai teknologi terkait, seperti Yahoo, Cisco, Microsoft, Oracle, dan lain sebagainya; dan
- *Commercial CERT* - institusi yang biasanya dibentuk oleh sejumlah praktisi dan ahli keamanan komputer/internet yang banyak menawarkan beragam produk/jasa kepada pihak lain terkait dengan tawaran membantu proses pengamanan teknologi informasi secara komersial.



Ruang Lingkup Pengamanan Internet

Tidak ada sebuah CERT atau CSIRT yang memiliki ruang lingkup tanggung jawab yang sama, demikian pula dengan ID-SIRTII. Ada CERT yang hanya melakukan pendidikan semata dan sama sekali tidak melakukan *monitoring* internet, sementara ada pula CERT yang memfokuskan diri pada analisa *malware*, sementara yang lain lebih senang memberikan jasa pelatihan dan konsultasi.

Secara prinsip, ada tiga jenis tanggung jawab sebuah CERT atau CSIRT. Domain pertama terkait dengan usaha yang bersifat reaktif, yaitu terkait dengan langkah-langkah yang harus dilakukan seandainya sebuah *incident*terjadi, sepeti: bagaimana cara memberikan *alert* atau peringatan kepada para pemangku kepentingan, teknis mengambil dan menyimpan alat bukti digital, prosedur diseminasi informasi kepada mereka yang terkait, mekanisme deteksi penyelusupan atau *intrusion* pada *incident* terkait, dan lain sebagainya. Domain kedua berhubungan erat dengan strategi pencegahan atau preventif, dimana didalamnya terkandung beraneka ragam hal seperti: memberikan wawasan dan pendidikan kepada khalayak luas mengenai isu-isu seputar keamanan internet, melakukan audit terhadap teknologi informasi yang dipergunakan

organisasi, menjalankan prosedur tes penetrasi kepada sistem yang dimiliki untuk mengidentifikasikan potensi kerawanan yang ada, mempelajari trend teknologi informasi dan internet ke depan - terutama terkait dengan isu keamanan perangkat lunak dan peralatan-peralatan baru, dan lain sebagainya

Dan domain terkahir atau ketiga, adalah suatu usaha untuk meningkatkan level atau mutu kualitas organisasi yang saat ini telah dimiliki, agar semakin baik dalam aspek pengamanan informasi yang dimaksud. Usaha yang biasa dilakukan menyangkut hal-hal semacam: menyewa konsultan untuk mengukur dan meningkatkan level kematangan (baca: *maturity level*) aspek keamanan informasi, menjalankan aktivitas manajemen resiko, melakukan evaluasi terhadap semua perangkat dan aplikasi yang dimiliki, melatih atau memberikan *training* kepada sebanyak mungkin manajemen dan karyawan/staff organisasi, dan lain sebagainya.

Konstituen ID-SIRTII

Hampir 99% CERT/CSIRT di seluruh dunia dibangun pada mulanya melalui dana pemerintah, karena memang merekalah yang pertama kali merasa pentingnya lembaga tersebut. Sejalan dengan perkembangannya, maka mulai tumbuhlah sejumlah CERT/CSIRT yang dikelola oleh swasta secara mandiri. Oleh karena itulah maka, setiap lembaga CERT/CSIRT memiliki konstituennya masing-masing, karena perbedaan misi yang diembannya. Dalam hal ini, ID-SIRTII dibangun sepenuhnya melalui dana pemerintah Indonesia, yaitu melalui Direktorat Jenderal Pos dan Telekomunikasi, Departemen Komunikasi dan Informatika Republik Indonesia. Oleh karena itulah maka untuk sementara ini, keberadaan ID-SIRTII tidak dapat dipisahkan dari peranan Dirjen Postel Depkominfo.

Melihat misi serta tugas utamanya, terutama dipandang dari sudut karakteristik *customer* atau pelanggan utamanya, konstituen ID-SIRTII dapat dibagi menjadi 2 (dua) kelompok utama: konstituen langsung (internal) dan konstituen tidak langsung (eksternal). Termasuk dalam konstituen internet adalah empat kelompok komunitas, yaitu:

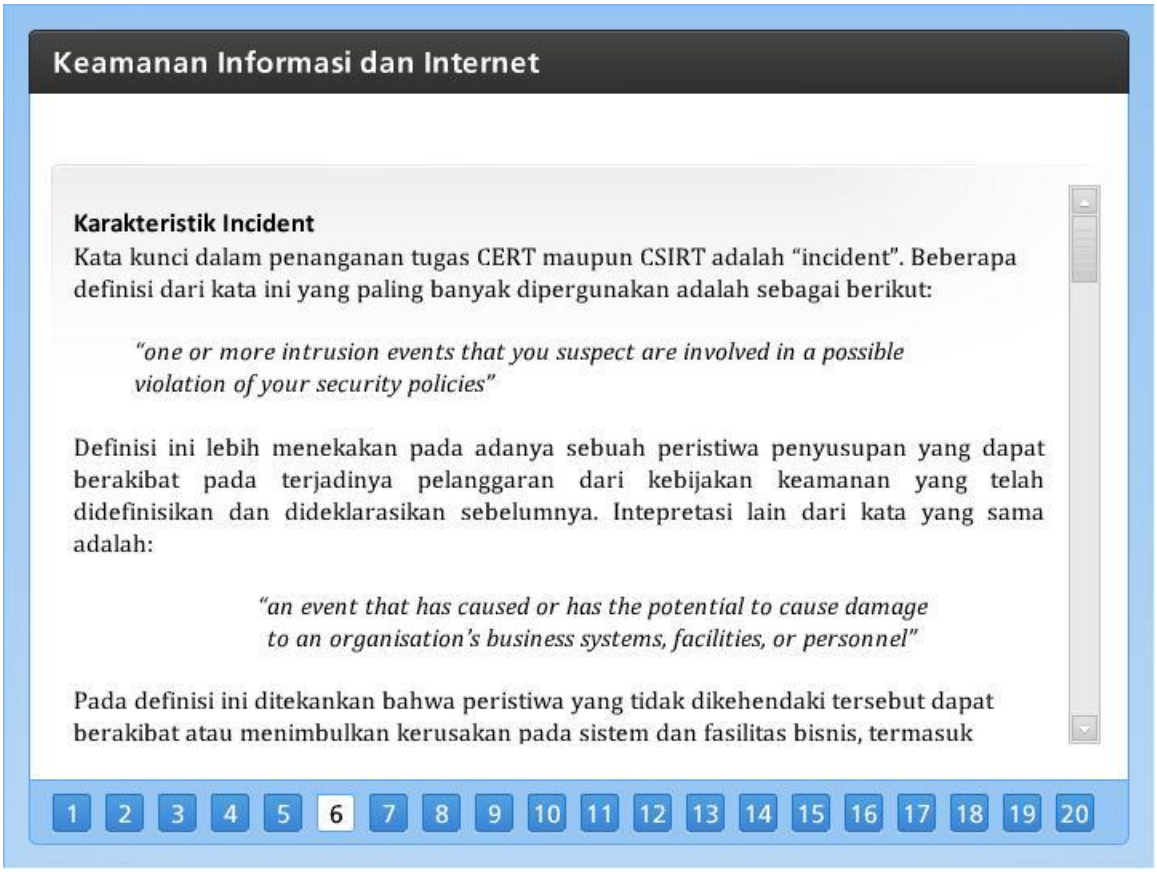
- Internet Service Providers, Internet Exchange Points, dan Network Access Points;
- Penegak hukum, yang terdiri dari Kepolisian, Kejaksaan, dan Departemen Kehakiman;
- CERT/CSIRTS serupa dari negara luar, terutama yang tergabung dalam APCERT (Asia Pacific CERTs); dan

- Beragam institusi dan/atau komunitas keamanan informasi dan internet di Indonesia lainnya.

Sementara itu, konstituen eksternal dari ID-SIRTII (seperti yang terlihat pada gambar) pada dasarnya adalah *customer* langsung dari keempat konstituen internal terdahulu, sehingga jika dipetakan menjadi:

- Pengguna internet yang merupakan sebuah korporasi/organisasi maupun individu, dimana pada dasarnya mereka adalah pelanggan dari beragam ISP yang beroperasi di tanah air;
- Para polisi, jaksa, dan hakim yang ditugaskan oleh institusinya masing-masing dalam menangani kasus-kasus kejahatan kriminal teknologi informasi;
- CERT/CSIRT yang ada di setiap negara maupun yang telah membentuk kelompok atau asosiasi yang berbeda-beda seperti APCERT dan FIRST; serta

Seluruh CERT/CSIRT yang ada di tanah air, termasuk di dalamnya institusi swasta, pemerintahan, dan perguruan tinggi yang terlibat secara langsung maupun tidak langsung terhadap isu-isu seputar kemanan informasi



Karakteristik Incident

Kata kunci dalam penanganan tugas CERT maupun CSIRT adalah "incident". Beberapa definisi dari kata ini yang paling banyak dipergunakan adalah sebagai berikut:

> *"one or more intrusion events that you suspect are involved in a possible violation of your security policies"*

Definisi ini lebih menekakan pada adanya sebuah peristiwa penyusupan yang dapat berakibat pada terjadinya pelanggaran dari kebijakan keamanan yang telah didefinisikan dan dideklarasikan sebelumnya. Intepretasi lain dari kata yang sama adalah:

> *"an event that has caused or has the potential to cause damage to an organisation's business systems, facilities, or personnel"*

Pada definisi ini ditekankan bahwa peristiwa yang tidak dikehendaki tersebut dapat berakibat atau menimbulkan kerusakan pada sistem dan fasilitas bisnis, termasuk individu yang ada di dalamnya. Lihatlah definisi berikutnya dari kata *incident* berikut ini:

> *"any occurrence or series of occurences having the same origin that results in the discharge or substabtial threat"*

Yang menarik dari definisi ini adalah diperkenalkannya kata "substantial threat" atau ancaman yang subsansial terhadap suatu sistem. Frase ini dipergunakan untuk menekankan bahwa peristiwa yang tidak diinginkan tersebut dapat benar-benar menimbulkan kerusakan fundamental (fatal) terhadap sebuah sistem. Menggabungkan ketiga ragam definisi di atas, Carnegie Mellon University dalam bukunya CSIRT Handbook mendefinisikan *incident* sebagai:

> *"an undesired event that could have resulted in harm to people, damage to property, loss to process, or harm to the environment"*

atau "suatu peristiwa yang tidak diharapkan/diinginkan terjadi, yang dapat merugikan manusia, menghancurkan aset atau fasilitas, mengganggu proses, dan merusak lingkungan sekitarnya.

Melalui definisi dari kata "incident" ini semakin jelas terlihat strategisnya lembaga-lembaga semacam ID-SIRTII dimiliki oleh sebuah negara. Internet yang telah dipergunakan di berbagai bidang kehidupan masyarakat perlu dijaga keutuhan dan keamanannya dari peristiwa yang tidak diinginkan tersebut.

Ragam Incident Internet

Begitu banyak jenis *incident* yang terjadi di dunia maya, mulai dari yang sangat sederhana hingga yang sangat kompleks modus operandinya. Di Indonesia misalnya, *web defacement* merupakan jenis *incident* yang sangat sering terjadi, berupa pengrusakan atau perubahan terhadap isi sebuah situs internet (baca: *website*). Hingga saat ini, situs-situs resmi yang telah menjadi korban *web defacement* misalnya milik Departemen Luar Negeri, Bank Indonesia, Partai Golongan Karya, Departemen Komunikasi dan Informatika, Komite Pemilihan Umum, dan lain-lain. Jenis *incident* lainnya yang juga cukup banyak terjadi di tanah air adalah yang dikenal

sebagai istilah *phishing*, yaitu tindakan penyamaran oleh seseorang atau individu terhadap sebuah organisasi, sehingga sang korban merasa bahwa yang bersangkutan adalah benar-benar pihak yang sah, sehingga "secara sadar" terjadi proses pengiriman data rahasia seperti *password*atau nomor kartu kredit. Kasus terkemuka yang menimpa Bank BCA mengawali kegiatan *phishing* yang terjadi di tanah air, dimana diikuti oleh beraneka ragam variasinya - seperti penipuan melalui SMS yang paling banyak memakan korban dewasa ini. Di kancah dunia kriminalisasi, Indonesia sangat dikenal dengan tingginya kuantitas penipuan dunia maya melalui upaya penggunaan kartu kredit secara tidak sah, atau yang lebih dikenal dengan istilah *carding*. Jenis *incident* ini menimpa pemegang kartu kredit yang nomornya serta informasi penting lainnya telah diketahui oleh orang lain dan disalahgunakan untuk membeli barang-barang atau jasa-jasa tertentu via internet.

Belakangan ini, fenomena *spamming*atau pengiriman *brosur elektronik* via internet sering pula dikategorikan sebagai *incident* karena begitu banyaknya *spam* yang di isinya adalah program-program (baca: *file*) jahat yang dapat merusak sistem komputer, seperti *virus, worms,* dan *trojan horse*. Banyak pengguna awam yang dikirimi *electronic email (email)* - yang pada dasarnya merupakan *spam* ini - membukanya, sehingga berakibat pada masuknya virus atau *worms* tersebut ke dalam sistem komputernya, dan tanpa disadari dapat menularkannya ke komputer-komputer lainnya melalui jejaring internet. Dalam konteks ini, para pengguna internet harus pula berhati-hati jika mengunduh (baca: *download*) *file* dari internet - terutama yang gratis - karena tidak semua *file* yang diambil tersebut bebas dari program-program jahat. Para kriminal di dunia maya, sangat senang meletakkan program-program jahat tersebut di *file-file* yang digemari masyarakat, seperti: lagu-lagu mp3, film atau video, gambar-gambar porno, *wallpaper* komputer, dan lain sebagainya.

Seperti layaknya sebuah jalan raya utama (baca: jalan tol), internet dipenuhi oleh paket-paket data/informasi yang dipertukarkan oleh seluruh penggunanya di muka bumi ini. Tidak jarang terjadi kemacetan yang mengakibatkan terganggunya lalu lintas data di jejaring maya ini. Dari seluruh kemacetan yang pernah terjadi, banyak yang sebenarnya merupakan *incident*, alias adanya pihak-pihak yang secara sengaja "membanjiri" internet dengan paket-paket data informasi tertentu sehingga membuat lalu lintas data menjadi macet total, dan merusak interaksi atau pun transaksi yang seharusnya terjadi. Jenis *incident* ini dinamakan sebagai DoS yang merupakan singkatan dari *Denial of Services* - dengan variasi utamanya adalah DDoS (Distributed Denial of Services). Beratus-ratus ribu bahkan berjuta-juta paket data "tak berguna" dikirimkan seseorang untuk membanjiri jalan raya internet sehingga terjadilah "kemacetan" dimana-mana. Belakangan ini terdapat fenomena *incident* yang membuat seluruh praktisi internet di dunia pusing tujuh keliling karena kompleksitasnya yang sedemikian tinggi.

Sebuah *incident* yang dikenal dengan istilah *botnet* atau *robot network*. Cara kerja *botnet* adalah sebagai berikut. Seseorang kriminal, sebut saja sebagai *the puppet master*, secara diam-diam meletakkan program-program jahat di beribu-ribu komputer yang tersebar dimana-mana melalui koneksi internet. Keberadaan *file* tersebut tidak disadari oleh pengguna komputer, karena sifatnya yang pasif - alias tidak melakukan apa-apa. Oleh karena itulah maka *file* ini dinamakan sebagai *zombie* alias "mayat hidup". Pada saat tertentulah, jika serangan telah ditetapkan untuk dilakukan, sang *puppet master* mengerahkan seluruh *zombie* yang tersebar di seluruh dunia untuk menyerang infrastruktur sebuah sistem komputer secara simultan dan kolosal. Tentu saja gerakan gala DDoS ini akan langsung membuat sistem komputer yang diserang menjadi tidak berfungsi - sebagaimana layaknya terjadi keroyokan dalam sebuah perkelahian tidak seimbang. Peristiwa yang menimpa Estonia merupakan salah satu bukti betapa ampuhnya dan besarnya dampak yang dapat terjadi melalui *incident* berjenis botnet ini.

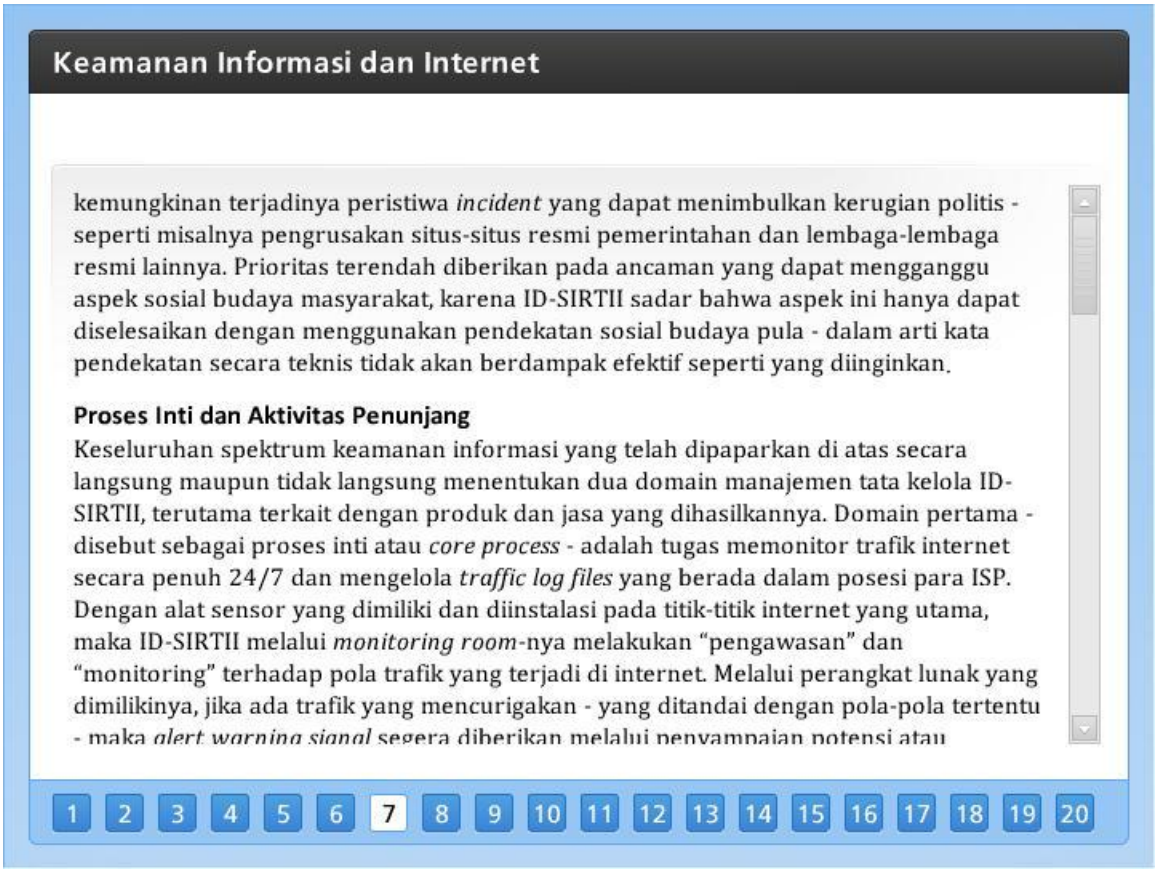
Riset dan statistik memperlihatkan, bahwa terjadi peningkatan yang signifikan terhadap kuantitas dan kualitas *incident* atau pun serangan di dunia maya. Gagal untuk memitigasi ancaman terjadinya serangan ini dapat berakibat serius dan fatal bagi organisasi ata institusi yang terlibat di dalamnya.

Strategi Prioritas Penanganan Incident

Melihat begitu banyaknya jenis dan karakteristik *incident* yang dapat menimpa seluruh pengguna internet, maka lembaga pengaman semacam ID-SIRTII harus memiliki strategi prioritas penanganan *incident* yang mungkin terjadi. Terkait dengan klasifikasi *incident*- seperti *interception, interuption, modification,* dan *fabrication* - ID-SIRTII memiliki empat level prioritas dalam penanganan *incident*. Prioritas pertama ditujukan pada *incident* yang dampaknya dapat berakibat pada terganggunya keamanan publik/masyarakat dan keamanan negara. Misalnya adalah *incident* yang dapat merusak sistem pengamanan lalu lintas penerbangan udara atau sistem persenjataan militer. Jika terdapat potensi ataupun peristiwa *incident* terkait dengan hal ini, maka ID-SIRTII akan mengerahkan sejumlah stafnya untuk berkonsentrasi penuh menangani kasus ini saja (dikenal dengan tingkat keterhubungan *many-to-one*).

Sementara itu prioritas kedua ditujukan pada penanganan *incident*yang dapat mengganggu sistem ekonomi suatu negara - misalnya adalah sistem transaksi perbankan dan sistem telekomunikasi masyarakat. Jika terjadi hal ini, maka ID-SIRTII siap mengerahkan dan mengalokasikan individu-individu yang dimilikinya untuk menangani hal tersebut dalam

hubungan relasi *one-to-many* - seorang ahli ditugaskan untuk menjaga sejumlah organisasi dari kemungkinan terjadinya *incident* yang dapat berdampak kerugian ekonomis.



kemungkinan terjadinya peristiwa *incident* yang dapat menimbulkan kerugian politis - seperti misalnya pengrusakan situs-situs resmi pemerintahan dan lembaga-lembaga resmi lainnya. Prioritas terendah diberikan pada ancaman yang dapat mengganggu aspek sosial budaya masyarakat, karena ID-SIRTII sadar bahwa aspek ini hanya dapat diselesaikan dengan menggunakan pendekatan sosial budaya pula - dalam arti kata pendekatan secara teknis tidak akan berdampak efektif seperti yang diinginkan.

Proses Inti dan Aktivitas Penunjang

Keseluruhan spektrum keamanan informasi yang telah dipaparkan di atas secara langsung maupun tidak langsung menentukan dua domain manajemen tata kelola ID-SIRTII, terutama terkait dengan produk dan jasa yang dihasilkannya. Domain pertama - disebut sebagai proses inti atau *core process* - adalah tugas memonitor trafik internet secara penuh 24/7 dan mengelola *traffic log files* yang berada dalam posesi para ISP. Dengan alat sensor yang dimiliki dan diinstalasi pada titik-titik internet

yang utama, maka ID-SIRTII melalui *monitoring room*-nya melakukan "pengawasan" dan "monitoring" terhadap pola trafik yang terjadi di internet. Melalui perangkat lunak yang dimilikinya, jika ada trafik yang mencurigakan - yang ditandai dengan pola-pola tertentu - maka *alert warning signal* segera diberikan melalui penyampaian potensi atau peristiwa *incident*tersebut kepada yang bersangkutan. Perlu diingat, bahwa walaupun ID-SIRTII memiliki kemampuan untuk melakukan mitigasi, namun secara tugas dan tanggung jawab yang dibebankan kepadanya, kegiatan mitigasi tersebut tidak boleh dilakukan. Artinya adalah bahwa tindakan mitigasi terhadap *incident* yang ditemukan harus dilakukan secara mandiri oleh pihak-pihak yang terlibat dan berkepentingan.

Masih terkait dengan tugas inti atau tugas pokok, ID-SIRTII juga memiliki tanggung jawab untuk mengelola *traffic log file* yang dihimpun oleh setiap ISP yang beroperasi di Indonesia. Perlu diketahui bahwa salah satu kewajiban ISP yang dinyatakan dalam kontrak lisensi antara dirinya dengan Dirjen Postel selaku pemerintah adalah kesanggupan dan kesediaannya dalam merekam dan menghimpun *traffic log file* yang terjadi pada jaringan infrastrukturnya. Sehubungan dengan hal ini, maka Dirjen Postel memerintahkan kepada seluruh ISP yang ada di Indonesia, untuk menyerahkan *traffic log file* yang dimilikinya untuk dikelola oleh ID-SIRTII demi kepentingan nasional.

Secara langsung, kedua tugas inti ID-SIRTII tersebut mendatangkan keuntungan bagi konstituennya, terutama dalam konteks sebagai berikut:

- Seyogiyanya, setiap ISP harus memiliki peralatan untuk memonitor dan menangani *incident* yang dapat menimpa para pelanggannya. Mengingat cukup tingginya investasi yang perlu dikeluarkan untuk membangun peralatan tersebut, maka melalui ID-SIRTII, ISP yang bersangkutan tidak perlu mengadakannya, karena dapat dipakai secara bersama-sama (baca: *shared services*);
- Begitu banyaknya peristiwa kriminal di dunia maya memaksa polisi untuk mengumpulkan alat bukti yang kebanyakan berada dalam posesi ISP terkait. Semakin banyak peristiwa yang terjadi berakibat semakin sering "diganggunya" ISP oleh kebutuhan penegak hukum tersebut. Dengan dikelolanya *traffic log file*oleh pihak ID-SIRTII, maka penegak hukum seperti polisi atau jaksa tidak perlu memintanya pada ISP, karena ID-SIRTII akan menyediakannya langsung kepada pihak-pihak yang berwenang; dan
- Sejumlah kasus kriminal di dunia maya sering berakhir dengan dilepaskannya terdakwa karena hakim berhasil diyakinkan oleh pembelanya bahwa cara polisi dan jaksa dalam

mengambil barang bukti digital yang dibutuhkan pengadilan adalah melalui mekanisme yang tidak sah dan/atau meragukan. Karena ID-SIRTII memiliki prosedur dan mekanisme manajemen *traffic log file* yang telah diakui secara internasional karena memenuhi standar yang berlaku, maka hakim tidak perlu ragu-ragu lagi dalam menerima alat bukti yang berasal dari lembaga resmi semacam ID-SIRTII.

Dalam kesehari-hariannya, sesuai amanat Peraturan Menteri terkait, ID-SIRTII disamping melakukan dua tugas pokok tadi, menjalankan pula sejumlah aktivitas penunjang. Aktivitas pertama adalah melakukan edukasi kepada publik dan kepada seluruh pihak yang berkepentingan terhadap keamanan informasi. Dalam hal ini ID-SIRTII bekerjasama dengan beragam asosiasi, seperti: Aspiluki, Apkomindo, APJII, Mastel, Awari, Aptikom, I2BC, Ipkin, dan lain sebagainya.

Aktivitas kedua adalah menjadi mitra bagi institusi-institusi atau organisasi-organisasi yang terkait langsung dengan manajemen obyek-obyek vital industri, seperti BUMN, Departemen dan Kementrian, Badan Kepresidenan, dan Perhimpunan Bank Umum Nasional (PERBANAS). Aktivitas ketiga adalah menyelenggarakan pelatihan-pelatihan terkait dengan kiat-kiat pengamanan informasi bagi mereka yang membutuhkan. Dalam hal ini ID-SIRTII banyak bekerjasama dengan lembaga-lembaga sejenis yang telah memiliki pengalaman internasional. Aktivitas keempat adalah mendirikan dan menjalankan laboratorium simulasi, tempat belajarnya sejumlah praktisi keamanan informasi dan internet untuk meningkatkan kompetensi maupun keahliannya memperbaiki kinerja keamanan di masing-masing organisasinya. Dan aktivitas kelima adalah menjalin kerjasama dengan lembaga-lembaga sejenis dari luar negeri, karena kebanyakan *incident* yang terjadi bersifat internasional. Kerjasama dengan luar negeri merupakan hal yang sangat mutlak perlu dilakukan mengingat kebanyakan *incident* perlu dipecahkan secara cepat dengan cara koordinasi, komunikasi, dan kooperasi antar negara untuk mencegah terjadinya penularan.

Mengingat betapa pentingnya kualitas dari kinerja lembaga semacam ID-SIRTII, maka dalam kegiatan rutinitas sehari-hari, ID-SIRTII memiliki *Standard Operating Procedures (SOP)* yang baku dan mengacu pada standar internasional. Pada saatnya nanti, ID-SIRTII harus berhasil memperoleh sertifikasi internasional standar yang terkait dengan peranan dan fungsi kerjanya, seperti: ISO17799/BS7799, ISO27001, dan ISO9001:2000. Hingga saat ini sebagian rutinitas kerja dari ID-SIRTII telah mengacu pada penerapan standar-standar yang disebutkan tadi.

Struktur Tim Kerja

Agar seluruh rangkaian proses terkait dapat berjalan secara efektif, maka struktur organisasi dari *response team* yang dimaksud haruslah sesuai dan selaras dengan karakteristik ruang lingkup kerja serta misi yang diemban. Secara struktur, otoritas tertinggi sebagai penanggung jawab kinerja kerja ID-SIRTII di Indonesia dipegang oleh Menteri Komunikasi dan Informatika, yang dalam hal ini dilimpahkan secara langsung kepada Direktur Jenderal Pos dan Telekomunikasi. Sebagai penanggung jawab implementasi sehari-hari, ditunjuklah sepasang pimpinan secara "tandem" yaitu Ketua Pelaksana dan Wakil Ketua Pelaksana ID-SIRTII. Dalam aktivitas kesehariannya, Ketua Pelaksana lebih memfokuskan diri pada aspek-aspek yang bersifat strategis, sementara Wakil Ketua Pelaksana bertugas secara khusus menangani hal-hal yang bersifat teknis operasional. Dengan demikian, maka sepasang pimpinan yang ada saling melengkapi untuk menjalankan ketujuh tugas pokok ID-SIRTII seperti yang telah dikemukakan sebelumnya.

Untuk mendukung pimpinan dalam kegiatan yang lebih operasional, maka ditunjuklah lima orang deputi untuk memimpin lima unit utama ID-SIRTII, masing-masing adalah:

1. Deputi Operasional dan Keamanan - dengan tugas pokok melakukan pemantauan atau *monitoring* terhadap trafik internet yang terjadi di Indonesia dalam mode 24/7;
2. Deputi Aplikasi dan Basis Data - dengan tugas pokok mengelola manajemen *traffic log file* yang diperoleh dari beragam *stakeholder* terkait untuk dipergunakan sebagaimana mestinya;
3. Deputi Riset dan Pengembangan - dengan tugas pokok melakukan analisa terhadap tren teknologi dan hal-hal terkait dengan keamanan informasi, termasuk di dalamnya melakukan analisa terhadap kondisi keamanan internet Indonesia berdasarkan hasil pengamatan terhadap trafik yang dilakukan;
4. Deputi Pendidikan dan Hubungan Masyarakat - dengan tugas pokok menyelenggarakan sejumlah program atau aktivitas peningkatan wawasan, kepedulian, dan pendidikan masyarakat terhadap pentingnya melakukan pengamanan terhadap infrastruktur teknologi informasi yang dipergunakan; dan
5. Deputi Kolaborasi Eksternal dan Kemitraan Internasional - dengan tugas pokok mewakili lembaga dalam berbagai kerjasama dan kolaborasi kemitraan antara ID-SIRTII dengan pihak-pihak lain, baik yang berada di tanah air maupun di luar negeri.

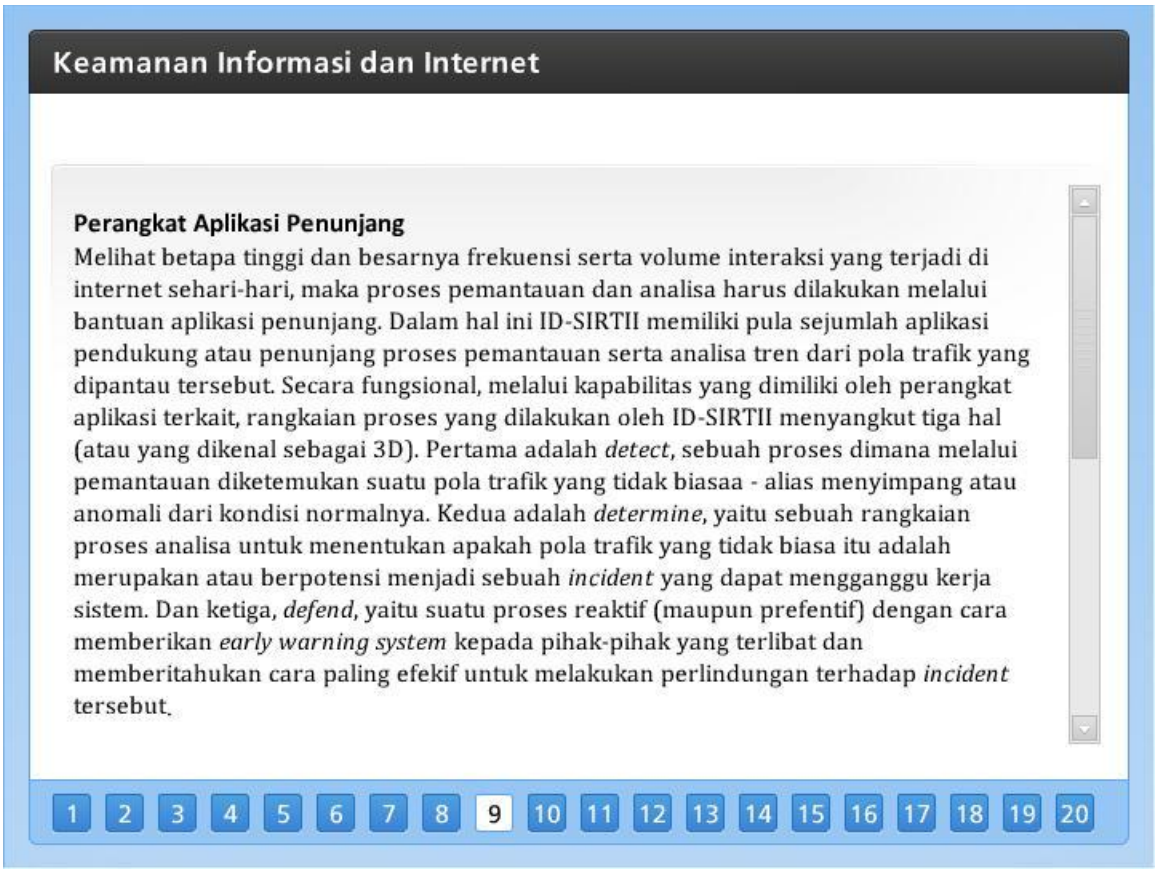
Masing-masing deputi yang ada dilengkapi dengan sejumlah staf dan personil untuk mengimplementasikan berbagai program yang telah disusun dan disepakati bersama. Seperti halnya lembaga-lembaga CERT/CSIRT serupa di negara lain, tim inti ID-SIRTII juga didukung oleh sebuah Tim Ahli yang secara independen dan periodik memberikan pandangan serta rekomendasi ke depan terkait dengan strategi manajemen dan operasional ID-SIRTII.

Tim Ahli ini dibagi menjadi tiga kelompok, masing-masing bertanggung jawab terhadap tiga aspek penting, yaitu: kelembagaan dan kebijakan, hukum dan perundang-undangan, serta teknis dan operasional. Agar ID-SIRTII dapat berjalan seperti yang diharapkan oleh seluruh pemangku kepentingan terkait dengannya, maka disusunlah standar *Key Performance Indicators* yang dipergunakan sebagai acuan ukuran kinerja keberhasilan organisasi. Untuk itulah maka selain Tim Ahli, dibentuk pula sebuah Tim Pengawas yang berfungsi untuk memonitor, menilai, dan mengevaluasi hasil kerja ID-SIRTII secara umum.

Topologi Teknologi Pendukung

Secara prinsip, hampir semua model teknologi *monitoring* yang dilakukan oleh berbagai lembaga CERT/CSIRT di dunia kurang lebih sama. Kuncinya terletak pada peletakan perangkat

sensor di titik-titik utama dimana nadi lalu lintas internet berada. Melalui sensor yang ada dapat diperoleh seluruh data yang diinginkan untuk dianalisa karakteristik dan polanya. Secara topologis, sensor-sensor yang tersebar di berbagai ISP, NAP, maupun IX tersebut dihubungkan secara terpusat ke pusat data dan *monitoring* ID-SIRTII - atau yang lebih dikenal sebagai "monitoring room". Di sinilah proses pemantauan dan analisanya dilakukan setiap hari tanpa henti. Jika terlihat terdapat hal-hal yang mencurigakan, setelah melalui proses analisa secara cepat dan cermat, maka ID-SIRTII langsung memberikan *early warning signal* kepada pihak-pihak terkait dengan *incident* yang diperkirakan akan dan/atau sedang terjadi. Pada awal pendiriannya, ID-SIRTII bekerjasama dengan *stakeholder* terkait telah memasang sembilan buah sensor di tempat-tempat utama, dimana kurang lebih 80% dari mayoritas trafik internet terjadi. Untuk sementara ini kesembilan sensor tersebut dianggap telah cukup memadai untuk melakukan pemantauan yang memberikan nilai tambah bagi pemangku kepentingan yang ada.



Perangkat Aplikasi Penunjang

Melihat betapa tinggi dan besarnya frekuensi serta volume interaksi yang terjadi di internet sehari-hari, maka proses pemantauan dan analisa harus dilakukan melalui bantuan aplikasi penunjang. Dalam hal ini ID-SIRTII memiliki pula sejumlah aplikasi pendukung atau penunjang proses pemantauan serta analisa tren dari pola trafik yang dipantau tersebut. Secara fungsional,

melalui kapabilitas yang dimiliki oleh perangkat aplikasi terkait, rangkaian proses yang dilakukan oleh ID-SIRTII menyangkut tiga hal (atau yang dikenal sebagai 3D). Pertama adalah *detect*, sebuah proses dimana melalui pemantauan diketemukan suatu pola trafik yang tidak biasaa - alias menyimpang atau anomali dari kondisi normalnya. Kedua adalah *determine*, yaitu sebuah rangkaian proses analisa untuk menentukan apakah pola trafik yang tidak biasa itu adalah merupakan atau berpotensi menjadi sebuah *incident* yang dapat mengganggu kerja sistem. Dan ketiga, *defend*, yaitu suatu proses reaktif (maupun prefentif) dengan cara memberikan *early warning system* kepada pihak-pihak yang terlibat dan memberitahukan cara paling efekif untuk melakukan perlindungan terhadap *incident* tersebut.

Filosofi Kerja dan Keberadaan Institusi

Terlepas dari berbagai peranan, fungsi, misi, dan manfaat dari adanya lembaga-lembaga semacam CERT/CSIRT, bagi negara-negara berkembang, yang komunitas "internet underground"-nya sangat aktif dan intensif berkomunikasi satu dan lainnya, kehadiran lembaga semacam ID-SIRTII kerap disambut secara skeptis dan berhati-hati. Melihat kenyataan bahwa lembaga-lembaga ini kebanyakan didanai oleh pemerintah, seringkali dianggap sebagai kaki tangan atau perpanjangan dari pemegang otoritas dalam memantau terjadinya pergerakan-pergerakan ilegal di dunia maya. Khusus di Indonesia, ID-SIRTII tidak memiliki tugas, misi, maupun wewenang untuk melakukan hal tersebut. Hak dan kewajibannya, sebagai lembaga publik, tidak boleh keluar dari ketujuh tugas pokok yang telah dicanangkan dan dijelaskan sebelumnya. Oleh karena itulah maka visi yang dicanangkan pun jelas, yaitu "menciptakan lingkungan dunia maya yang aman dan kondusif". Demikian pula dengan misi yang diemban, yaitu selaras dan sejalan dengan ketujuh tugas pokok yang telah dipaparkan pada Peraturan Menteri terkait.