KEAMANAN
INFORMASI DAN INTERNET

Seri Bunga Rampai Pemikiran EKOJI

PREINEXUS™
SHARING • COLLABORATION • NETWORK

Prof. Richardus Eko Indrajit

KEAMANAN INFORMASI DAN INTERNET

Seri Bunga Rampai Pemikiran EKOJI

KEAMANAN INFORMASI DAN INTERNET; Seri Bunga Rampai Pemikiran EKOJI, *oleh Prof. Richardus Eko Indrajit*

PREINEXUS™

Ruko Jambusari 7A Yogyakarta 55283
Telp: 0274-889398; E-mail: info@preinexus.com

ISBN:

Cetakan Pertama, tahun 2016

Semua informasi tentang buku ini, silahkan scan QR Code di cover belakang buku ini

PENGANTAR BADAN NASIONAL SERTIFIKASI PROFESI (BNSP)

Indonesia telah memasuki era Masyarakat Ekonomi ASEAN. Suatu masa dimana lalu lintas pergerakan sumber daya manusia di antara negara-negara anggota ASEAN terjadi secara bebas tanpa ada hambatan apapun. Situasi ini dapat dipandang sebagai peluang sekaligus tantangan (ancaman) bagi mereka yang berada dalam arena perdagangan bebas di wilayah Asia Tenggara ini.

Dalam menghadapi kondisi tersebut, tidak dapat dipungkiri lagi bahwa keberadaan sumber daya manusia berkualitas menjadi kunci daya saing suatu bangsa. Adalah merupakan suatu kenischayaan bahwa di era global saat ini, industri tidak hanya membutuhkan individu yang ahli dan kompeten di bidangnya, namun lebih jauh lagi mengharapkan kehadiran para profesional yang memiliki beragam kualifikasi. Kehadiran konsep National Qualification Framework di negara-negara ASEAN adalah merupakan jawaban terhadap kebutuhan ini.

Selaku institusi yang diberikan tugas dan tanggung jawab oleh negara untuk menyelenggarakan proses sertifikasi secara nasional, Badan Nasional Sertifikasi Profesi (BNSP) melihat pentingnya peranan lembaga pendidikan seperti perguruan tinggi dalam mempersiapkan sumber daya manusia Indonesia yang kompeten. Dalam konteks ini, sudah saatnya bagi kampus-kampus di tanah air untuk menata dan menyesuaikan kurikulum pendidikannya agar benar-benar relevan dengan kebutuhan dan dinamika perkembangan industri global.

Implementasi Kurikulum Berbasis Kompetensi yang berorientasi pada Kerangka Kualifikasi Nasional Indonesia (KKNI) membutuhkan buku referensi yang dikembangkan berdasarkan beragam standar “de jure” dan “de facto” yang dikenal dunia kerja (industri) – baik yang bersumber dari Standar Kompetensi Kerja Nasional Indonesia (SKKNI) maupun sumber-sumber lainnya (standar internasional dan standar khusus). Dalam khasanah ilmu pengetahuan, keberadaan buku semacam

ini sangatlah terbatas, terutama yang berbahasa Indonesia. Oleh karena itulah maka kami menyambut baik kehadiran karya ini, karena merupakan sebuah modul pembelajaran yang disusun berdasarkan sejumlah standar kompetensi yang dikenal industri.

Kami berharap di masa mendatang akan semakin banyak disusun dan diterbitkan buku semacam ini, agar lulusan perguruan tinggi di Indonesia benar-benar menjadi seorang profesional yang pengetahuan dan kompetensinya diakui oleh praktisi industri.

t.t.d.

Ir. Sumarna Abdurrahman

Ketua Badan Nasional Sertifikasi Profesi

PENGANTAR BADAN STANDAR NASIONAL PENDIDIKAN (BSNP)

Salah satu butir penting yang termaktub dalam Standar Nasional Pendidikan Tinggi di Indonesia yang disusun dan dikembangkan oleh Badan Standar Nasioanal Pendidikan (BSNP) adalah perlunya kampus mengembangkan dan mengadopsi model kurikulum yang berorientasi dengan Kerangka Kualifikasi Nasional Indonesia (KKNI). Hal ini didasarkan pada rpinsip perlunya seorang lulusan perguran tinggi untuk memiliki kualifikasi yang dikenal dan diakui oleh industri. Kualifikasi ini akan melengkapi bekal kompetensi yang telah dimiliki lulusan perguruan tinggi agar dapat bersaing secara profesional di era globalisasi.

Sesuai dengan delapan domain Standar Nasional Pendidikan yang ada – yaitu standar kompetensi lulusan, standar proses, standar isi, standar pendidik dan tenaga kependidikan, standar sarana prasarana, standar pengelolaan, standar penilaian, dan standar biaya – pengembangan kurikulum perguruan tinggi harus dilakukan secara komprehensif. Artinya adalah bahwa seluruh entitas pendukung pelaksanaan kurikulum dan penerapan standar nasional tersebut harus tersedia.

Buku teks pelajaran merupakan salah satu media pembelajaran pendukung yang sangat dibutuhkan oleh tenaga pendidik (dosen/infrastruktur) maupun peserta didik agar dapat melakukan proses pembelajaran yang bermuara pada terpenuhinya capaian pembelajaran yang telah ditetapkan. Tentu saja capaian pembelajaran yang didefinisikan tersebut haruslah disesuaikan dengan kebutuhan dunia industri tempat lulusan perguruan tinggi tersebut akan bekerja dan berkarir.

Kehadiran seri buku yang dikembangkan dengan berbasis pada Kerangka Kualifikasi Nasional Indonesia dan mengacu pada Standar Kualifikasi Kerja Nasional Indonesia (SKKNI) serta standar lain yang dikenal di dunia ini patut disambut dengan gembira, di tengah-tengah terbatasnya keberaaan buku referensi berbasis kompetensi yang berbahasa Indonesia. Karya ini selain memperkaya khasanah

dan koleksi ilmu pengetahuan di tanah air, diharapkan dapat dijadikan pedoman sekaligus pegangan dalam melakukan kegiatan pembelajaran di perguruan tinggi.

Mudah-mudahan di kemudian hari akan semakin banyak dijumpai karya-karya serupa yang dapat memberikan kontribusi positif dan signifikan bagi perkembangan kualitas pendidikan di Indonesia.

t.t.d.

Prof. Zainal A. Hasibuan

Ketua Badan Standar Nasional Pendidikan

SERIMODUL DIGITAL MULTIMEDIA PREINEXUS

Selain Seri Buku Preinexus, dikembangkan pula Seri Modul Digital Multimedia Preinexus untuk membantu mereka yang ingin mempelajari konten buku ini dalam bentuk format digital multimedia. Modul ini dapat dinikmati dalam berbagai format standar, seperti HTML 5 (dapat dipergunakan secara bebas di notebook, tablet, dan handphone) maupun SCORM (diintegrasikan dengan berbagai Learning Management System yang ada).

DAFTAR ISI

-oo0oo-

PENDAHULUAN

Sudah bukan merupakan rahasia lagi bahwa internet dan teknologi informasi telah memberikan begitu banyak manfaat signifikan bagi kehidupan manusia. Beragam aplikasi teknologi yang diterapkan di tengah-tengah masyarakat telah merubah cara orang berfikir, berperilaku, dan bertindak dalam kehidupan sehari- hari. Dampak dari penerapan teknologi ini begitu terasa di berbagai sektor kehidupan masyarakat, seperti pemerintahan, ekonomi, politik, sosial budaya, ideologi, dan lain sebagainya.

Seperti sebuah mata uang dengan dua sisi, selain sisi manfaat yang ditawarkan, terdapat pula sisi risiko yang dapak memberikan dampak negatif jika tidak dikelola dengan baik. Misalnya adalah penggunaan internet untuk menyebarkan faham terorisme, pornografi, perjudian, penyelundupan, pencurian, dan lain sebagainya – merupakan kenyataan sehari-hari yang frekuensinya semakin tinggi terjadi di dunia siber. Jenis risiko berikutnya adalah kejahatan yang dilakukan oleh kriminal sehingga menyebabkan berbagai teknologi dari berbagai instansi terganggu operasionalnya, seperti yang sering menimpa bank, portal informasi, website pemerintah, situs e-commerce, dan lain sebagainya.

Mempelajari mengenai isu keamanan informasi dan internet haruslah dengan menggunakan pendekatan komprehensif, holistik, dan sistemik. Alasannya adalah karena dalam ekosistem internet, terdapat begitu banyak komponen yang antar satu dan lainnya terkait. Konsep keamanan menekankan pada prinsip bahwa semakin banyak titik-titik atau entitas-entitas yang saling terkoneksi, akan semakin meningkatkan risiko kerawanan sistem. Dalam konteks inilah maka para praktisi internet harus memiliki pemahaman yang baik mengenai fenomena keamanan ini dengan tujuan menerapkan strategi yang efektif untuk memperlancar usaha bisnis elektroniknya.

Sebagai catatan akhir perlu dipahami bahwa isu keamanan merupakan paradoks dari manfaat yang diperoleh dengan adanya sistem dan teknologi informasi. Keberadaannya tidak dapat dihilangkan namun dapat dikelola secara sungguh-sungguh sebagai bagian dari mitigasi risiko bisnis.

CAPAIAN PEMBELAJARAN

- Menjelaskan mengenai fenomena keamanan dalam dunia siber secara holistik dan sistemik.
- Menguraikan tugas utama dari CSIRT/CERT yang dimiliki oleh sebuah negara.
- Menggambarkan berbagai ancaman keamanan yang ada di dunia siber.
- Mengidentifikasi beragam kelemahan yang ada dalam sebuah sistem informasi atau aplikasi berbasis internet.
- Memaparkan berbagai jenis serangan yang terjadi di dunia siber dan karakterisitk dari masing-masing serangan tersebut.
- Meranang model dan mekanisme keamanan yang perlu dibangun serta dikembangkan oleh perusahaan.
- Menerapkan berbagai pasal undang-undang dan peraturan yang terkait dengan permasalahan keamanan di dunia siber (cyberlaw).
- Mengoperasikan beberapa aplikasi untuk mengelola keamanan internet.

~ 1 ~

CYBER 6: FENOMENA KEAMANAN INFORMASI DALAM DUNIA SIBER

Capaian Pembelajaran (*Learning Outcomes)*:

1. Capaian Pembelajaran (*Learning Outcomes*):
2. Menggambarkan Ekosistem Cyber Space
3. Mendeteksi Keberadaan Cyber Threat
4. Mengantisipasi Fenomena Cyber Attack
5. Mempersiapkan Aspek Cyber Security
6. Mendeteksi Potensi Cyber Crime
7. Menerapkan Cyber Law

1.1 MENGGAMBARKAN EKOSISTEM CYBER SPACE

Internet telah menjadi bagian tak terpisahkan dari masyarakat moderen dewasa ini. Bahkan bagi generasi yang lahir setelah tahun 1995, internet telah membentuk sebuah dunia tersendiri seperti layaknya bumi di tempat manusia berada. Dalam dunia maya ini, melalui beraneka ragam peralatan teknologi informasi dan komunikasi, para individu maupun kelompok-kelompok masyarakat saling berinteraksi, bertukar pikiran, dan berkolaborasi untuk melakukan sejumlah aktivitas kehidupan. Dunia yang merupakan titik singgung antara dunia fisik dan dunia abstraksi ini[1] semakin lama semakin banyak pengunjungnya. Statistik terakhir memperlihatkan bahwa penetrasi internet pada tahun 2008 telah mencapai kurang lebih 21% dari total 6,676 milyar penduduk bumi. Artinya adalah bahwa satu dari lima individu di dunia ini adalah pengguna internet (baca: *internet user*).

WORLD INTERNET USAGE AND POPULATION STATISTICS

World Regions	Population (2008 Est.)	Population % of World	Internet Usage, Latest Data	% Population (Penetration)	Usage % of World	Usage Growth 2000-2008
Africa	955,206,348	14.3 %	51,022,400	5.3 %	3.6 %	1030.2 %
Asia	3,776,181,949	56.6 %	529,701,704	14.0 %	37.6 %	363.4 %
Europe	800,401,065	12.0 %	382,005,271	47.7 %	27.1 %	263.5 %
Middle East	197,090,443	3.0 %	41,939,200	21.3 %	3.0 %	1176.8 %
North America	337,167,248	5.1 %	246,402,574	73.1 %	17.5 %	127.9 %
Latin America/Caribbean	576,091,673	8.6 %	137,300,309	23.8 %	9.8 %	659.9 %
Oceania / Australia	33,981,562	0.5 %	19,353,462	57.0 %	1.4 %	154.0 %
WORLD TOTAL	6,676,120,288	100.0 %	1,407,724,920	21.1 %	100.0 %	290.0 %

Gambar 1.1 *Estimasi Profil Pengguna Internet di Lima Benua Tahun 2008*

Dibandingkan dengan penetrasi teknologi lainnya dalam sejarah manusia, penetrasi internet merupakan yang paling cepat, karena digambarkan dalam sebuah grafik pertumbuhan yang eksponensial. Pada saat yang sama disinyalir terjadi milyaran transaksi per hari dengan nilai transaksi mencapai milyaran dolar Amerika per detiknya – terjadi tanpa henti selama 24 jam sehari dan 7 hari seminggu. Suatu frekuensi dan volume perdangangan yang belum pernah sebelumya terjadi dalam sejarah kehidupan manusia. Semua fakta ini mengandung arti bahwa domain "pasar" yang terbentuk di internet memiliki nilai atau *value* yang sedemikian tingginya, karena lambat laun semakin banyak transaksi dan interaksi yang terjadi di sana. Bahkan sejumlah sumber mensinyalir, dalam waktu yang tidak lama lagi, nilai perdagangan di internet akan menjadi jauh lebih besar daripada yang terjadi di dunia nyata. Singkat kata, internet merupakan sebuah entitas yang

1 Istilah ini pertama kali diperkenalkan oleh Basuki Yusuf Iskandar (Direktur Jenderal Pos dan Telekomunikasi), ketika mencoba menggambarkan karakteristik dari dunia maya, yang merupakan domain kehidupan antara dunia nyata (bumi tempat manusia berpijak) dan dunia abstrak (panggung sandiwara teater dan sejenisnya).

tidak ternilai harganya – yang dari masa ke masa, akan semakin meningkat harga dan nilainya, karena semakin banyak aktivitas yang terjadi di sana.

1.2 MENDETEKSI KEBERADAAN CYBER THREAT

Sebagaimana adanya sebuah benda berharga, pasti diiringi pula dengan banyaknya pihak yang tertarik untuk "memilikinya". Perhiasan misalnya, sering kali diburu orang untuk dijadikan milik karena nilainya yang makin lama makin meningkat (baca: investasi berharga). Namun ada pula pihak-pihak yang ingin memilikinya dengan cara-cara yang jahat, seperti ingin mencurinya, merampok, bahkan merebutnya dari kepemilikan yang sah. Demikian pula hal yang sama menimpa internet. Semakin bertambah nilai dunia maya ini, semakin banyak pula ancaman yang menyertainya[2].

Ancaman pertama berupa keinginan sejumlah atau sekelompok orang maupun pihak yang ingin mengambil beraneka ragam harta atau barang berharga yang ditransaksikan atau dipertukarkan di internet. Mulai dari hal-hal yang secara langsung merepresentasikan sumber daya finansial, seperti uang digital, nilai kartu debit, kekayaan di rekening bank, jumlah tagihan kartu kredit, dan lain sebagainya – hingga entitas *intangible* yang memiliki nilai strategis tertentu seperti data intelijen, *password* rekening bank, informasi rahasia konsumen, dan lain-lain.

Ancaman kedua berupa niat orang-orang jahat tersebut untuk membuat agar internet tidak berfungsi secara normal, atau dengan kata lain mencoba membuat terjadinya mal fungsi pada internet. Harapannya adalah agar terjadi gangguan pada proses transaksi perdagangan, aktivitas akses informasi, prosedur administrasi pemerintahan, dan lain sebagainya. Karena semakin banyak aspek kehidupan yang tergantung pada internet, maka gangguan ini dapat mengakibatkan terjadinya *chaos* yang berkepanjangan.

Ancaman ketiga berupa usaha melakukan modifikasi terhadap data atau informasi yang mengalir di internet demi tujuan-tujuan destruktif, seperti memfitnah, menyesatkan, mengadu domba, menghancurkan citra, menipu, dan lain-lain. Bagi bangsa-bangsa yang secara fisik maupun ideologis masih berperang, cara-cara tersebut di atas merupakan aktivitas "perang" sehari-hari yang dapat terjadi di dunia maya.

2 Pernyataan ini sering diistilahkan oleh berbagai praktisi dan kalangan akademik sebagai sebuah paradoks dalam perkembangan internet.

Ancaman keempat berupa kehendak individu untuk menyebarkan hal-hal yang keliru ke seluruh penduduk di dunia, seperti: faham-faham yang menyesatkan, citra dan media pornografi, informasi pendukung tindakan terorisme, tawaran aktivitas perjudian, cara-cara melakukan kejahatan terselubung, dan lain sebagainya.

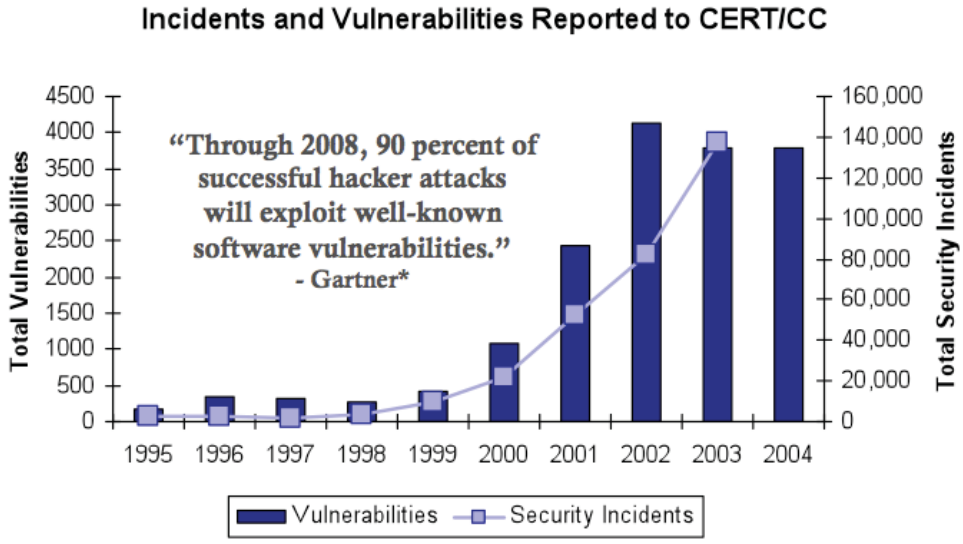
Ancaman kelima atau terakhir berupa penyebaran dan penanaman program-program jahat (baca: *malicious software*) ke komputer-komputer yang terhubung ke internet dengan tujuan yang berane-ragam, mulai dari yang bersifat non-destruktif - seperti adanya tampilan yang tidak diiginkan, mengacaukan fungsi huruf pada papan tekan (baca: *keyboard*), tidak bekerjanya peralatan input-output, dan lain-lain – hingga yang bersifat sangat destruktif, seperti menghapus isi pada *hard disk*, mengambil data tanpa sepengetahuan pemilik, memata-matai aktivitas pengguna, memacetkan komputer atau lebih dikenal dengan istilah "*hang*", menurunkan kinerja kecepatan prosesor, dan hal-hal lain yang sangat merugikan.

Informasi berikut memperlihatkan bagaimana mengerikannya ancaman yang ada di dunia maya saat ini. Sebagai contoh, ada sebuah situs yang menjual 29,000 alamat email individu dengan harga 5 dolar Amerika; sementara ada situs lain yang hanya dengan uang US$ 300 dapat memberikan informasi terkait dengan rekening bank individu yang memiliki uang di atas 100 juta rupiah; atau sebuah situs yang menawarkan jasa merusak situs (baca: *website*) dengan kisaran tarif tiga hingga lima dolar per situsnya.

Item	Advertised Price (in US Dollars)
United States-based credit card with card verification value	$1–$6
United Kingdom-based credit card with card verification value	$2–$12
An identity (including US bank account, credit card, date of birth, and government issued identification number)	$14–$18
List of 29,000 emails	$5
Online banking account with a $9,900 balance	$300
Yahoo Mail cookie exploit—advertised to facilitate full access when successful	$3
Valid Yahoo and Hotmail email cookies	$3
Compromised computer	$6–$20
Phishing Web site hosting—per site	$3–5
Verified PayPal account with balance (balance varies)	$50–$500
Unverified PayPal account with balance (balance varies)	$10–$50
Skype account	$12
World of Warcraft account—one month duration	$10

Gambar 1.2 *Ancaman Tindakan Kejahatan di Dunia Maya*

Keseluruhan ancaman atau *threat* ini merupakan hal yang wajar karena tingginya nilai internet seperti yang dijelaskan sebelumnya. Oleh karena itu, siapapun pengguna internet, hendaklah waspada dan berhati-hati terhadap resiko ancaman yang menyertainya.



Gambar 1.3 *Trend Lubang Kerawanan pada Perangkat Lunak*

Disamping itu, tidak ada teknologi informasi yang didesain secara sempurna sehingga bebas dari kerawanan (baca: *vulnerabilities*). Laporan dari berbagai lembaga riset dan pengawas internet[3] memperlihatkan bahwa kerawanan pada program aplikasi (baca: *software*) semakin lama semakin bertambah kuantitas dan kualitasnya. Hal ini sejalan dengan semakin banyak dan kompleksnya jumlah *incident* yang terjadi di dunia maya akibat eksploitasi terhadap kerawanan tersebut oleh pihak-pihak yang tidak bertanggung jawab[4]. Singkat kata, sejalan dengan bermanfaatnya aplikasi teknologi informasi bagi umat manusia, bertambah pula resiko intrinsik yang terkandung di dalamnya (baca: *embedded risk*). Melakukan mitigasi terhadap resiko tersebut – dalam arti kata mengurangi tingginya probabilitas terjadinya eksploitasi pada ancaman tersebut, atau paling tidak mengurangi dampak kerugian yang diakibatkan oleh *incident* yang tak terindahkan – merupakan hal bijaksana yang dapat dilakukan oleh semua orang.

1.3 MENGANTISIPASI FENOMENA CYBER ATTACK

Potensi ancaman seperti yang telah dijelaskan sebelumnya akan benar-benar menjadi masalah jika berhasil dieksploitasi oleh orang-orang jahat dalam rupa sebuah serangan[5]. Berdasarkan Konvensi Budapest[6], jenis serangan di dunia maya

3 Ada dua jenis lembaga utama di dunia ini yang bertugas mengawasi trafik internet yaitu model CSIRT (Computer Security Incident Response Team) dan CERT (Computer Emergency Response Team).

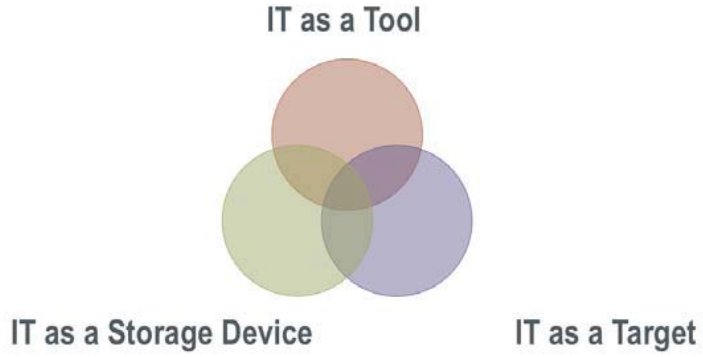
4 Diambil dari hasil penelitian Gartner (CIO Alert: Follow Gartner's Guidelines for Updating Security on Internet Servers, Reduce Risks by J. Pescatore, February 2003) dan data dari CERT/CC (No Longer Tracks Security Incident Statistics).

5 Patut dibedakan antara pengertian "ancaman" dan "serangan", dimana sebuah peristiwa baru dapat dikatakan sebuah serangan apabila pelaku kejahatan berhasil mengeksploitasi kelemahan-kelemahan sistem teknologi sehingga ancaman-ancaman yang ditakutkan telah benar-benar terjadi.

6 Hasil pertemuan para praktisi keamanan internet yang bersepakat untuk mengembangkan standar interoperabilitas penanganan kasus-kasus kejahatan dunia maya.

dapat dikategorikan menjadi tiga jenis. Kategori pertama adalah kumpulan jenis serangan dimana teknologi informasi dan komunikasi menjadi alat atau senjata utama untuk melakukan kejahatan. Contohnya adalah:

- Komputer dan internet dipergunakan sebagai alat dan medium untuk menyebarkan aliran-aliran sesat;
- Telpon genggam (baca: *handphone*) dimanfaatkan untuk mengirimkan pesan-pesan atau SMS yang menipu calon korban[7];
- *Electronic Mail* dipakai sebagai sarana untuk mengirimkan gambar-gambar atau video bernuansa pornografi; dan lain sebagainya.



Gambar 1.4 *Tiga Kategori Serangan Dunia Maya*

Kategori kedua adalah kumpulan peristiwa dimana komputer atau teknologi informasi menjadi sasaran pusat serangan dari pelaku tindak kejahatan, seperti:

- Melakukan transaksi keuangan fiktif dalam sebuah sistem perbankan berbasis internet (baca: *e-banking*);
- Mematikan atau memacetkan kerja sebuah jejaring internet (baca: *LAN* atau *WAN*) secara *remote*;
- Menyebarkan virus-virus untuk mengganggu kinerja komputer-komputer tertentu; dan lain sebagainya.

Adapun kategori jenis serangan ketiga ditujukan bagi peristiwa yang bertujuan utama untuk merusak (termasuk memodifikasi dan memfabrikasinya) data atau informasi yang tersimpan di dalam media perangkat teknologi informasi[8]. Serangan yang dimaksud antara lain:

- Merubah isi sebuah situs tanpa sepengetahuan pemiliknya;
- Mengambil kumpulan *password* atau informasi lengkap kartu kredit sekelompok individu untuk disalahgunakan atau diperjualbelikan;

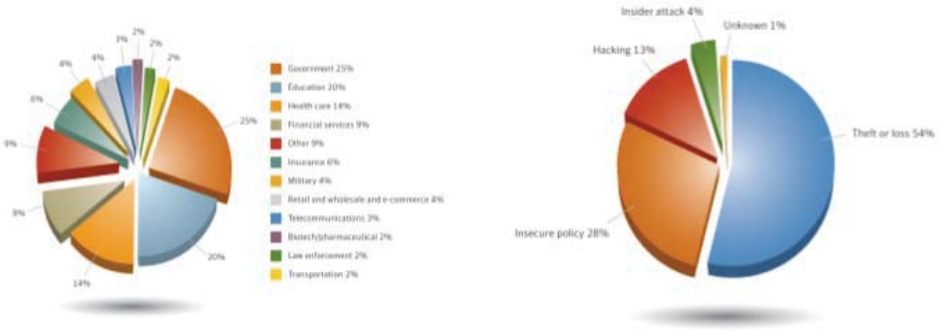
7 Kasus ini sangat banyak terjadi di tanah air, dan menimbulkan kerugian finansial yang cukup besar di pihak korban yang mempercayainya.

8 Data dan informasi menjadi sasaran utama karena merupakan entitas yang paling bernilai tinggi dalam suatu sistem informasi korporasi.

- Merusak sistem basis data utama sehingga semua informasi di dalamnya menjadi tidak dapat terbaca atau diakses secara normal; dan lain sebagainya.

Informasi berikut memperlihatkan *ranking* negara-negara tempat asalnya berbagai program-program pengrusak (baca: *malware*) yang bertujuan menyerang sistem komputer atau teknologi informasi di dunia maya.

Overall Rank	Country	Overall Proportion	Malicious Code Rank	Spam Host Rank	Command and Control Server Rank	Phishing Host Rank	Bot Rank	Attack Rank
1	United States	31%	1	1	1	1	2	1
2	China	10%	3	2	4	8	1	2
3	Germany	7%	7	3	3	2	4	3
4	France	4%	9	4	14	4	3	4
5	United Kingdom	4%	4	13	9	3	6	6
6	South Korea	4%	12	9	2	9	11	9
7	Canada	3%	5	23	5	7	10	5
8	Spain	3%	13	5	15	16	5	7
9	Taiwan	3%	8	11	6	6	7	11
10	Italy	3%	2	8	10	14	12	10

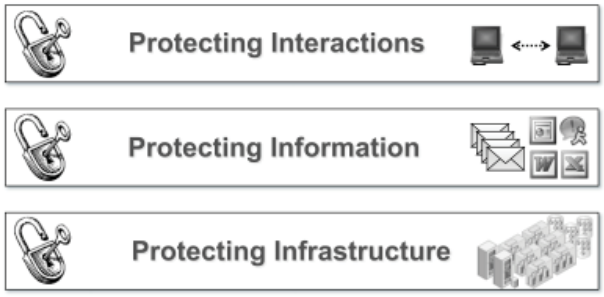


Gambar 1.5 *Profil Negara-Negara dengan Program Perusak Dunia Maya*

1.4 MEMPERSIAPKAN ASPEK CYBER SECURITY

Serangan yang cenderung bersifat destruktif tersebut sudah selayaknya harus ditangkal dan dihindari agar tidak merugikan banyak pihak. Oleh karena itu sejumlah usaha pengamanan harus dilakukan oleh mereka yang berkepentingan. Secara prinsip ada tiga cara utama untuk memproteksi diri. Cara pertama adalah memproteksi infrastruktur tempat mengalirnya data dan informasi dalam proses transmisi. Artinya adalah bahwa semua infrastruktur baik yang melalui darat (seperti *fiber optic*), laut (seperti kabel bawah laut), dan udara (seperti satelit), secara fisik maupun operasional harus dilindungi dan diproteksi dari beraneka ragam potensi gangguan yang mungkin timbul. Cara kedua adalah memproteksi data, informasi, atau konten yang ada dan/atau mengalir dalam sebuah sistem komunikasi dan teknologi informasi. Metode seperti penyandian atau kriptografi informasi merupakan salah satu cara umum dan ampuh untuk dilaksanakan oleh

para *stakeholder* teknologi informasi[9]. Dengan disandikannya atau diacaknya data maupun pesan elektronik tersebut, maka akan mempersulit para pencuri data untuk mengetahui isi sesungguhnya.



Gambar 1.6 *Profil Negara-Negara dengan Program Perusak Dunia Maya*

Cara ketiga adalah melakukan proteksi terhadap komponen-komponen terkait dengan proses interaksi. Mulai dari pemilihan jenis media dan perangkat lunak komunikasi *email, chatting, browsing, blogging,* dan lain sebagainya – hingga melakukan *setting* konfigurasi program agar keamanan proses interaksi dapat terjamin dari ancaman. Khusus untuk interaksi yang melibatkan transaksi keuangan misalnya, perlu ditambahkan mekanisme standar pengaman dan prosedur khusus agar tidak terjadi kebocoran dan pencurian data keuangan. Proteksi yang dimaksud, seperti telah disampaikan sebelumnya, adalah dalam rangka mengimplementasikan manajemen resiko atau yang kerap dikatakan sebagai *risk mitigation*[10].

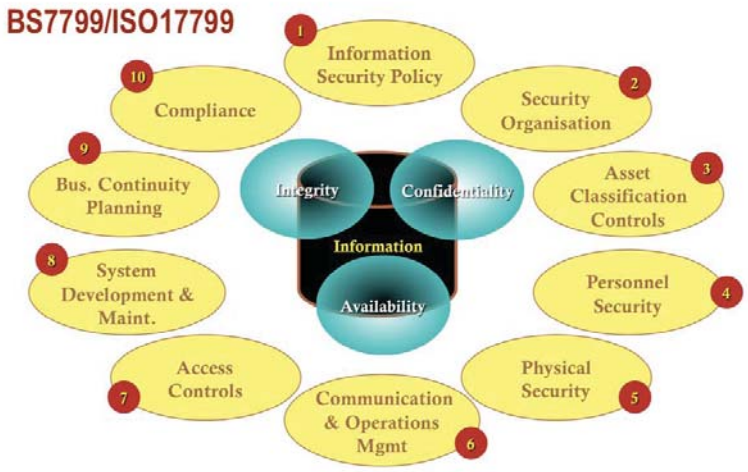
Gambar 1.7 *Kerangka Pemikiran Manajemen Resiko*

9 Di Indonesia terdapat Lembaga Sandi Negara yang memiliki tugas dan kompetensi handal dalam bidang kriptografi dan teknik persandian.

10 Kerangka umum yang kerap dipergunakan oleh para praktisi dan akademisi manajemen resiko sistem informasi, diperkenalkan pertama kali oleh the International Standard Organisation (ISO).

Dalam kerangka ini terlihat secara jelas, bahwa keberhasilan eksploitasi pada kerawanan teknologi informasi akan mengurangi nilai aset informasi yang dimiliki perusahaan, yang jika tidak diproteksi dengan sistem pengamanan yang memadai serta manajemen kendali yang efektif (baca: kontrol)akan berdampak serius terhadap organisasi terkait.

Banyak orang bertanya-tanya mengenai hal-hal apa saja yang harus diperhatikan dalam rangka mengembangkan sebuah sistem pengamanan yang efektif dan menyeluruh. Standar internasional BS7799/ISO17799 menekankan perlunya memperhatikan 10 (sepuluh) aspek utama untuk memperoleh sistem keamanan yang utuh, holistik, dan menyeluruh. Yang menarik dari standar ini adalah diperhatikannya pula aspek keamanan dalam dunia nyata, dimana perilaku dan pengetahuan sumber daya manusia menjadi aspek utama yang perlu untuk diperhatikan.



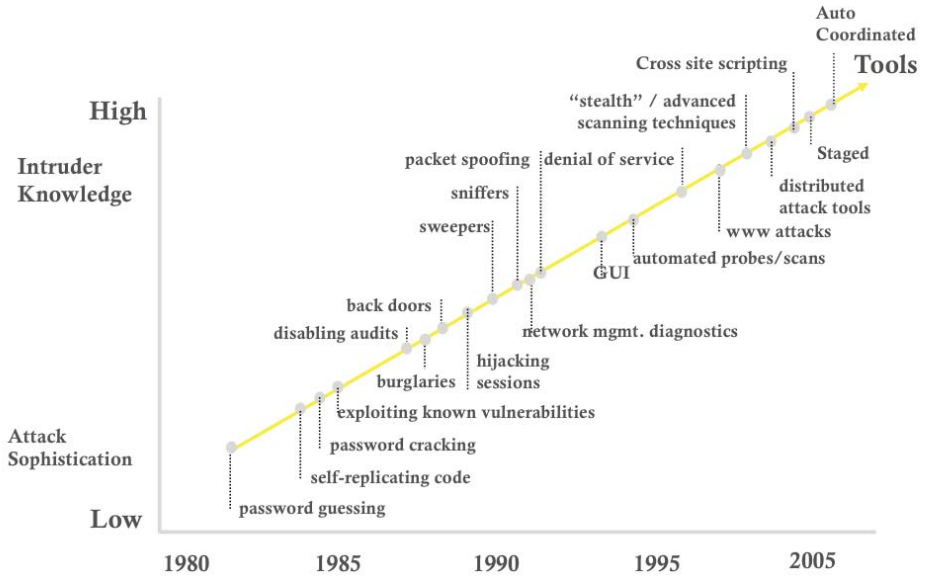
Gambar 1.8 *Sepuluh Domain Standar Keamanan Informasi*

1.5 MENDETEKSI POTENSI CYBER CRIME

Sejalan dengan kemajuan teknologi komunikasi dan informasi, semakin kompleks pula jenis serangan yang terjadi di dunia maya. Jika dahulu diperkenalkan istilah *hacker*dan *cracker* yang menunjuk pada individu dengan kemampuan dan aktivitas khusus memasuki sistem komputer lain untuk beraneka ragam tujuan, maka saat ini sudah banyak diciptakan mesin atau sistem yang dapat bekerja sendiri secara intelijen untuk melakukan teknik-teknik penyusupan dan perusakan sistem[11]. Intinya adalah bahwa serangan terhadap sistem keamanan teknologi informasi organisasi telah masuk pada kategori kriminal, baik yang bersifat pidana maupun

11 Misalnya fenomena botnet atau robot network yang menjadi bahan percakapan dan penelitian dewasa ini.

perdata. Walaupun kebanyakan jenis tindakan kriminal tersebut berkaitan erat dengan urusan finansial, tidak jarang akibat serangan tersebut, sejumlah nyawa manusia melayang, karena menimpa sistem yang sangat vital bagi kehidupan manusia[12]. Ilustrasi berikut memperlihatkan begitu banyaknya jenis tindakan atau serangan yang mengarah pada kriminalisasi dari tahun ke tahun.



Gambar 1.9 *Jenis-jenis Serangan yang Mengarah pada Kriminalisasi*

Terlepas dari semakin beraneka ragamnya jenis serangan yang ada, secara prinsip terdapat 4 (empat) jenis aktivitas yang kerap dikategorisasikan sebagai tindakan kriminal dalam dunia teknologi informasi. Pertama adalah *interception*, yaitu tindakan menyadap transmisi yang terjadi antara satu pihak dengan pihak yang lain. Seperti diketahui, di Indonesia misalnya, hanya sejumlah lembaga yang memiliki hak untuk melakukan penyadapan atau intersepsi, seperti Kepolisian Republik Indonesia, Badan Intelijen Nasional, dan Komisi Pemberantasan Korupsi. Individu atau organisasi yang tidak memiliki wewenang untuk melakukan hal tersebut dapat diadili jika melakukan tindakan terkait dengan penyadapan. Kedua adalah *interruption*, yaitu tindakan yang mengakibatkan terjadinya pemutusan komunikasi antara dua buah pihak yang seharusnya berinteraksi. Fenomena *Denial of Services (DoS)* atau *Distributed Denial of Services (DDoS)* merupakan salah satu serangan yang dapat mengakibatkan terjadinya kondisi interupsi pada sistem komputer. Ketiga adalah *modification*, yaitu tindakan melakukan perubahan terhadap data atau informasi atau konten yang mengalir dalam sebuah infrastruktur

12 Sering disebut sebagai critical infrastructure(jaringan listrik, radar bandara udara, sistem peluru kendali, jaringan perbankan, dan lain sebagainya), karena jika terjadi gangguan pada sistem tersebut, dapat mengakibatkan incident yang membahayakan kehidupan manusia.

teknologi informasi tanpa sepengetahuan yang mengirimkan/menerimanya. *Web defacement*merupakan salah satu jenis serangan yang bisa dikategorikan dalam kelas ini. Dan yang keempat adalah *fabrication*, yaitu tindakan mengelabui seolah-olah terjadi suatu permintaan interaksi dari seseorang seperti yang dewasa ini dikenal dengan istiliah *phishing*.

Studi mendalam mengenai tindakan kriminal di dunia maya memperlihatkan berbagai motif atau alasan seseorang melakukannya, mulai dari mencari sensasi semata hingga dibiayai oleh sekelompok sponsor teroris internasional. Hampir seluruh negara melaporkan bahwa tindakan kriminal di dunia maya menunjukkan pertumbuhan yang semakin signifikan, baik dilihat dari sisi kuantitas maupun kualitasnya.

Gambar 1.10 *Motif Tindakan Kriminal di Dunia Maya*

1.6 MENERAPKAN CYBER LAW

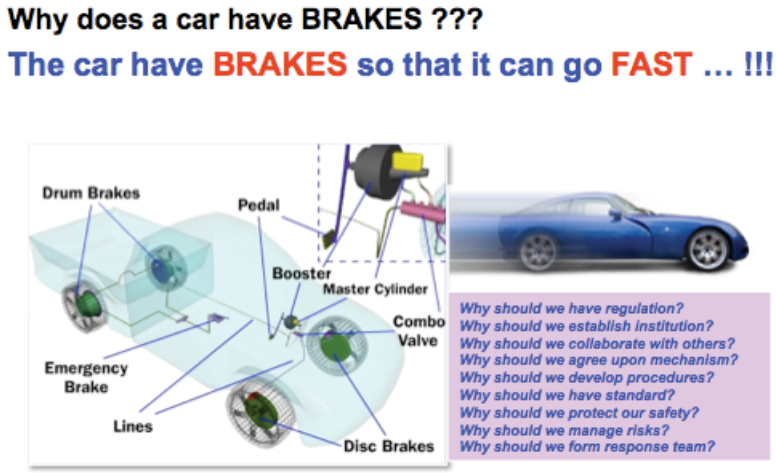
Pada akhirnya, *cyber security* semata tidak dapat mencegah terjadinya motif kriminal di dunia maya, perlu perangkat lain yang lebih canggih dan efektif. Dalam kaitan inilah maka beberapa negara mulai menyusun dan memberlakukan undang-undang dunia maya (baca: *cyber law*). Dalam undang-undang ini biasanya disusun berbagai jenis klasifikasi dan ancaman hukuman terhadap beraneka ragam tindakan kriminal terkait dengan dunia komputer dan/atau teknologi informasi. Walaupun relatif terlambat dibandingkan dengan negara lain, pada akhirnya Indonesia memiliki undang-undang *cyber law*pertamanya yang disusun oleh Departemen Komunikasi dan Informatika dan disetujui oleh Dewan Perwakilan Rakyat untuk mulai diundangkan semenjak tanggal 25 Maret 2008. Undang-undang no.11 tahun 2008 ini dikenal dengan nama Undang-Undang ITE atau Undang-Undang Informasi dan Transaksi Elektronik. Dengan diberlakukannya undang-undang ini, maka berbagai jenis tindakan kriminal di dunia maya dapat dikenakan sanksi tegas secara perdata maupun pidana[12].

12 Menurut undang-undang tersebut, seseorang yang terbukti melakukan kejahatan di dunia maya dapat didenda uang sebesar 600 juta hingga 12 milyar rupiah atau dihukum penjara antara 6 hingga 12 tahun.

Terlepas dari telah berlakunya undang-undang tersebut, hal yang merupakan tantangan utama adalah implementasinya. Terutama dilihat dari kesiapan sumber daya penegak hukumnya. Sistem hukum di Indonesia menuntut agar polisi, jaksa, pengacara, dan hakim dipersenjatai dengan pengetahuan yang cukup di bidang teknologi informasi agar dapat menghadapi beraneka ragam jenis kasus kriminal di dunia maya. Belum lagi terhitung diperlukannya para saksi ahli di bidang teknologi informasi yang memiliki pengetahuan, kemampuan, kompetensi, dan keahlian terkait dengan keamanan komputer, pengamanan data, forensik alat bukti digital, dan lain sebagainya.

Disamping sumber daya manusia, dibutuhkan pula sejumlah laboratorium dan pusat penelitian di bidang teknologi informasi untuk membantu para penegak hukum dalam menjalankan tugasnya. Keberadaan *Cyber Crime Unit* di Mabes Polri dan *ID-SIRTII* misalnya, dapat membantu para penegak hukum di Indonesia dalam usahanya untuk melindungi dunia maya dari tangan-tangan jahat.

Pada akhirnya, paradoks antara semakin bernilainya internet akibat manfaat yang ditawarkan kepada khalayak dengan tingginya resiko yang menyertainya, harus dipecahkan dalam tataran filosofis atau pemikiran. Jika tidak, maka keberadaan *cyber security*dan *cyberlaw*misalnya, justru akan menjauhkan orang dari internet – yang tentu saja akan menjadi suatu usaha yang kontra produktif. Bagaimana cara melihat paradoks ini dari kacamata yang lain?



Gambar 1.11 *Perspektif Berbeda Terhadap Fungsi Cyber Security dan Cyber Law*

Jika seseorang ditanya, “apakah fungsi sebuah rem bagi kendaraan?” Jawabannya adalah bukan karena ingin agar mobil yang bersangkutan dapat berhenti, namun justru sebaliknya, yaitu agar supir dari mobil yang bersangkutan berani ngebut. Fungsi *cyber security* dan *cyber law*barulah akan efektif jika dengan

keberadaannya, justru jumlah pengguna internet di Indonesia meningkat secara signifikan, demikian juga dengan frekuensi dan volume interaksi di internet. Jika dengan keberadaan kedua perangkat tersebut justru membuat pertumbuhan internet menjadi stagnan, berarti banyak hal salah yang perlu untuk diperbaiki.

-oo0oo-

~ 2 ~

CSIRT/CERT: TIM PENGAWAS KEAMANAN INTERNET

Capaian Pembelajaran (*Learning Outcomes*):

1. Mendeteksi Masyarakat Dunia Maya
2. Mengidentifikasi Masalah Internet dan Lembaga Pengaman
3. Menjelaskan Kebutuhan Pendirian ID-SIRTII
4. Menjelaskan Ruang Lingkup Pengamanan Internet
5. Mengidentifikasi Konstituen ID-SIRTII
6. Menjelaskan Karakteristik Incident
7. Memetakan Ragam Incident Internet
8. Menyusun Strategi Prioritas Penanganan Incident
9. Memetakan Proses Inti dan Aktivitas Penunjang
10. Menformulasikan Struktur Tim Kerja
11. Merancang Topologi Teknologi Pendukung
12. Mempersiapkan Perangkat Aplikasi Penunjang
13. Menjelaskan Filosofi Kerja dan Keberadaan Institusi

2.1 MENDETEKSI 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.

2.2 MENGIDENTIFIKASI 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[1]. 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[2]. 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.

---

1 "Sengaja" seperti yang dilakukan oleh para hacker, cracker, terrorist, spy, dan sejenisnya; sementara "tidak sengaja" bisa disebabkan karena gangguan infrastruktur (akibat bencana alam) atau masalah teknologi lainnya (malfungsi).

2 Istilah CERT pada awalnya ditujukan pada tim pemadam kebakaran di Amerika Serikat karena kemiripan tugas dan tanggung jawabnya, yaitu singkatan dari Community Emergency Response Team.

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[3]. 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.

2.3 MENJELASKAN KEBUTUHAN 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[4]. 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 Direk-

3 Walaupun dibentuk oleh Carnegie Mellon University, CERT/CC yang didirikan bukan untuk mengelola keamanan perguruan tinggi yang bersangkutan, tetapi merupakan pusat koordinasi sejumlah CERT yang menjadi anggotanya.

4 Dalam dunia keamanan informasi obyek vital tersebut dinamakan sebagai "the critical infrastructure" karena peranan dan fungsinya yang sedemikian penting.

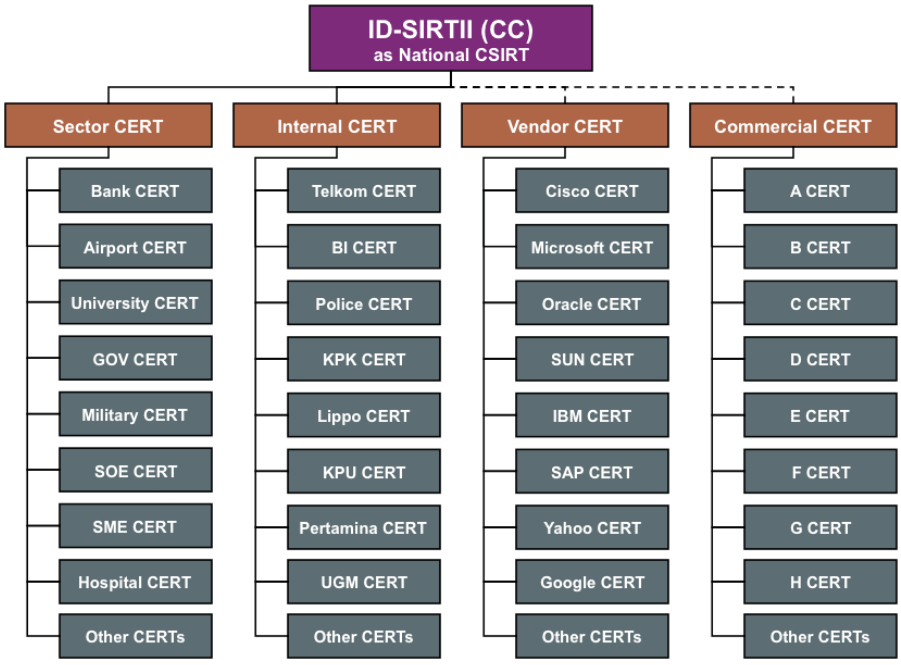
torat Jenderal Post dan Telekomunikasi Departemen Komunikasi dan Informatika Republik Indonesia – berjuang keras untuk membentuk lembaga CSIRT untuk tingkat nasional Indonesia. Akhirnya pada tahun 2007, melalui Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 26/PER/M.KOMINFO/5/2007 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 kegiatan 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.



Gambar 2.1 *Relasi antara ID-SIRTII dan CERT di Masa Mendatang*

2.4 MENJELASKAN 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.

INCIDENT HANDLING DOMAIN and ID-SIRTII MAIN TASKS	Reactive Services	Proactive Services	Security Quality Management Services
1. Monitoring traffic	Alerts and Warnings	Announcements Technology Watch Intrusion Detection Services	x
2. Managing log files	Artifact Handling	x	x
3. Educating public	x	x	Awareness Building
4. Assisting institutions	Security-Related Information Dissemnination Vulnerability Handling Intrusion Detection Services	Security Audit and Assessment Configuration and Maintenenace of Security Tools, Applications, and Infrastructure	Security Consulting
5. Provide training	x	X	Education Training
6. Running laboratory	x	x	Risk Analysis BCP and DRP
7. Establish collaborations	Incident Handling	x	Product Evaluation

Gambar 2.2 *Klasifikasi Ruang Lingkup Pengamanan Internet*

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.

2.5 MENGIDENTIFIKASI KONSTITUEN ID-SIRTII

Hampir 99% CERT/CSIRT di seluruh dunia dibangun pada mulanya melalui dana pemerintah[5], karena memang merekalah yang pertama kali merasa pentingnya lembaga tersebut[6]. Sejalan dengan perkembangannya, maka mulai tumbuhlah sejumlah CERT/CSIRT yang dikelola oleh swasta secara mandiri[7]. Oleh karena itulah maka, setiap lembaga CERT/CSIRT memiliki konstituennya masing-masing, karena perbedaan misi yang diembannya[8]. 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[9].

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)[10]; dan
- Beragam institusi dan/atau komunitas keamanan informasi dan internet di Indonesia lainnya[11].

---

5 Kecuali AusCERT (Australia) misalnya yang didanai secara patungan dan diselenggarakan serta dikelola oleh komunitas perguruan tinggi sebagai penyedia jasa bagi ISP dan pihak lain yang berkepentingan.

6 Terutama dalam kaitannya untuk menjaga obyek-obyek vital atau critical infrastructure seperti perusahaan listrik, pertambangan minyak dan gas bumi, perbankan, fasilitas militer, bandara udara, dan lain sebagainya.

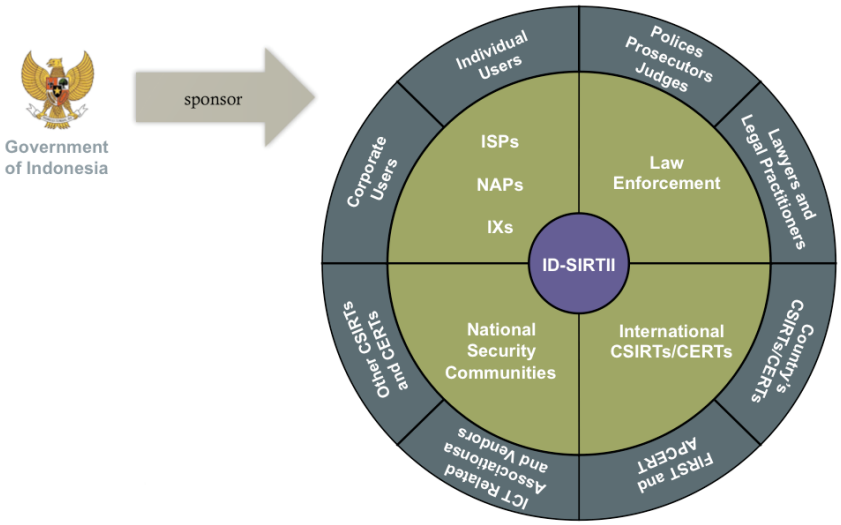
7 Jepang merupakan salah satu contoh negara dimana pertumbuhan jumlah lembaga CERT/CSIRT-nya tertinggi di dunia.

8 Misi dan tugas khusus yang dimaksud adalah portofolio dari fungsi-fungsi reaktif, preventif, dan peningkatan kualitas seperti yang telah dijelaskan sebelumnya.

9 Dikatakan sementara ini adalah karena pada waktunya nanti, kurang lebih 3-5 tahun ke depan, ID-SIRTII diharapkan dapat menjadi lembaga independen yang mandiri.

10 Negara-negara Asia yang sudah tergabung dalam APCERT antara lain: Malaysia, Jepang, Singapura, Australia, Thailand, Srilanka, Brunei, Filipina, Korea, China, Hongkong, dan India. Segera menyusul untuk bergabung adalah Indonesia, Vietnam, Kamboja, Laos, dan Myanmar.

11 Komunitas yang dimaksud seperti: KKI (Komunitas Keamanan Informasi), Lembaga Sandi Negara, Badan Intelijen Negara, ID-CERT (Indonesia CERT), dan lain-lain.



Gambar 2.3 *Kelompok Konstituen ID-SIRTII*

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.

2.6 MENJELASKAN 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.

2.7 MEMETAKAN 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[12] 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

12 Terjadi pada saat BCA meluncurkan internet banking-nya yang dikenal dengan situs www.klikbca.com.

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[13] 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.

2.8 MENYUSUN 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*[14]– 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*[15]).

13 Dipacu oleh kemarahan warga setempat akibat dipindahkannya patung Lenin, Estonia diserang botnet yang melumpuhkan seluruh sistem obyek vitalnya sehingga berakibat pada tidak berfungsinya utilitas penting seperti listrik dan sistem perbankan, yang menyebabkan kekacauan disana sini selama lebih dari satu minggu.

14 Empat klasifikasi jenis-jenis incident yang kerap dipergunakan oleh praktisi maupun akademisi keamanan informasi dan internet.

15 Istilah "many-to-one" berarti "banyak orang dikerahkan dan dialokasikan untuk menangani sebuah perkara".

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.

TYPE OF INCIDENT AND ITS PRIORITY	Public Safety and National Defense (Very Priority)	Economic Welfare (High Priority)	Political Matters (Medium Priority)	Social and Culture Threats (Low Priority)
1. Interception	Many to One	One to Many	Many to Many	Automated Tool (KM-Based Website)
2. Interruption	Many to One	One to Many	Many to Many	Automated Tool (KM-Based Website)
3. Modification	Many to One	One to Many	Many to Many	Automated Tool (KM-Based Website)
4. Fabrication	Many to One	One to Many	Many to Many	Automated Tool (KM-Based Website)

Gambar 2.4 *Tingkatan Prioritas Penanganan Incident*

Adapun prioritas ketiga adalah hubungan secara *many-to-one*, yaitu bagi 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[16].

2.9 MEMETAKAN 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

16 Demikianlah cara pandang ID-SIRTII terhadap fenomena semacam pornografi, child abuse, terorisme, dan lain sebagainya. Peralatan yang dimiliki oleh ID-SIRTII hanya dapat mengurangi probabilitas dan tingginya dampak yang terjadi, namun tidak dapat secara signifikan mengelimintasinya, karena fenomena tersebut memiliki dimensi sosial budaya yang kental.

trafik internet secara penuh 24/7[17] 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[18]. 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*[19] 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[20].

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"

17 24 jam sehari dan 7 hari dalam seminggu secara tidak berkesudahan.

18 Misalnya diberitahukan kepada ISP yang berpotensi menjadi "korban" incident atau yang dikhawatirkan dipergunakan kriminal sebagai "pusat" terjadinya incident.

19 Catatan elektronik dari sistem berupa rekaman data/informasi terkait dengan trafik internet yang terjadi pada durasi tertentu.

20 Pola seperti ini dikenal sebagai aktivitas "outsource" atau pengalihdayaan dari Dirjen Postel kepada ID-SIRTII selaku lembaga yang dibentuknya.

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[21].

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.

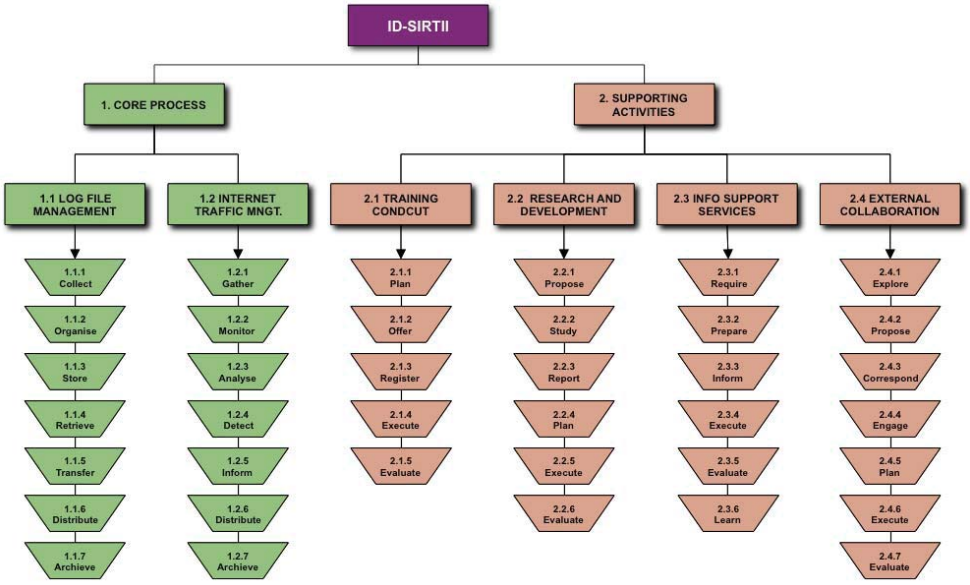
Gambar 2.5 *Rangkaian Proses dan Aktivitas ID-SIRTII*

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

21 Sesuai dengan kebutuhan, maka data traffic log fileyang diminta meliputi informasi terkait dengan source, destination, port, protocol, dan time stamp.

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[22]. 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[23].

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.



Gambar 2.6 *Klasifikasi Proses Kerja Rutin ID-SIRTII*

22 Kriminal yang cerdik akan cenderung menyesatkan penegak hukum dengan cara melibatkan sumber daya-sumber daya komputasi dari berbagai titik-titik negara yang terhubung ke internet.

23 Jika kerjasama tidak dilakukan, maka harus melalui jalur protokol dan birokrasi resmi melalui Departemen Luar Negeri pihak-pihak yang berkoordinasi sehingga membutuhkan waktu yang lama dan proses bertele-tele.

2.10 MENFORMULASIKAN 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[24]. 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[25]. 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:

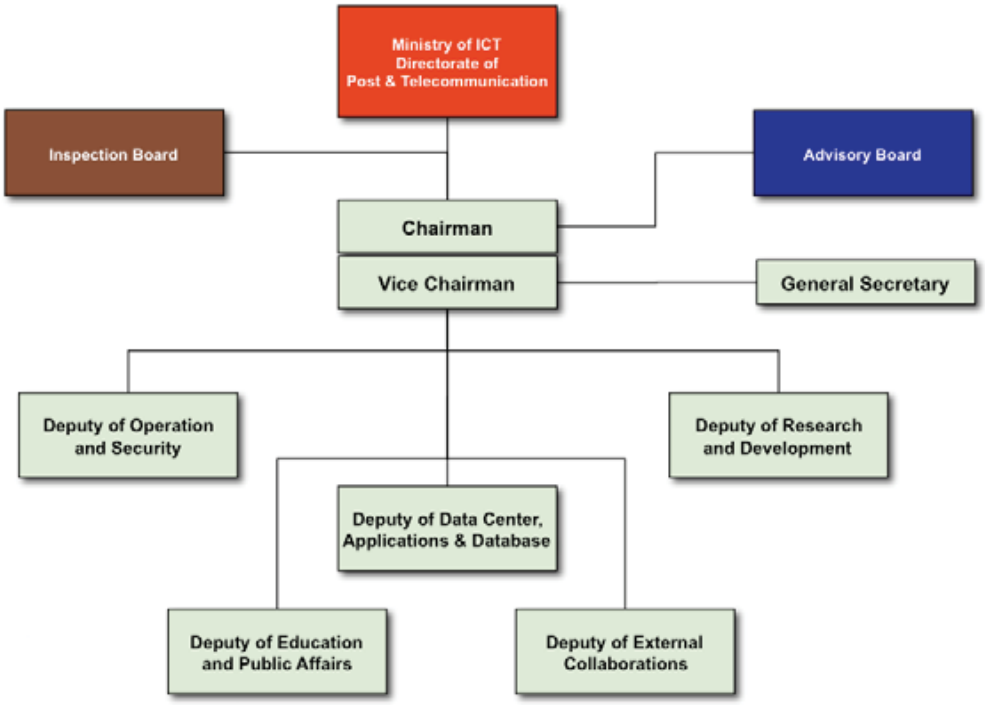
1. Deputi Operasional dan Keamanan – dengan tugas pokok melakukan pemantauan atau *monitoring* terhadap trafik internet yang terjadi di Indonesia dalam mode 24/7;
2. Deputi Aplikasi dan Basis Data – dengan tugas pokok mengelola manajemen *traffic log file* yang diperoleh dari beragam *stakeholder* terkait 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.

---

24 Hal inilah yang membuat setiap CERT/CSIRT memiliki struktur organisasi yang tipikal dan berbeda satu dengan lainnya.

25 Sesuai bidang tugas dan tanggung jawabnya terkait dengan kinerja infrastruktur teknologi informasi dan komunikasi (baca: internet).

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.



Gambar 2.7 *Struktur Organisasi ID-SIRTII*

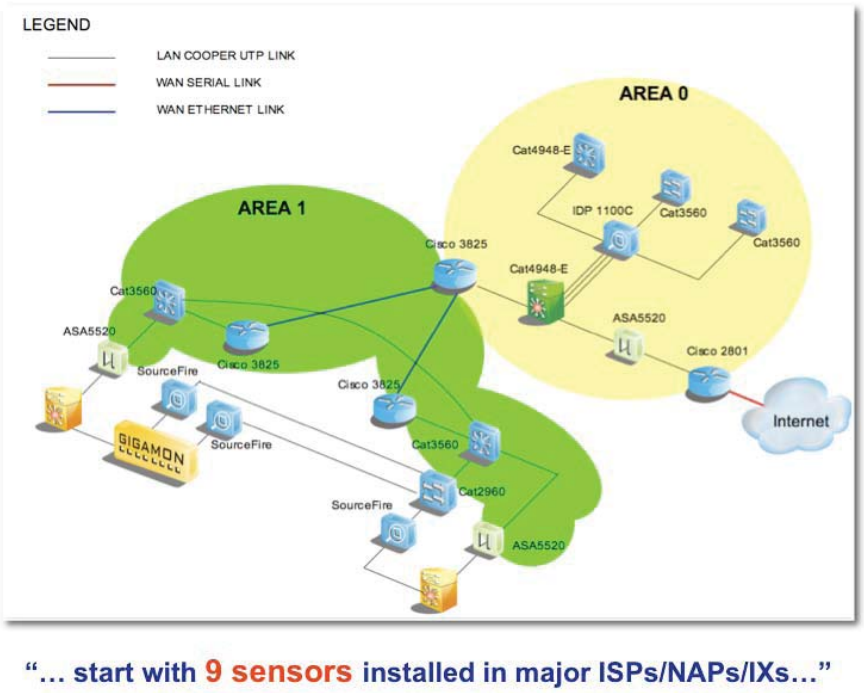
Tim Ahli ini dibagi menjadi tiga kelompok, masing-masing bertanggung jawab terhadap tiga aspek penting, yaitu: kelembagaan dan kebijakan, hukum dan perundang-undangan, serta teknis dan operasional. Agar ID-SIRTII dapat berjalan seperti yang diharapkan oleh seluruh pemangku kepentingan terkait dengannya, 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[26].

2.11 MERANCANG 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

26 Jika Tim Ahli terdiri dari sejumlah pakar-pakar dan/atau praktisi di bidangnya, Tim Pengawas terdiri dari wakil-wakil komunitas dan pemerintahan.

peletakan perangkat sensor di titik-titik utama dimana nadi lalu lintas internet berada[27]. 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[28]. Pada awal pendiriannya, ID-SIRTII bekerjasama dengan *stakeholder* terkait telah memasang sembilan buah sensor di tempat-tempat utama, dimana kurang lebih 80%[29] 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[30].



Gambar 2.8 *Topologi Jaringan Sederhana Perangkat ID-SIRTII*

27 Analoginya adalah pemantauan trafik lalu lintas mobil pada jalan-jalan protokol dan persimpangan-persimpangan besar.

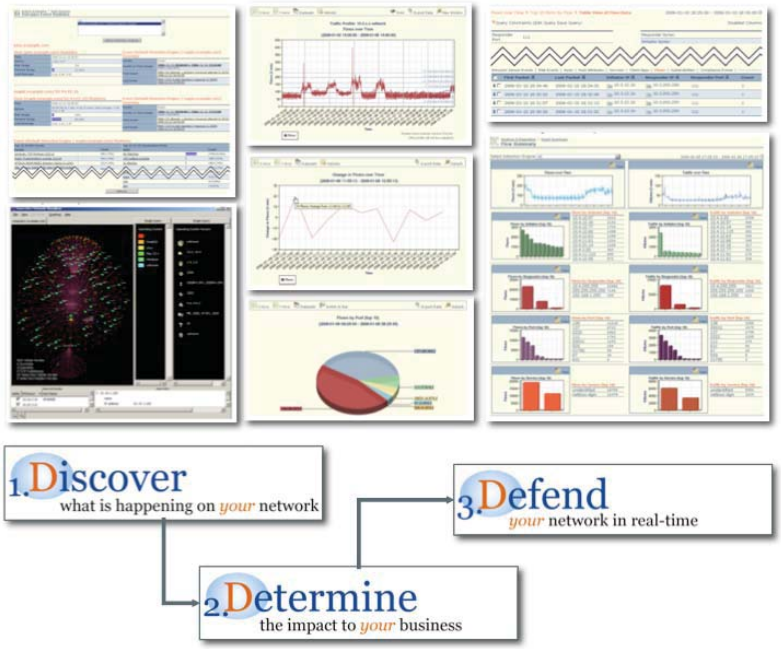
28 Biasanya dilakukan melalui identifikasi internet protocol address dari pihak-pihak yang terkait dengan terjadinya sebuah incident, baik dalam posisinya sebagai "calon" korban, sumber, maupun perantara.

29 Dengan menggunakan prinsip hukum pareto 20:80.

30 Sebagai perbandingan, sebuah perusahaan yang berfungsi sebagai CERT di Jepang, yaitu Little Earth Corporation, pada saat ini telah memiliki 700 buah sensor yang tersebar di berbagai tempat dan konstituen, yang dihubungkan ke 500 buah komputer server yang beroperasi secara simultan.

2.12 MEMPERSIAPKAN 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)[31]. 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[32].



Gambar 2.9 *Kapabilitas Perangkat Lunak Penunjang Pemantauan Internet*

31 Istilah 3D ini khusus diperkenalkan dan diperuntukkan untuk perangkat aplikasi Sourcefire – pengembangan dari Snort – untuk merepresenasikan keungulan dan kapabilias peragkat lunaknya yang dikeluarkan pada awal than 2007.

32 Di beberapa negara teradapat CERT atau CSIRT/CC yang diberikan wewenang untuk melakukan mitigasi (mengurangi probabilitas terjadinya incident, dan seandainya telah terjadi, berusaha mengurangi dampak negatif yang dihasilkannya) melalui berbagai cara; bahkan ada yang diberikan wewenang penuh dari pemerintahnya untuk melakukan pengeblokan terhadap alamat IP tertentu jika dianggap perlu. Hak-hak ini tidak dimiliki oleh ID-SIRTII karena keterbatasan wewenangnya sebagai pemberi early warning signal semata.

2.13 MENJELASKAN 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[33]. 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.

-oo0oo-

33 Di beberapa negara ada yang secara tegas ditekankan misi CERT/CSIRT-nya adalah untuk melakukan pemantauan terhadap hal-hal ilegal yang dilakukan oleh warga negaranya di dunia maya.

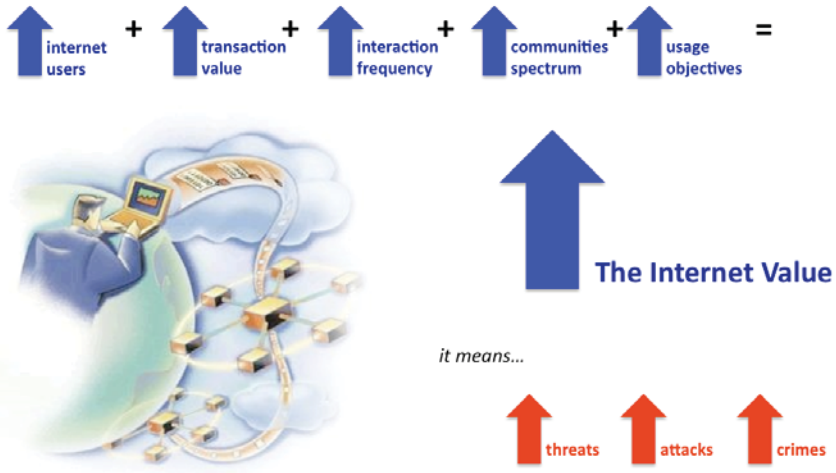
~ 3 ~

PERMASALAHAN MENDASAR KEAMANAN INTERNET

Capaian Pembelajaran (*Learning Outcomes*):

1. Mengembangkan Keamanan Internet dari Aspek Teknis
2. Mengembangkan Keamanan Internet dari Aspek Bisnis
3. Mengembangkan Keamanan Internet dari Aspek Sosial
4. Memetakan Rantai Jejaring Internet
5. Melaksanakan Langkah-Langkah Pengamanan
6. Menjalin Kerjasama Antar Lembaga Keamanan

Seperti yang telah diketahui bersama, fakta dan statistik memperlihatkan terjadinya sejumlah kecenderungan yang meningkat di dalam dunia maya, seperti: jumlah pengguna dan pelanggan yang semakin bertambah, nilai transaksi perdagangan yang meningkat nilainya, frekuensi transaksi yang meningkat tajam, tumbuh beranekaragamnya komunitas baru, dan lain sebagainya. Karena semakin banyak orang yang memanfaatkan internet, maka "nilai" atau *value* dari dunia maya ini semakin meningkat. Akibatnya, semakin banyak pihak yang merasa berkepentingan dengan keberadaan internet, dari mereka yang ingin memanfaatkan berbagai peluang yang ada, hingga para kriminal yang ingin memperoleh keuntungan melalui perbuatan-perbuatan yang tidak baik.



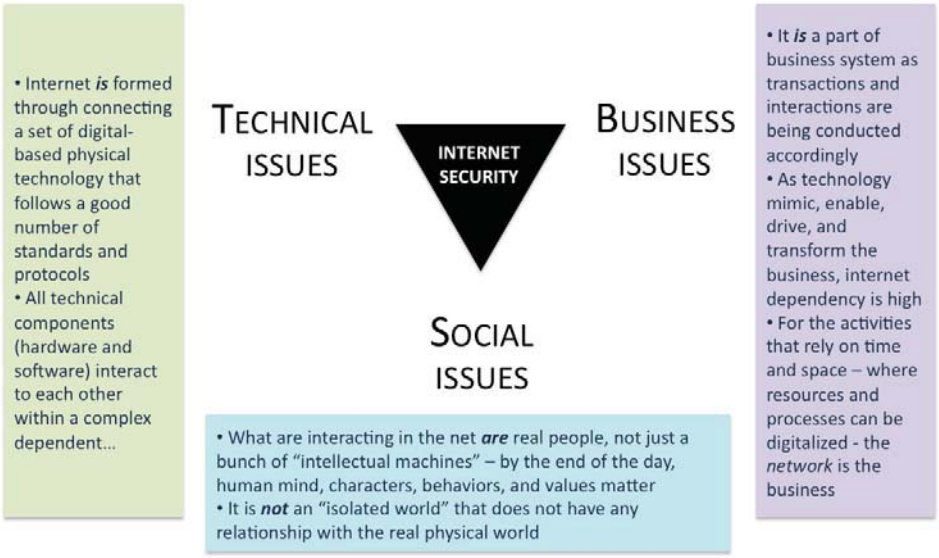
Gambar 3.1 *Trend Dunia Maya dan Potensi Kejahatan Internet*

Untuk dapat mengurangi atau memitigasi meningkatnya jumlah kejadian kejahatan (kriminal) di dunia maya, perlu diperhatikan akar penyebabnya terlebih dahulu[1]. Dari berbagai pendapat dan pendekatan yang ada, terlihat adanya tiga jenis aspek usaha mengatasinya, yaitu masing-masing dipandang dari sisi teknis, bisnis, dan sosial.

Aspek teknis digunakan sebagai pendekatan karena menimbang bahwa pada tataran infrastruktur, internet tidak lain terbentuk dari gabungan sejumlah komponen teknis –seperti komputer, router, hub, modem, database, aplikasi, printer, website, firewalls, dan lain-lain – yang membentuk sebuah jejaring raksasa, dimana secara bebas data dan informasi dapat dipertukarkan untuk beragam keputusan. Berdasarkan konteks ini maka terlihat jelas adanya langkah-langkah secara teknis yang harus dilakukan untuk dapat mengawasi keberlangsungan operasional infrastruktur jejaring internet. Sementara itu dipandang dari perspektif

1 Sebagaimana layaknya fenomena puncak gunung es, perlu dikaji dasar atau inti penyebab kejadian terkait agar dapat dicari solusinya yang mendasar.

bisnis, internet dianggap sebagai suatu medium atau alat atau sarana berbagai pemangku kepentingan dalam usahanya untuk melakukan kegiatan pertukaran barang dan/atau jasa (baca: bisnis). Tanpa adanya konteks kebutuhan, maka tidak terjadi peristiwa bisnis.



Gambar 3.2 *Tiga Aspek Keamanan Internet*

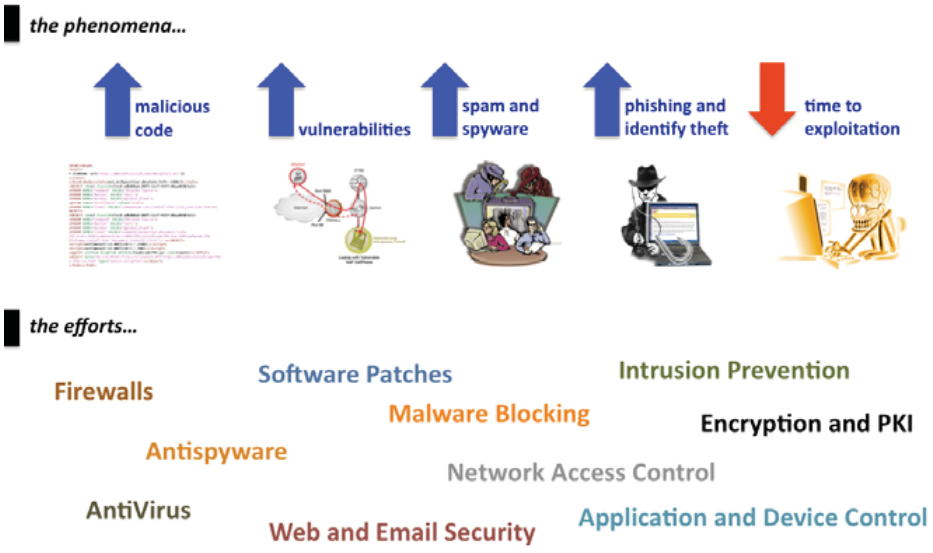
Di satu sisi ada perusahaan yang jika internetnya tidak jalan akan menimbulkan kerugian yang luar biasa, sementara di pihak lain ada organisasi yang tanpa internet masih dapat berjalan dengan baik. Sehingga kebutuhan untuk mengamankan internet harus dipandang dari sisi ini. Sementara itu aspek sosial menekankan bahwa walau bagaimanapun juga, yang berinteraksi dalam internet adalah manusia – bukan robot atau mesin, sehingga harus diperhatikan pula aspek psikologis dan perilaku mereka sebagai individu yang berakal budi. Marilah satu-satu aspek terkait dibedah untuk melihat bagaimana usaha yang telah dilakukan untuk mempromosikan keamanan dalam berinternet. Perlu diingat bahwa dalam implementasinya, ketiga aspek ini biasanya dilihat sebagai sebuah kesatuan holistik – dalam arti kata bahwa untuk mendapatkan pengamanan yang maksimal, ketiga aspek tersebut harus dilihat dan dipelajari secara lebih mendalam.

3.1 MENGEMBANGKAN KEAMANAN INTERNET DARI ASPEK TEKNIS

Dilihat dari perspektif teknis, terjadi trend dimana jumlah dan variasi *malicious software* bertambah dari masa ke masa. Hal yang sama terjadi pula dengan total kasus *vulnerabilities*yang ditemui dalam berbagai produk perangkat keras maupun perangkat lunak teknologi informasi. Dari segi ancaman atau serangan, data memperlihatkan adanya peningkatan tajam pula terhadap pertumbuhan *spam*

maupun *spyware*. Begitu pula halnya dengan kecenderungan terjadinya peningkatan yang berarti terhadap tindakan kriminal seperti *phishing* maupun *identity theft*, yang telah mengakibatkan terjadinya kerugian ekonomis maupun politis. Yang menarik untuk dicermati adalah, terlepas dari adanya trend peningkatan dari seluruh komponen atau entitas di atas, waktu bagi seorang kriminal untuk mengeksploitasi berbagai kelemahan sistem komputer atau jaringan semakin sedikit – alias proses untuk membobol sebuah jaringan komputer menjadi semakin cepat dari hari ke hari. Tentu saja kenyataan menakutkan ini harus diwaspadai secara serius bagi mereka yang keberlangsungan hidup bisnisnya sangat ditentukan oleh kinerja teknologi informasi yang dimilikinya.

Secara teknis, cara untuk menanggulangi ancaman tersebut, adalah melalui instalasi berbagai produk pengamanan internet maupun komputer untuk mencegah kemungkinan dieksploitasinya berbagai kelemahan yang dimiliki oleh sebuah sistem.



Gambar 3.3 *Aspek Teknis Pengamanan Internet*

Misalnya adalah instalasi *firewalls* untuk melindungan jaringan internal perusahaan dari akses pihak yang berada pada jejaring eksternal (baca: internet), atau dilibatkannya program *anti-virus* dan *anti-spyware* untuk mencegah berbagai program jahat masuk ke dalam sistem komputer, atau pemasangan *software patches* untuk menambal lubang-lubang kerawanan yang ada pada sistem aplikasi, atau melakukan proses *encryption* untuk mencegah pihak yang tidak berwenang mengerti isi dari suatu pesan atau informasi rahasia. Keseluruhan usaha yang bertujuan untuk mengurangi probabilitas terjadinya eksploitasi terhadap kerawanan sistem ini (baca: mitigasi) dilakukan pada level teknis operasional, dalam arti kata dikembangkan dengan cara mengadakan sejumlah piranti lunak/

keras yang kemudian dipasang atau diinstalasi pada sistem komputer atau jaringan yang ingin dilindungi.

3.2 MENGEMBANGKAN KEAMANAN INTERNET DARI ASPEK BISNIS

Dalam perspektif bisnis, tindakan pengamanan terhadap internet dari sebuah organisasi komersial semacam perusahaan dapat dilihat dari berbagai sudut.

Gambar 3.4 *Aspek Bisnis Pengamanan Internet*

Yang pertama adalah memandang isu keamanan internet dari sisi manajemen resiko. Jika sebuah perusahaan sangat tergantung bisnisnya dengan kinerja sistem aplikasi yang terhubung dengan internet, sementara berdasarkan kajian/ analisa resiko terdapat sejumlah potensi gangguan yang probabilitas terjadinya tinggi dan dapat mengakibatkan dampak yang signifikan jika sampai terjadi, maka perlu dilakukan tindakan pengamanan secara serius untuk mencegah terjadinya gangguan atau *un-intended event* tersebut. Konteks yang kedua adalah dengan mempertimbangkan tindakan pengamanan yang dimaksud berdasarkan analisa *cost benefit*. Sejauh manfaat yang diperoleh dengan mengamankan sebuah sistem jauh lebih besar dibandingkan dengan biaya yang dikeluarkan, maka tindakan pengamanan tersebut perlu dilakukan. Sementara pendekatan ketiga adalah pemenuhan aspek pengamanan sistem komputer atau internet karena mengacu pada peraturan internal maupun eksternal yang berlaku – misalnya yang telah dikeluarkan oleh pemerintah atau pun pihak otoritas lain berdasarkan standar baku mutu (inter-) nasional. Konteks berikutnya adalah pemenuhan kebutuhan modul pengamanan karena merupakan bagian tak terpisahkan dari tuntutan aspek tata kelola (baca: *governance*) yang baik, seperti transparansi, akuntabilitas, responsibilitas, dan independensi. Perspektif lain yang belakangan

ini juga mengemuka adalah alasan pelaksanaan pengamanan yang disebabkan karena tingginya nilai sejumlah aset data dan/atau informasi yang dimiliki oleh perusahaan, sehingga untuk melindunginya, dilakukan sejumlah usaha pengamanan. Misalnya adalah keberadaan data pelanggan yang harus dilindungi, atau informasi intelijen yang bersifat rahasia, atau rumusan/formula paten tertentu, dan lain sebagainya. Dan yang terakhir, kegiatan pengamanan dilakukan oleh segenap pemangku kepentingan karena telah menjadi bagian tak terpisahkan dari manajemen pengelolaan organisasi atau korporasi yang dimaksud (baca: SOP=*Standard Operating Procedure*). Biasanya hal ini dilakukan oleh sebuah perusahaan multi-nasional yang membuka cabangnya di beberapa negara. Agar seluruh manajemen dan karyawan patuh serta tertib dalam menjaga keamanan informasinya, maka dibuatlah SOP yang harus ditaati dalam kegiatan operasional sehari-hari.

Gambar 3.5 *Aspek Sosial Pengamanan Internet*

3.3 MENGEMBANGKAN KEAMANAN INTERNET DARI ASPEK SOSIAL

Sifat dan karakteristik manusia sangat dipengaruhi oleh keadaan lingkungan di sekitarnya. Dalam jaman moderen ini, dimana teknologi informasi dan komunikasi telah merasuki seluruh aspek kegiatan dan kehidupan manusia, para generasi muda semakin akrab dengan keberadaan teknologi ini. Sifat "technology savvy" tersebut sangat kental melekat pada komunitas kota-kota besar maupun daerah-daerah keramaian lainnya. Kenyataan ini didukung dengan data semakin pesatnya penggunaan telepon genggam dan piranti-piranti digital lainnya (baca: *digital gadgets*) oleh masyarakat luas. Didukung oleh arusnya deras globalisasi dalam dunia perdagangan maupun politis, para generasi muda ini sudah menganggap

dunia maya atau internet menjadi bagian dari kehidupannya sehari-hari. Aplikasi semacam *email, chatting, mailing list, blogging, newsgroup,* dan lain-lain sudah merupakan santapan sehari-hari yang tiada henti dimanfaatkan. Namun kenyataan membuktikan bahwa komunitas digital ini terlampau "disilaukan" oleh manfaat internet dan agak lupa atau lalai dalam memandang sisi negatifnya yang dapat merugikan seandainya tidak dikelola dan diperhatikan secara sungguh-sungguh. Jika hal keamanan informasi ini diabaikan, isu-isu seperti pornografi, pelanggaran hak-hak pribadi (baca: *privacy*), kriminalitas, penyadapan, pencurian informasi, dan lain sebagainya dengan leluasa dapat terjadi.

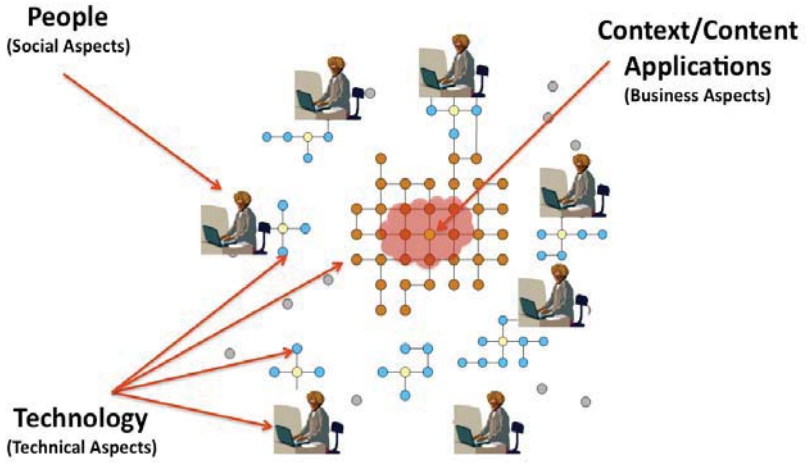
Untuk membiasakan diri peduli dengan keamanan informasi, memang harus dilakukan sejumlah usaha seperti sosialisasi dan pelatihan. Namun terlepas dari hal itu, banyak hal yang dapat dilakukan agar tindakan preventif maupun korektif terkait dapat secara efektif diterapkan. Belajar dan berkaca dari pengalaman organisasi yang berhasil membudayakan kebiasaan mengamankan informasi, berikut adalah ragam "pasangan" pendekatan yang bisa dipergunakan:

1. Antara menerapkan kebijakan dengan mengembangkan desain teknis yang mendukung keamanan (baca: *policy vs. design).* Contohnya kebijakan adalah dengan mengeluarkan surat keputusan berisi butir-butir prosedur yang harus ditaati oleh seluruh karyawan dalam hal mengoperasikan komputer di lingkungan organisasi terkait. Sementara melalui desain teknis adalah dengan mengkondisikan terjadinya suatu status aplikasi yang memaksa pengguna atau *user* taat untuk melakukan tindakan tertentu. Misalnya adalah "paksaan" dari sebuah sistem agar setiap tiga bulan sekali setiap pengguna harus mengganti *password*-nya. Jika tak dilakukan, maka yang bersangkutan tidak dapat mengoperasikan sistem aplikasinya. Contoh lainnya adalah keharusan melakukan proses enkripsi terhadap setiap email yang ingin dikirimkan ke mitra bisnis, tanpa dilakukan proses enkripsi yang benar, maka surat elektronik yang dibuat tidak dapat dikirimkan karena ditolak oleh sistem;
2. Antara menerapkan sistem bonus dengan hukuman penalti (baca: *reward vs. punishment*) terhadap seluruh staf dan karyawan yang berperan sebagai pengguna sistem. Melalui pendekatan bonus, sejumlah "hadiah" atau insentif tertentu diberikan oleh perusahaan kepada karyawannya yang melalui rekam jejak yang dipelajari terbukti selalu patuh dan peduli dengan mekanisme pengamanan informasi yang diberlakukan oleh perusahaan – terutama dalam mencegah terjadinya hal-hal yang tidak diinginkan (usaha preventif). Sementara untuk setiap kasus kebocoran informasi yang terjadi, baik disengaja maupun tidak, sejumlah hukuman secara individu maupun kolektif telah siap dibebankan kepada mereka yang terbukti lalai mengabaikan aspek keamanan informasi tersebut;

3. Antara memberikan "tekanan" atau *pressure* terhadap seluruh karyawan untuk mendapatkan hasil yang cepat dengan memilih pendekatan edukatif yang lebih lambat namun akan jauh lebih efektif;
4. Antara pendekatan "top down" dimana setiap pimpinan akan memberikan instruksi kepada bawahannya secara berkala untuk peduli dan menjalankan prosedur keamanan, dengan pendekatan "bottom up" dimana terjadi proses sosialisasi mekanisme pengamanan informasi dari level staf maupun karyawan yang sehari-harinya berhadapan langsung dengan permasalahan operasional ke pihak manajemen dengan menggunakan bahasa dan kasus yang kontekstual;dan lain sebagainya.

3.4 MEMETAKAN RANTAI JEJARING INTERNET

Singkat cerita, jika ketiga aspek tersebut dicoba untuk dihubungkan satu dengan lainnya, maka akan terlihat secara jelas relasi di antaranya, yaitu:



Gambar 3.6 *Relasi Antar Tiga Aspek Pengamanan Informasi dalam Konteks Internet*

1. Internet merupakan suatu jejaring raksasa yang mempertemukan berbagai jaringan komputer yang ada di muka bumi ini. Jejaring raksasa tersebut terjadi dengan cara menghubungkan beraneka ragam pusat-pusat penyimpanan data dan informasi yang tersebar lokasinya di seluruh dunia dengan memanfaatkan teknologi informasi dan komunikasi. Berbagai peralatan teknis dan piranti teknologi ini merupakan kunci terciptanya sebuah jaringan raksasa yang tumbuh secara eksponensial dari waktu ke waktu.
2. Jejaring raksasa ini pada dasarnya merupakan sebuah infrastruktur komunikasi yang di atasnya dapat diimplementasikan berbagai aplikasi untuk memenuhi sejumlah kebutuhan hidup manusia, seperti: keperluan

pendidikan, interaksi sosial, transaksi bisnis, pengembangan pribadi, dan lain sebagainya. Konteks pertukaran barang dan jasa tersebut (baca: bisnis) kerap mendominasi pemanfaatan infrastruktur internet ini.

3. Pada akhirnya, sang pengguna berbagai aplikasi yang berjalan di atas internet ini adalah para individu atau komunitas yang berkepentingan, mulai dari anak-anak, orang tua, karyawan, pengusaha, seniman, politikus, pendidik, wiraswastawan, dan lain sebagainya.

Melihat adanya keterhubungan yang jelas baik secara fisik maupun virtual antara ketiga komponen ini, maka dapat disimpulkan bahwa kunci sukses tidaknya atau tinggi rendahnya tingkat keamanan internet sangat ditentukan oleh setiap perangkat teknis, setiap aplikasi, dan setiap individu yang mempergunakannya[2].

Since the strength of a chain
depends on the weakest link,

then YOUR SECURITY is MY SECURITY...

Gambar 3.7 *Prinsip Keamanan Rantai Jejaring Internet*

Dengan mengibaratkan jejaring raksasa ini sebagaimana halnya sebuah rantai, maka berlaku prinsip yang menyatakan bahwa "kekuatan sebuah rantai sangat ditentukan oleh mata rantai yang terlemah". Dalam perspektif inilah maka prinsip keamanan "your security is my security" menemukan konteksnya. Tidak ada gunanya atau kecil perannya sebuah *firewalls*dalam sebuah organisasi tanpa diiringi dengan perilaku/budaya pengamanan oleh seluruh pengguna sistem maupun kualitas keamanan seluruh aplikasi yang dipergunakan.

3.5 MELAKSANAKAN LANGKAH-LANGKAH PENGAMANAN

Dalam perspektif jejaring yang sedemikian rupa, ada sejumlah langkah-langkah yang dapat dipergunakan oleh sebuah perusahaan untuk memitigasi resiko terjadinya hal-hal yang tidak diinginkan terhadap jaringan komputer atau internet yang dipergunakannya. Berikut adalah 8 (delapan) langkah yang dimaksud:

2 Dalam dunia organisasi maupun arsitektur sistem informasi, ketiga komponen ini sering diidentikkan atau diistilahkan sebagai people, process, and technology.

- Tentukan aset-aset informasi apa saja yang paling berharga bagi perusahaan yang perlu untuk diamankan.
- Tentukanlah batasan-batasan jejaring yang terhubung dan/atau terkait dengan aset informasi yang dimaksud (baca: perimeter).
- Identifikasikan para pihak pemangku kepentingan yang berada dalam wilayah atau perimeter tersebut.
- Lakukan analisa resiko terkait hal-hal yang dapat mengancam keberadaan aset berharga tersebut dalam konteks kemungkinan terjadinya peristiwa yang tidak diinginkan dengan *magnitude* kerugian yang ditimbulkannya.
- Pastikan dilakukan mitigasi resiko berupa instalasi piranti keras, penerapan piranti lunak, dan prosedur keamanan pengguna sebagai suatu bagian kesatuan implementasi sistem pengamanan.
- Buat payung peraturan dan perangkat penerapan model keamanan yang dimaksud agar dapat di-*enforce* dan diterapkan oleh seluruh lapisan manajemen dan staf dalam organisasi.

Gambar 3.8 *Delapan Langkah Manajemen Keamanan Internet dan Jaringan*

Berdasarkan kinerja dan pemantauan efektivitas sehari-hari, lakukan diskusi dan berbagi pengalaman dengan seluruh pihak dan pemangku kepentingan yang terlibat untuk keperluan perbaikan sistem.

Secara terus-menerus perbaikilah kualitas sistem keamanan yang dimiliki, misalnya dengan menggunakan "theory of constraint". Prinsip dari pendekatan ini sangatlah sederhana, yaitu: carilah mata rantai yang paling lemah dalam sebuah sistem jejaring, dan perbaikilah (lakukanlah hal ini berulang-ulang secara terus-menerus sebagai bagian dari *continuous improvement*).

3.6 MENJALIN KERJASAMA ANTAR LEMBAGA KEAMANAN

Melalui paparan dan deskripsi di atas, semakin jelaslah peranan berbagai lembaga keamanan informasi seperti CERTs, CSIRTs, interpol, *cyber crime unit*, ASEAN's *task*

force on cyber security, dan lain sebagainya. Setiap negara sadar, bahwa keamanan internet sangatlah ditentukan oleh seluruh komponen penggunanya. Tidak ada gunanya bagi sebuah negara moderen yang telah tangguh mengamankan sistem komputernya namun tidak diimbangi oleh hal yang sama oleh negara-negara lain. Kondisi negara terlemah dalam bidang keamanan internet akan mempengaruhi negara-negara lain karena sifat internet yang lintas batas negara dan geografis. Oleh karena itulah maka terjalin kerjasama antara berbagai lembaga-lembaga keamanan informasi antar negara. APCERT adalah contoh kerjasama koordinasi antara CERT negara-negara Asia Pasifik, atau FIRST yang merupakan suatu forum internasional tempat berkumpulnya para penanggung-jawab CERT yang ada di seluruh dunia, atau China-ASEAN Task Force yang merupakan suatu gugus kerja sama antara CERT yang tergabung dalam ASEAN dengan negeri raksasa Cina, dan lain sebagainya. Mengapa lembaga-lembaga ini berniat untuk melakukan kolaborasi? Karena jika mengandalkan dunia nyata, seluruh kerjasama tukar-menukar informasi antar negara dalam menghadapi berbagai insiden keamanan internet harus melalui birokrasi dan protokoler antar departemen luar negeri yang terkadang sangat lambat – dimana situasi ini bukanlah merupakan jawaban untuk mencegah dan menangani kejahatan internet yang terjadi dalam hitungan detik.

-oo0oo-

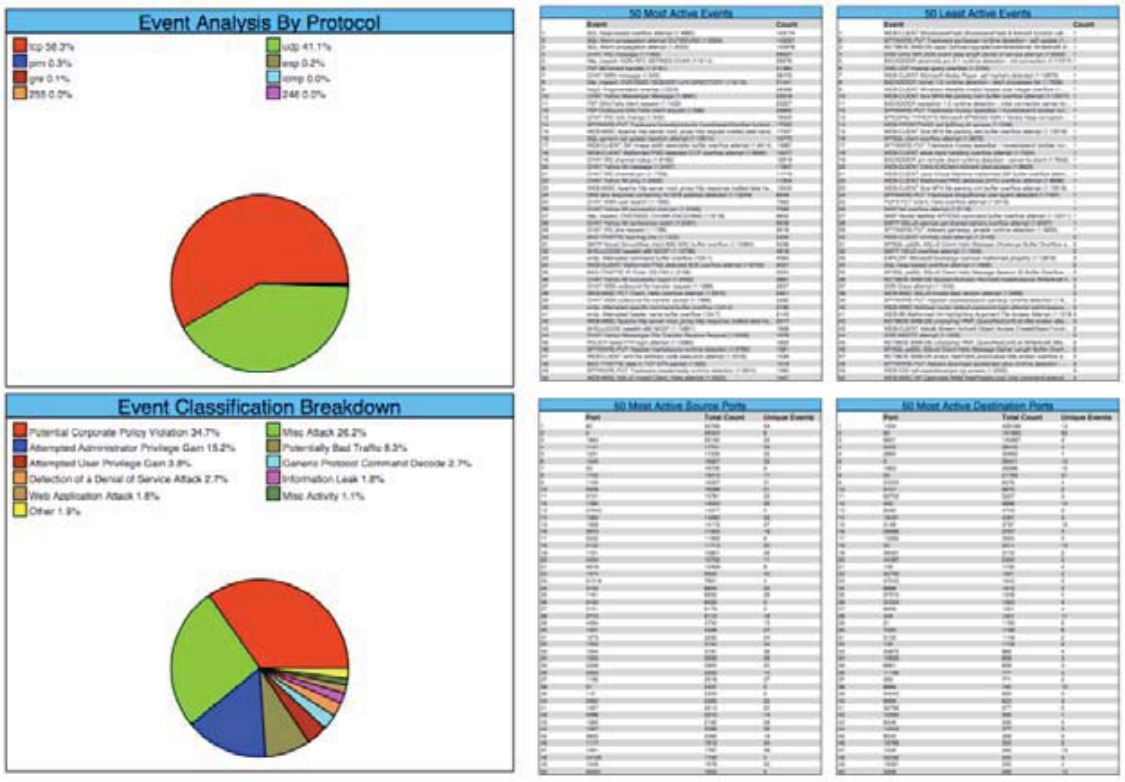
~ 4 ~

RELASI ANTARA DUNIA NYATA DENGAN SIBER DALAM HAL KEAMANAN

Capaian Pembelajaran (*Learning Outcomes*):

1. Menyatukan Karakteristik Dua Dunia
2. Mempelajari Fenomena Dua Dunia
3. Memahami Pengaruh Dunia Maya terhadap Dunia Nyata
4. Membangun Strategi Pengamanan Dua Dunia

Ada suatu hal yang menarik dalam dunia keamanan informasi dan internet yang patut untuk dicermati dan dipelajari lebih lanjut. Hal ini berdasarkan riset dan pengamatan ID-SIRTII terhadap pola kejadian potensi serangan internet yang ada di Indonesia. Melalui studi tersebut, ada sebuah hipotesa yang dikembangkan dan dicoba untuk dibuktikan, yaitu: terdapat suatu hubungan yang signifikan antara kejadian di dunia nyata dengan peristiwa serangan di dunia maya (baca: interent) dan sebaliknya.

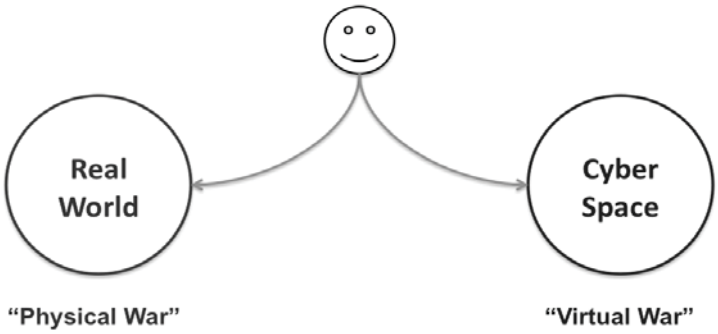


Gambar 4.1 *Contoh Hasil Monitoring Trafik ID-SIRTII*

4.1 MENYATUKAN KARAKTERISTIK DUA DUNIA

Pada awal mulanya lahir dan dimanfaatkannya internet, terkenal suatu istilah semacam *virtual world* atau *cyber world* untuk menggambarkannya. Dunia maya ini dianggap sebagai sebuah arena interaksi antara mereka yang memiliki "hak eksklusif" penggunaan sistem komputer yang terhubung dalam sebuah jejaring raksasa. Peristiwa historis tersebut secara tidak langsung mewarnai pola pikir manusia di masa-masa awal perkembangan internet, yang mendikotomikan antara dunia nyata dengan dunia maya.

1. Dikatakan sebagai hak eksklusif karena pada mulanya hanya sejumlah perguruan tinggi di Amerika yang bersepakat untuk melakukan kerjasama riset saja yang memiliki akses ke internet generasi awal ini.

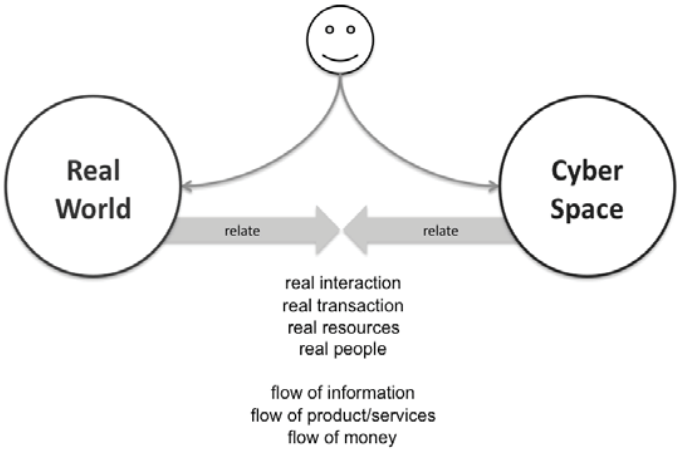


Gambar 4.2 *Dikotomi Dua Dunia Manusia*

Dalam konteks dikotomi inilah kemudian terbentuk suatu opini bahwa tidak adanya hubungan yang jelas dan tegas antara dua dunia ini. Masing-masing berdiri sendiri dan tidak saling mempengaruhi. Contohnya adalah pendapat yang mengatakan bahwa peperangan yang terjadi di dunia nyata, tidak akan berpengaruh di dunia maya, dan sebaliknya. Bahkan pengguna atau *user* atau individu terkadang memiliki "dua kepribadian" yang berbeda ketika berinteraksi dengan dua dunia ini. Ketika di dunia nyata, yang bersangkutan memiliki data, perilaku, dan profil seperti apa adanya; namun ketika masuk ke dunia maya, yang bersangkutan dapat "menyamar" menjadi orang lain karena keleluasaan dan kemungkinan-kemungkinan yang ditawarkan.

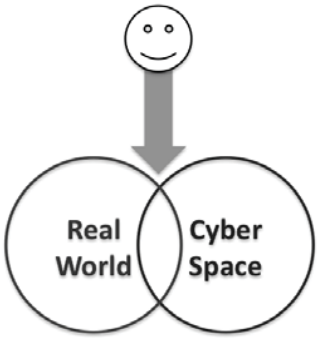
Lambat laun, sesuai dengan perkembangan internet dan teknologi informasi yang sedemikian cepat, yang tadinya internet hanya dipergunakan unuk riset dan pendidikan, mulai berkembang ke industri serta aspek kehidupan lainnya. Transaksi bisnis mulai terjadi, interaksi sosial antar individu semakin menggejala, penyebaran budaya terjadi secara intensif, keterbukaan politik dan kebebasan media mendominasi kehidupan sehari-hari, dan lain sebagainya. Beberapa pusat riset dunia bahkan mensinyalir, telah terjadi penurunan secara cukup signifikan jumlah transaksi ekonomi yang biasanya terjadi di dunia nyata – karena berpindah ke dunia maya yang memberikan sejumlah manfaat semacam efisiensi dan optimalitas. Misalnya adalah dalam hal kecenderungan membeli barang yang beralih dari uang tunai menjadi model pembayaran berbasis elektronik (seperti kartu kredit, kartu debit, pulsa telepon, dan lain sebagainya).

Fenomena tersebut mengandung arti bahwa apa yang terjadi di dunia maya, tidak dapat dilepaskan begitu saja dengan kenyataan di dunia nyata, mengingat terjadinya kecenderungan keberhimpitan kedua dunia tersebut yang menampakkan irisan semakin lama semakin bertambah besar.



Gambar 4.3 *Trend Berhimpitannya Dua Dunia*

Hal ini semakin diperjelas dengan kenyataan yang memperlihatkan bahwa yang berinteraksi di dunia maya adalah benar-benar individu manusia, dengan menggunakan alat pembayaran uang yang sah, dan melibatkan sejumlah dokumen perjanjian yang legal[2]. Dengan berhimpitnya dua dunia tersebut, maka jelas akan terjadi hubungan keterkaitan yang cukup erat antara satu dunia dengan dunia lainnya. Apa yang terjadi di dunia maya akan sangat mempengaruhi mereka yang ada di dunia nyata, dan berlaku pula sebaliknya. Bahkan di masa mendatang, ketika seluruh individu telah terhubung dan dapat mengakses inernet, maka kedua dunia tersebut akan menyatu secara identik.



Gambar 4.4 *Trend Semakin Berhimpitannya Dua Dunia*

Terkait dengan isu keamanan internet yang menjadi pembicaraan banyak orang dewasa ini, terbersit pula sejumlah praduga alias "hipotesa" tidak tertulis yang memperkirakan bahwa hal-hal yang terjadi di dunia nyata dapat berpengaruh di dunia maya dan sebaliknya – terutama hal-hal yang terkait dengan berbagai peristiwa (baca: *incident*) kejahatan internet.

2 Khususnya di Indonesia setelah diberlakukannya UU No.11 tahun 2008 mengenai Informasi dan Transaksi Elektronik.

Gambar 4.5 *Dua Kaitan Penyebab Kejahatan Internet*

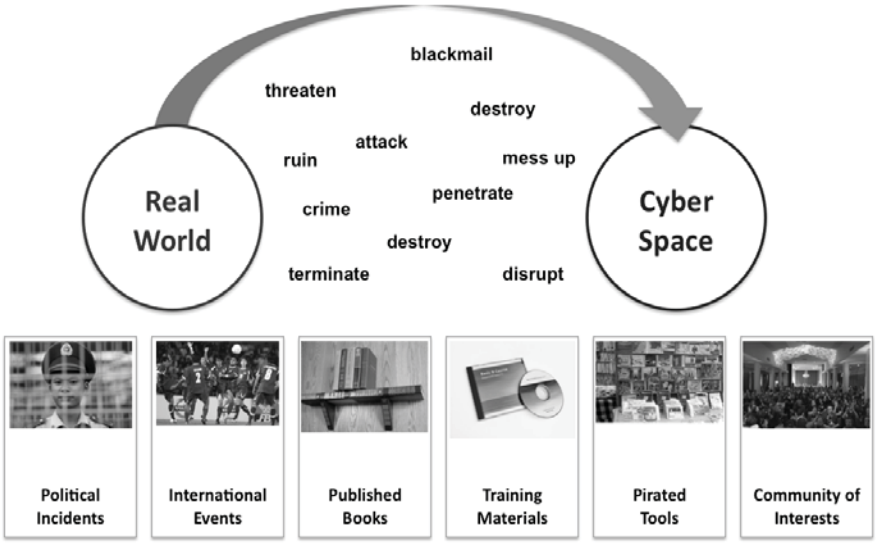
4.2 MEMPELAJARI FENOMENA DUA DUNIA

Dari berbagai hasil pemantauan sejumlah praktisi keamanan informasi dan internet, terdapat sejumlah kejadian di dunia nyata yang secara langsung maupun tidak langsung berpengaruh terhadap berbagai peristiwa yang berlangsung dalam dunia maya. Berikut adalah beberapa jenis pemicu terjadinya sejumlah peristiwa tersebut.

Pertama adalah dipicu oleh kejadian bernuansa politis. Contohnya adalah ketika Indonesia dan Malaysia "berhadapan" secara politis dalam kasus perebutan wilayah Ambalat, maka sekonyong-konyong terjadi "perang" *web defacement* atau "permak tampilan situs" antara *hacker underground* Indonesia dan Malaysia. Berbagai situs dengan domain .id dicoba di-*hack* oleh pihak Malaysia, demikian juga dengan situs berakhiran .my yang coba diserang oleh pihak Indonesia. Tidak tanggung-tanggung berbagai pihak di Indonesia maupun Malaysia berusaha "menenangkan" para pihak yang terbakar emosinya ini di dunia maya. Hal yang sama beralangsung pula antara Indonesia dan Australia misalnya setiap kali ada satu atau dua buah berita politik yang mendatangkan ketegangan hubungan bilateral antara dua buah negara terkait. Yang menarik adalah bahwa tidak jarang terjadi peristiwa dimana negara-negara simpatisan atau sekutu juga turut serta "meramaikan dunia persilatan" jika dipandang perlu. Tengoklah apa yang terjadi di dunia maya ketika terjadi perseteruan antara China dan Tibet, Malaysia dan Singapura, Rusia dan Georgia, dan lain sebagainya.

Kedua adalah peristiwa-peristiwa yang dipicu oleh terselenggaranya berbagai *event* atau kegiatan berskala internasional, semacam Olimpiade, Sea Games, Asian Games, World Cup, dan lain sebagainya. Hal-hal menarik yang terjadi di dalam momen-momen olah rata tersebut adalah persaingan ketat antara sejumlah negara maupun peristiwa-peristiwa tertentu yang menodai rasa keadilan. Lihatlah contohnya ketika terjadi final piala sepakbola antara dua negara, maka tidak jarang di dunia maya pun terjadi peristiwa "serang-serangan" ide, gagasan, maupun situs-sius terkait. Kejadian dipukulinya wasit karateka Indonesia oleh sejumlah atlet Malaysia juga memicu serangan besar-besaran di dunia maya yang sulit dikendalikan. Perlu dicatat bahwa tidak hanya *event* olah raga saja, namun

pertemuan-pertemuan akbar seperti PBB, G8, OPEC, dan lain-lain juga sering menjadi pemicu serangan yang terjadi di dunia maya.



Gambar 4.6 *Dunia Nyata sebagai Pemicu Kejadian*

Ketiga merupakan hasil kajian yang sungguh menarik dari sejumlah pihak terkait. Ternyata trend jenis-jenis serangan di dunia maya – seperti *SQL Injection, Web Defacement, Botnet, DOS/ DDOS Attack*, dan lain sebagainya – sangat berkaitan erat dengan buku-buku publikasi terkait dengan proses *hacking*yang dijual bebas di pasaran. Alasannya cukup sederhana. Biasanya buku-buku berbahasa Indonesia maupun Inggris tersebut dalam memberikan penjelasannya disertai dengan contoh kasus atau latihan-latihan yang melibatkan situs-situs tertentu. Dengan sedikit kreativitas pembaca, maka yang bersangkutan dapat mencoba teknik terkait ke sejumlah situs atau website atau sistem komputer atau jaringan yang ada di tanah air.

Keempat yang merupakan fenomena serupa tapi tak sama adalah trend kejadian "penyerangan" di dunia maya dengan modus operandi seperti yang sering dicontohkan lembaga-lembaga penyelenggara pelatihan *internet security*atau *ethical hacker*. Sesuai yang dicontohkan oleh instruktur pengajarnya maupun yang ditulis dalam buku materi pelatihan yang diberikan ke peserta. Hal ini dapatlah dimengerti mengingat sejumlah alasan. Misalnya adalah sangat sulit memahami teori keamanan internet tanpa memberikan dan melakukan sejumlah contoh-contoh analisa kerawanan (baca: *vulnerabilitiesi*), atau aktivitas uji coba keamanan (baca: *penetration test*), atau tindakan eksploitasi kerawanan. Alasan lain yang berpegang pada prinsip untuk menjadi seorang "defenser" yang baik, maka harus mengerti cara-cara kerja "offenser" – alias untuk dapat menjadi polisi yang baik, harus tahu persis bagaimana orang jahat atau kriminal berfikir dan bekerja. Sangat

sulit melakukan contoh-contoh yang kontekstual tanpa melibatkan jaringan yang riil.

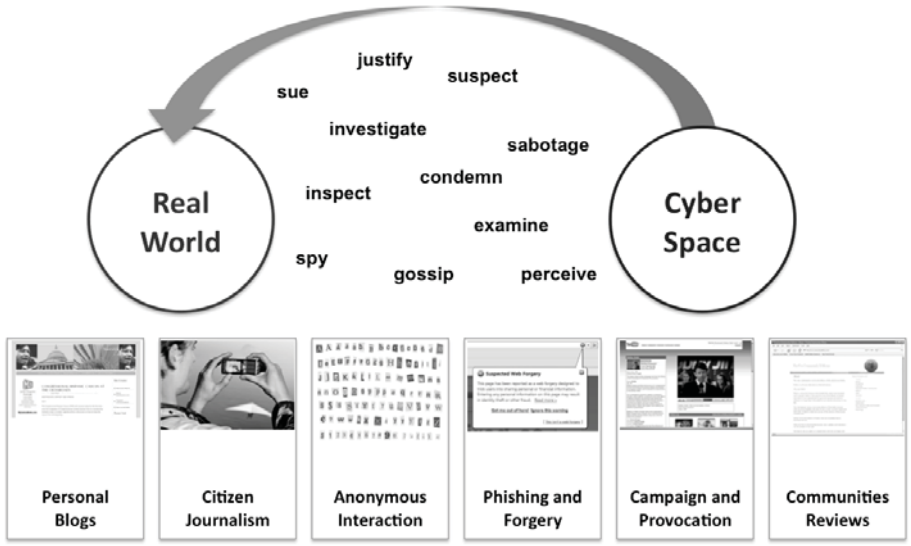
Kelima adalah disebabkan karena begitu banyaknya di pasaran piranti lunak atau *tools* untuk melakukan *hacking* yang diperjualbelikan secara gratis – yang kebanyakan merupakan *software*bajakan. Program-program yang dijual bebas dengan harga murah ini tidak saja memberikan keleluasaan kepada penggunanya untuk melakukan berbagai jenis serangan di dunia maya, namun dari hari ke hari menawarkan pula kemudahan-kemudahan dalam menggunakannya (baca: semakin *user friendly*). Bagi mereka yang memiliki hobi menekuni dunia keamanan internet, perangkat-perangkat lunak penunjang ini sangatlah berguna karena memberikan berbagai trik, fasilitas, fitur, dan kapabilitas yang sangat beragam.

Keenam yang kerap memicu terjadinya tindakan maupun peristiwa di dunia maya adalah dimulai dari sejumlah pertemuan *community of interest* baik secara terbuka maupun tertutup (baca: *underground*) yang membahas berbagai fenomena yang terjadi di dunia maya. Tidak jarang hasil dari diskusi, tukar pikiran, lokakarya, seminar, maupun pertemuan ini bermuara pada uji coba atau tindakan penetrasi terhadap situs atau jaringan tertentu yang menjadi bahan pembicaraan khalayak atau komunitas sejenis ini.

4.3 MEMAHAMI PENGARUH DUNIA MAYA TERHADAP DUNIA NYATA

Relasi antara dua dunia tersebut berlaku pula sebaliknya. Tidak jarang terjadi suatu sengketa serius di dunia nyata, yang pada awal mulanya sebenarnya terjadi di dunia maya. Hal ini semakin lama semakin banyak terjadi seiring dengan semakin berkembangnya komunitas pengguna internet, dan mulai diperkenalkannya *cyber law* di Indonesia melalui UU ITE No.11 tahun 2008. Berikut adalah sejumlah fenomena kejadian di dunia maya yang memicu terjadinya peristiwa menarik di dunia nyata.

Pertama, yang paling banyak terjadi dan menggejala belakangan ini adalah dimulai dari penulisan *blog*oleh seseorang. Sering kali isinya *blog* lebih merupakan suatu pengalaman dan pandangan pribadi terhadap individu maupun peristiwa atau kejadian tertentu yang didasarkan pada perasaan, persepsi, sangkaan, maupun asumsi tertentu dari si pengarang atau penulis. Tidak jarang ditemui dalam *blog* tersebut disebutkannya secara jelas dan tegas nama-nama individu pelaku yang terkait dengan isi cerita yang ada.



Gambar 4.7 *Dunia Maya sebagai Pemicu Kejadian*

Dalam konteks ini ternyata tidak semua individu dalam dunia nyata telah siap berhadapan dengan alam "demokrasi mengemukakan pendapat" semacam itu, sehingga cukup banyak yang berlanjut dengan adanya tuntutan "pencemaran nama baik" dari mereka yang namanya disebutkan dalam sejumlah blog-blog pribadi yang menjamur di dunia maya. Dengan menggunakan berbagai jenis pasal dalam UU ITE, yang bersangkutan berusaha mempidanakan si penulis blog.

Kedua merupakan fenomena yang dipicu dengan berkembangnya komunitas *citizen journalism*. Dengan menggunakan berbagai *electronic gadget* seperti kamera digital, telepon genggam, *personal digital assistant*, dan lain sebagainya – seorang awam dapat menjadi wartawan karena kemampuannya dalam meliput berita dimana saja yang bersangkutan beraktivitas. Lihatlah bagaimana dibukanya jalur-jalur komunikasi antara televisi dan radio dengan para individu tersebut seperti yang dilakukan oleh kantor berita terkemuka di dunia CNN maupun YouTube. Tidak jarang seorang individu dalam melakukan aktivitasnya sehari-hari berjumpa dengan peristiwa menarik seperti: anggota parlemen yang sedang memarahi pelayan rumah makan, atau mantan pejabat yang sedang memaki-maki satpam, atau artis yang sedang mencak-mencak kesal dengan penjual, atau tokoh masyarakat yang sedang bersua dengan konglomerat hitam, dan lain sebagainya. Kejadian tersebut dengan mudahnya direkam dan diliput dengan menggunakan telepon genggam atau piranti digital yang dibawa untuk selanjutnya di-*upload* ke internet untuk dapat diakses dan dinikmati oleh publik. Tentu saja yang bersangkutan dengan berbagai dalih menyangkal dirinya yang berada dalam rekaman tersebut dan berbalik bersengketa serta menuntut si "wartawan amatir" tersebut.

Ketiga adalah banyaknya beredar email-email gelap alias "email kaleng" yang isinya berupa ancaman, tuduhan, diskriminasi, maupun hal-hal lain yang bersifat menakut-nakuti maupun mendeskreditkan seseorang atau lembaga di dunia maya. Walaupun tidak jelas identitas pengirimnya (baca: *anonymous*), namun jika isi ancaman terkait dengan terorisme misalnya, atau mereka yang diancam adalah tokoh-tokoh penting seperti para pejabat pemerintahan, terlepas dari benar atau tidaknya konten ancaman tersebut, keberadaannya patutlah ditanggapi secara serius. Misalnya adalah kasus beredarnya surat wasiat pelaku bom Bali yang mengancam keselamatan Presiden Republik Indonesia yang langsung mendapatkan tanggapan serius dari polisi, intelijen, dan segenap penegak hukum beserta praktisi keamanan internet yang ada di tanah air.

Keempat adalah terjadinya berbagai jenis kejahatan atau *forgery* yang bersifat melakukan penipuan identitas atau *phishing* terhadap para pelanggan perusahaan tertentu, terutama bank. Modul operandi yang paling banyak dipergunakan adalah menggunakan media email dan SMS. Dengan berkedok seolah-olah yang bersangkutan merupakan pihak yang sah, para pelanggan diminta untuk melakukan tindakan pengiriman uang maupun pemberitahuan kata kunci (baca: *password*) tertentu yang bermuara pada raibnya harta finansial milik si korban tersebut. Kejadian di dunia maya ini benar-benar berdampak pada dunia nyata karena si pelaku tahu persis kelemahan atau keterbatasan pengetahuan dari para calon korbannya.

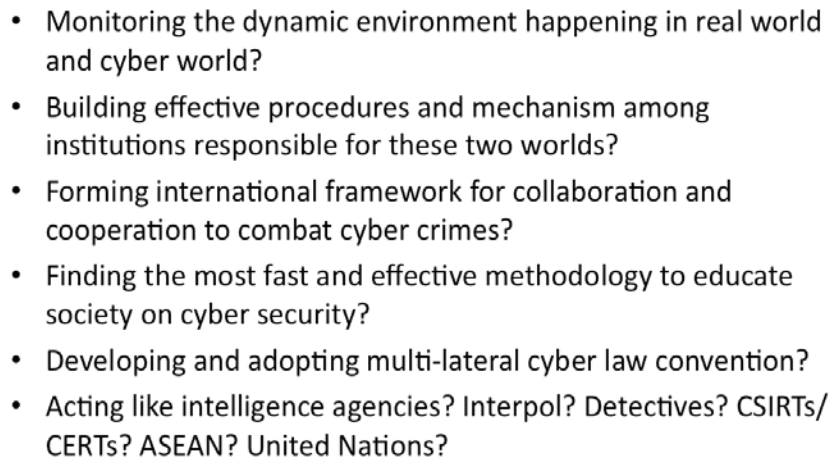
Kelima merupakan suatu tindakan di dunia nyata yang bermula dari diskursus yang terjadi di dunia nyata melalui email, situs, *mailing list, newsgroup, social networking application, chatting room,* dan lain sebagainya yang bernuansa kampanye atau persuasif untuk melakukan tindakan tertentu – baik yang bersifat positif maupun negatif. Misalnya adalah sebuah email yang menceritakan suatu peristiwa yang berbau SARA. Terlepas dari benar atau tidak, keberadaan email berantai ini telah memicu kemarahan pihak-pihak yang merasa tersinggung dan berniat untuk melakukan demo besar-besaran di dunia nyata. Atau sebuah *mailing list* yang menyarankan agar para anggotanya untuk melakukan hal tertentu, seperti: tidak berpartisipasi dalam pemilu alias menjadi golput, memboikot produk-produk asing, memusuhi organisasi tertentu, dan lain sebagainya. Tentu saja segala bentuk himbauan di dunia maya ini sedikit banyak berpengaruh pada kehidupan sehari-hari.

Keenam adalah kejadian di dunia nyata akibat berbagai penilaian yang dilakukan oleh sejumlah individu atau komunitas terhadap suatu hal tertentu – barang, jasa, produk, individu, organisasi, dan lain sebagainya - yang memberikan dampak cukup luas di dunia nyata. Lihatlah bagaimana seorang pelanggan yang

kecewa dengan kualitasnya produk yang dibelinya kemudian membeberkan seluruh kegundahannya di dunia maya. Atau seorang wisatawan yang mengalami pengalaman buruk ketika sedang berada di suatu daerah wisata tertentu yang menyarankan orang lain untuk tidak pergi ke sana. Atau bagaimana sekelompok orang yang pernah merasa dirugikan oleh pelayanan bank tertentu menceritakan pengalaman pribadi masing-masing mereka yang dapat berakibat terjadinya *rush* dari para pelanggan yang masih menjadi nasabah aktif di bank yang bersangkutan, dan lain sebagainya. Jika pada jaman dahulu pengalaman-pengalaman semacam ini dapat terisolisasi beritanya, maka dengan adanya internet, publik dapat turut mengetahuinya dalam waktu sangat singkat.

4.4 MEMBANGUN STRATEGI PENGAMANAN DUA DUNIA

Keseluruhan fenomena di atas menyiratkan perlu dilakukannya usaha yang terus menerus dan tidak berkesudahan untuk mengedukasi dan meningkatkan wawasan masyarakat dan komunitas terkait dengan pentingnya berhati-hati serta memperhatikan etika ketika berinteraksi di dunia nyata maupun di dunia nyata. Jika terjadi peristiwa yang tidak diinginkan terjadi di dunia nyata, seluruh pihak harus bersiap-siap jika hal tersebut akan dan pasti menular ke dunia maya – sehingga seluruh aset data maupun informasi yang ada di internet haruslah dijaga keamanannya. Demikian pula mereka yang berfikir dapat berkomunikasi secara bebas tak terbatas di internet patut pula berhati-hati karena jika yang bersangkutan melakukan perbuatan tertentu yang dapat merugikan orang lain dan telah diatur mekanismenya dalam undang-undang yang berlaku, maka hukuman perdata maupun pidana di dunia nyata dapat ditimpakan kepadanya.



Gambar 4.8 *Sejumlah Pertanyaan Strategi Pengamanan Internet*

Komunitas internet dunia sadar akan seluruh hal ini, dan mereka semua pun paham akan kompleksitas penanganannya mengingat internet merupakan sebuah

jejaring raksasa yang bersifat lintas bidang dan geografis. Beberapa pertanyaan mendasar sering terbersit oleh komunitas keamanan internet.

Berbagai pertanyaan yang terkait dengan strategi serta prosedur mengamankan internet antara lain:

1. Perlukah ada lembaga yang mengawasi dunia maya seperti halnya pemerintahan dan penegakan hukum di dunia nyata?
2. Haruskah ada suatu cara atau mekanisme atau prosedur yang menghubungkan kedua dunia tersebut?
3. Perlukah ada sebuah konvensi internasional yang harus diratifikasi oleh seluruh pihak yang paham akan perlunya kolaborasi dalam mengamankan internet?
4. Apakah perlu dilakukan berbagai kerjasama bilateral atau multilateral antar negara terkait dengan pemanfaatan internet?
5. Perlukah lembaga seperti interpol dibentuk di internet? Atau CERTs dan CSIRTs saja sudah cukup membantu untuk melakukan mitigasi keamanan internet?
6. Apakah lembaga semacam PBB, ITU, ASEAN, dan lain sebagainya perlu membentuk kelompok kerja khusus untuk mengamankan internet?

… dan lain sebagainya.

Tentu saja keseluruhan ide maupun inisiatif yang ada akan memberikan sedikit banyak kontribusi terhadap keamanan internet. Namun berpegang pada prinsip bahwa kekuatan sebuah rantai sangat ditentukan oleh mata rantai terlemah, jelas tersirat bahwa pada akhirnya faktor manusia lah yang akan menentukan kualitas keamanan dari internet. Dengan berpegang pada kenyataan bahwa di dunia ini lebih banyak jumlah orang baiknya dibandingkan dengan yang jahat, maka mudah-mudahan di dunia maya situasi yang sama dapat terjadi, sehingga keberadaan internet lebih dirasakan manfaatnya daripada kerugiannya.

-oo0oo-

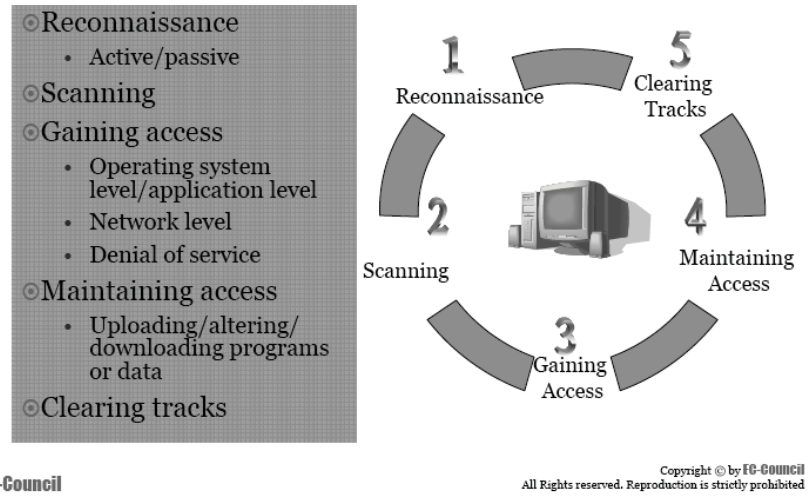
~ 5 ~

STRATEGI DAN CARA HACKER DALAM MENYERANG KEAMANAN INTERNET

Capaian Pembelajaran (*Learning Outcomes*):

1. Menjelaskan Teknik Reconnaissance
2. Menjelaskan Teknik Scanning
3. Menjelaskan Teknik Gaining Access
4. Menjelaskan Teknik Maintaining Access
5. Menjelaskan Teknik Covering Tracks

Mendengar kata “hacker”, biasanya jaman dahulu langsung tergambar di dalam benak seseorang dengan kata mata tebal dan bersifat “kuper” (kurang pergaulan) yang berjam-jam berada di depan komputer untuk berusaha masuk ke dalam sistem pertahanan jaringan yang berada dalam wilayah institusi lain. Kalau hal yang sama dibayangkan sekarang, yang ada di dalam gambaran pikiran adalah pemuda berambut gondrong yang sedang memelototi komputer sambil makan sepotong pizza, yang menggunakan seluruh kreatifitasnya untuk dapat “membobol” sistem pertahanan jaringan komputer dari organisasi yang menjadi targetnya. Terlepas dari perbedaan dulu dan sekarang, ada satu kesan yang sering tampak dalam membayangkan aktivitas mereka. Sekilas nampak apa yang mereka lakukan bersifat sporadis, serampangan, sembarangan, tidak tersruktur, “trial and error”, dan lain sebagainya. Pada dasarnya, apakah yang bersangkutan merupakan “hacker jalanan” atau pun “hacker profesional”, yang bersangkutan sebenarnya melakukan langkah-langkah proses aktivitas yang terstruktur dengan baik untuk dijaga efektivitas dan efisiensinya. EC-Council, sebuah institusi terkemuka di dunia yang bergerak di bidang keamanan informasi dan internet membagi langkah-langkah yang dilakukan hacker dalam “beroperasi” menjadi 5 (lima) bagian yang berurutan satu dengan yang lainnya, yaitu: (i) Reconnaissance; (ii) *Scanning*; (iii) *Gaining Access*; (iv) *Maintaining Access*; dan (v) *Clearing Tracks*.



Gambar 5.1 *Lima Langkah Operasional Hacker*

5.1 MENJELASKAN TEKNIK RECONNAISSANCE

Yang dimaksud dengan “reconnaissance” adalah suatu tahap persiapan dimana hacker atau pihak yang akan melakukan “serangan” berusaha mencari informasi sebanyak-banyaknya mengenai target atau sasaran sistem yang ingin diserang sebelum rangkaian proses penyerangan dilaksanakan. Ada dua jenis model

reconnaissance yang dikenal, yaitu yang bersifat pasif dan aktif. Usaha terkait dikatakan aktif apabila tidak ada interaksi langsung antara pihak penyerang dengan target atau sasaran yang ingin diserang. Katakanlah seorang hacker yang ingin menyerang sebuah bank, maka yang bersangkutan akan melakukan studi pustaka atau mempelajari lewat *browsing* internet mengenai seluk beluk sistem yang ingin diserang. Dengan mendapatkan referensi dari berbagai sumber seperti artikel, majalah, koran, *vendor release*, dan lain sebagainya – tidak jarang yang bersangkutan dapat mengetahui jenis sistem komputer yang dipergunakan oleh bank terkait, lengkap dengan tipe sistem operasi dan topologi jaringannya. Sementara proses terkait dikatakan aktif, jika dilakukan aktivitas interaksi secara langsung dengan sistem atau pemangku kepentingan pada bank terkait. Misalnya sang hacker berpura-pura ingin membuka rekening bank sehingga dapat mempelajari sistem komputer yang dioperasikan oleh *customer service*, atau menelepon ke *help desk* bank yang bersangkutan untuk melihat mekanisme dan prosedur yang dipergunakan dalam menjawab kebutuhan pelanggan, atau dengan cara mengunjungi situs *internet bank* terkait untuk melihat dan menduga-duga teknologi yang berada di belakang aplikasi tersebut, dan lain sebagainya.

5.2 MENJELASKAN TEKNIK SCANNING

Setelah mengetahui seluk beluk sekilas mengenai lingkungan dan karakteristik dari target sistem yang ingin diserang, barulah tahap berikutnya adalah melakukan "scanning". Sesuai dengan definisi dan konteksnya, "scan" merupakan sebuah proses dimana hacker dengan menggunakan berbagai alat dan *tools* berusaha mencari celah masuk atau lokasi tempat serangan akan diluncurkan. Seperti halnya seorang pencuri yang dapat masuk ke dalam rumah melalui pintu, jendela, atap rumah, atau gorong-gorong bawah tanah, seorang hacker melalui aktivitas ini berusaha mencari lubang-lubang kerawanan tempat serangan masuk. Biasanya, yang akan di-*scan* pertama kali adalah *port* dalam sistem komputer *(port scanning)*, atau melalui pemetaan jaringan *(network mapping)*, atau melalui pencarian kerawanan/kerapuhan *(vulnerability scanning)*, dan lain sebagainya. Hal yang perlu baik-baik diperhatikan adalah bahwa perbuatan "scanning" terhadap sistem jaringan komputer milik orang lain pada dasarnya merupakan aktivitas yang melanggar undang-undang, kecuali seijin pihak yang berkepentingan[1]. Dan jika tidak hati-hati, maka pihak terkait akan dengan mudah mengetahui kegiatan ini, terlebih-lebih jika yang bersangkutan memiliki perangkat IDS*(Intrusion Detection System)* yang dapat mendeteksi seandainya terjadi penyusupan atau *intrusion* dari

1 Misalnya aktivitas tersebut dilakukan sebagai bagian dari serangkaian program atau proyek "penetration test" yang dilakukan oleh hacker.

pihak luar ke dalam sistem yang dilindungi. Hasil dari tahap *scanning* adalah diketemukannya cara bagi hacker untuk masuk ke dalam sistem.

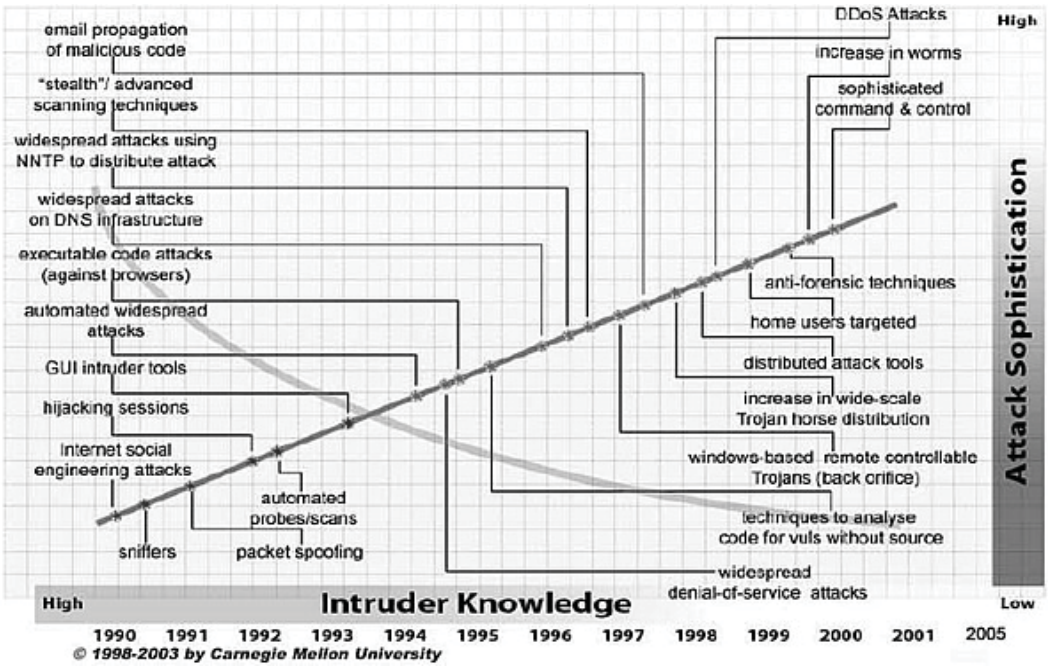
5.3 MENJELASKAN TEKNIK GAINING ACCESS

Jika dua tahap sebelumnya yaitu *reconnaissance*dan *scanning* masih bersifat "pasif", dalam arti kata bahwa aktivitas yang dilakukan masih sekedar meraba-raba kehandalan sistem yang ingin diserang, pada tahap *gaining access* ini usaha penetrasi aktif mulai dilaksanakan. Pada dasarnya yang dilakukan oleh hacker adalah melakukan eksploitasi terhadap kelemahan, kerawanan, dan/atau kerapuhan (baca: *vulberability*) yang ada pada sistem. Cara mendapatkan akses yang dimaksud sangatlah beraneka-ragam, tergantung karakteristik dan hasil dari proses *scanning* sebelumnya. Misalnya adalah dengan melakukan *password cracking* alias mencoba menebak hingga "memaksakan" kata kunci rahasia yang memungkinkan hacker memperoleh hak akses untuk masuk ke dalam sistem. Jenis lainnya adalah mekakukan aktivitas yang menyebabkan terjadinya fenomena *buffer overflows* sehingga data rahasia yang seharusnya tersimpan aman dapat diakses dan diambil oleh yang tidak memiliki otoritas. Pendekatan *gaining access* lainnya adalah dengan melakukan apa yang dinamakan sebagai *session hijacking* alias melakukan pembajakan hak akses seseorang oleh hacker sehingga yang bersangkutan dapat masuk ke dalam sistem yang bukan merupakan teritorinya. Proses memperoleh hak akses ini dapat berlangsung dalam waktu yang cukup singkat hingga memakan waktu yang relatif panjang, tergantung dari sejumlah faktor, seperti: arsitektur dan konfigurasi jaringan, jenis sistem operasi yang dipergunakan, keahlian hacker yang bersangkutan, jenis *tool* atau alat bantu yang dipergunakan, dan lain sebagainya. Jika hacker telah berhasil masuk ke tahap ini, maka ekspose resiko yang dihadapi organisasi atau institusi yang memiliki sistem terkait sudah sedemikian tingginya. Gagal mendeteksi percobaan ini akan mendatangkan malapetaka yang cukup besar bagi yang bersangkutan.

5.4 MENJELASKAN TEKNIK MAINTAINING ACCESS

Tahap ini adalah sebuah periode dimana setelah hacker berhasil masuk ke dalam sistem, yang bersangkutan berusaha untuk tetap bertahan memperoleh hak akses tersebut. Pada saat inilah sering diistilahkan bahwa sistem yang ada telah berhasil diambil alih oleh pihak yang tidak berhak (baca: *compromised*). Ketika periode ini berlangsung, kendali sepenuhnya berada di tangan hacker. Yang bersangkutan dapat melakukan apa saja yang diinginkannya, seperti melakukan hal-hal yang tidak berbahaya – seperti menuliskan pesan peringatan kepada pemilik sistem – hingga melakukan tindakan yang destruktif, seperti mencuri data, merubah

konten, menanam aplikasi mata-mata, mengacaukan konfigurasi, memanipulasi informasi, merusak isi *hard disk*, dan lain sebagainya. Tidak banyak yang dapat dilakukan oleh pemilik sistem jika hacker telah memasuki tahap ini, kecuali berusaha melakukan *counter measures* agar dampak atau akibat negatif yang ditimbulkan hacker dapat ditekan seminimal mungkin.



Gambar 5.2 *Aneka Ragam Jenis Serangan ke Sistem*

5.5 MENJELASKAN TEKNIK COVERING TRACKS

Akhirnya tahap akhir yang dipandang sulit dan sering dilupakan oleh hacker – karena alasan buru-buru, ceroboh, atau kurang keahlian – adalah aktivitas penghapusan jejak. Dikatakan sulit karena selain banyak hal yang harus dilakukan oleh hacker dan cukup memakan waktu, penegak hukum selalu saja memiliki cara untuk mencari tahu jejak keteledoran pelaku kejahatan seperti hacker ini. Untuk dapat melakukan penghapusan jejak secara nyaris "sempurna", selain membutuhkan sumber daya yang tidak sedikit, diperlukan pula pengetahuan dan keahlian yang prima dari hacker yang bersangkutan. Rekam jejak memperlihatkan bahwa dari berbagai jenis kejahatan hacking di dunia, jarang sekali yang jarang terungkap pelaku dan modus operandinya. Berbagai jenis pengapusan jejak banyak dikenal di kalangan hacker, misalnya teknik *steganography, tunneling, log files altering,* dan lain sebagainya.

Dengan mengetahui tahapan-tahapan hacker beroperasi ini maka diharapkan para praktisi pengaman jaringan komputer dan internet paham betul kompleksitas

proses dan ekspose resiko yang dihadapi sehari-hari. Semakin dalam seorang hacker masuk ke dalam rangkaian proses terkait, semakin tinggi ancaman resiko yang dihadapi oleh calon korban yang bersangkutan.

-oo0oo-

~ 6 ~

SEPULUH ASPEK KEAMANAN DALAM STANDAR INTERNASIONAL

Capaian Pembelajaran (*Learning Outcomes*):

1. Menyebutkan Berbagai Standar Keamanan
2. Menjelaskan Pentingya Keamanan Informasi
3. Menyampaikan Alasan Perlunya Keamanan Informasi
4. Mengidentifikasi Pemangku Kepentingan Keamanan Informasi
5. Menyusun Strategi Sosialisasi Organisasi
6. Mengimplementasikan Keamanan Informasi
7. Menerapkan Sistem Keamanan Informasi
8. Menetapkan Standar Keamanan Informasi
9. Menyusun Dokumen Standar
10. Memahami Sepuluh Aspek Keamanan Informasi

6.1 MENYEBUTKAN BERBAGAI STANDAR KEAMANAN

ISO (the International Organization for Standarization) dan IEC (the International Electrotechnical Commission) membentuk sistem khusus untuk standardisasi universal. Badan-badan nasional anggota ISO dan IEC berpartisipasi dalam pengembangan standardisasi internasional melalui panitia teknis yang disepakati oleh organisasi-organisasi yang terpercaya keahliannya dalam aktivitas-aktivitas teknis. Panitia Teknis ISO dan IEC berkolaborasi dengan prinsip saling menguntungkan. Organisasi-organisasi internasional lainnya, baik pemerintah maupun non-pemerintah, bekerja sama dengan ISO dan IEC, juga ambil bagian dalam kegiatan tersebut.

Di bidang teknologi informasi, ISO dan IEC telah menetapkan suatu Panitia Teknis Gabungan (ISO/IEC JTC 1). Rancangan standar internasional yang diadopsi oleh panitia teknis gabungan diedarkan kepada seluruh badan-badan nasional untuk diambil suara (voting). Penentuan sebagai satu sebuah standar internasional memerlukan persetujuan minimal 75% dari badan-badan nasional yang memberikan suara (pilihan).

Perlu diperhatikan terhadap kemungkinan bahwa beberapa elemen dari standar internasional ini, masih menjadi subyek bahasan hak-hak paten. Dalam hal ini, ISO dan IEC tidak bertanggung jawab untuk mengidentifikasi bagian manapun tentang hak-hak paten tersebut. Standar internasional ISO/IEC 17799 dipersiapkan oleh Institut Standar Inggris (dikenal sebagai BS 7799) dan diadopsi di bawah “prosedur jalur cepat” khusus oleh Panitia Teknis Gabungan ISO/IEC JTC 1, Teknologi Informasi, secara bersamaan dengan persetujuan dari badan-badan nasional ISO dan IEC).

6.2 MENJELASKAN PENTINGYA KEAMANAN INFORMASI

Informasi merupakan aset yang sangat berharga bagi sebuah organisasi karena merupakan salah satu sumber daya strategis dalam meningkatkan nilai usaha. Oleh karena itu maka perlindungan terhadap informasi (keamanan informasi) merupakan hal yang mutlak harus diperhatikan secara sungguh-sungguh oleh segenap jajaran pemilik, manajemen, dan karyawan organisasi yang bersangkutan. Keamanan informasi yang dimaksud menyangkut kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman terhadapnya sehingga daapt menyebabkan terjadinya kerugian-kerugian bagi kelangsungan hidup organisasi.

Informasi dikumpulkan, disimpan, diorganisasikan, dan disebarluaskan dalam berbagai bentuk – baik dokumen berbasis kertas hingga berkas elektronik. Apapun

bentuk maupun cara penyimpanannya, harus selalu ada upaya dan untuk melindungi keamanannya sebaik mungkin. Keamanan yang dimaksud harus memperhatikan sejumlah aspek, yaitu:

1. Kerahasiaan – memastikan bahwa informasi tertentu hanya dapat diakses oleh mereka yang berhak atau memiliki wewenang untuk memperolehnya;
2. Integritas – melindungi akurasi dan kelengkapan informasi melalui sejumlah metodologi pengolahan yang efektif; dan
3. Ketersediaan – memastikan bahwa informasi terkait dapat diakses oleh mereka yang berwenang sesuai dengan kebutuhan.

Jaminan kemanan informasi dapat dicapai melalui aktivitas penerapan sejumlah kontrol yang sesuai. Kontrol yang dimaksud meliputi penerapan berbagai kebijakan, prosedur, struktur, praktek, dan fungsi-fungsi tertentu. Keseluruhan kontrol tersebut harus diterapkan oleh organisasi agar seluruh sasaran keamanan yang dimaksud dapat tercapai.

6.3 MENYAMPAIKAN ALASAN PERLUNYA KEAMANAN INFORMASI

Menjaga keamanan informasi berarti pula perlunya usaha dalam memperhatikan faktor-faktor keamanan dari keseluruhan piranti pendukung, jaringan, dan fasilitas lain yang terkait langsung maupun tidak langsung dengan proses pengolahan informasi. Dengan amannya keseluruhan lingkungan tempat informasi tersebut berada, maka kerahasiaan, integritas, dan ketersediaan informasi akan dapat secara efektif berperan dalam meningkatkan keunggulan, keuntungan, nilai komersial, dan citra organisasi yang memiliki aset penting tersebut.

Adalah merupakan suatu kenyataan bahwa pada abad globalisasi ini, berbagai organisasi dihadapkan pada sejumlah ancaman-ancaman keamanan informasi dari berbagai sumber, seperti yang diperlihatkan dengan keberadaan sejumlah kasus kejahatan komputer secara sengaja, seperti: pencurian data, aktivitas spionase, percobaan *hacking*, tindakan vandalisme, dan lain-lain, maupun ancaman yang disebabkan karena kejadian-kejadian lain seperti bencana alam, misalnya: banjir, gempa bumi, tsunami, dan kebakaran. Bergantungnya kinerja organisasi pada sistem informasi mengandung arti bahwa keseluruhan ancaman terhadap keamanan tersebut merupakan portofolio resiko yang dihadapi oleh organisasi yang bersangkutan.

Perencanaan dan pengembangan sistem keamanan informasi yang baik semakin mendapatkan tantangan dengan adanya interkoneksi antara berbagai jaringan publik dan privat, terutama terkait dengan proses pemakaian bersama sejumlah sumber daya informasi untuk meningkatkan optimalisasi akses. Manfaat yang

didapatkan melalui pendistribusian komputasi ini disaat yang sama melemahkan efektivitas kontrol secara terpusat, yang berarti pula menciptakan suatu kelemahan-kelemahan baru pada sistem tersebut. Kenyataan memperlihatkan bahwa sebagian besar sistem informasi yang dirancang dan dibangun dewasa ini kurang begitu memperhatikan faktor-faktor keamanan tersebut. Padahal untuk membangun sistem keamanan informasi yang baik, perlu dilakukan sejumlah langkah-langkah metodologis tertentu.

Keamanan informasi yang baik dapat dicapai melalui penerapan sejumlah upaya-upaya teknis (operasional) yang didukung oleh berbagai kebijakan dan prosedur manajemen yang sesuai. Proses tersebut dimulai dari pengidentifikasian sejumlah kontrol yang relevan untuk diterapkan dalam organisasi, yang tentu saja harus berdasarkan pada analisa kebutuhan aspek keamanan informasi seperti apa yang harus dimiliki perusahaan. Setelah kebijakan, prosedur, dan panduan teknis operasional mengenai kontrol-kontrol yang harus diterapkan dalam organisasi disusun, langkah berikutnya adalah sosialisasi keseluruhan piranti tersebut ke segenap lapisan manajemen dan karyawan organisasi untuk mendapatkan dukungan dan komitmen. Selanjutnya, para pihak berkepentingan lain yang berada di luar organisasi – seperti pemasok, pelanggan, mitra kerja, dan pemegang saham – harus pula dilibatkan dalam proses sosialisasi tersebut karena mereka merupakan bagian tidak terpisahkan dari sistem keamanan informasi yang dibangun. Keterlibatan sejumlah pakar maupun ahli dari luar organisasi kerap kali dibutuhkan untuk membantu organisasi dalam menerapkan langkah-langkah di tersebut. Dengan adanya pengetahuan yang mereka miliki, terutama dalam membantu organisasi menyusun kebutuhan dan mengidentifikasikan kontrol-kontrol yang dibutuhkan, niscaya sistem keamanan informasi yang dibangun dapat lebih efektif dan ekonomis.

6.4 MENGIDENTIFIKASI PEMANGKU KEPENTINGAN KEAMANAN INFORMASI

Dari penjabaran sebelumnya jelas terlihat bahwa semua pihak di dalam organisasi (manajemen dan karyawan) maupun di luar organisasi (pemasok, pelanggan, mitra kerja, dan pemegang saham) bertanggung jawab secara penuh dalam proses keamanan informasi. Hal tersebut disebabkan karena mereka semua terlibat secara langsung maupun tidak langsung dalam proses penyediaan, penyimpanan, pemanfaatan, dan penyebarluasan informasi dalam organisasi. Untuk menjamin adanya kesadaran, kemauan, dan komitmen untuk melakukan hal tersebut, maka perlu adanya pihak yang memiliki tugas dan kewajiban khusus untuk memantau efektivitas keamaman informasi tersebut. Keberadaan pihak tersebut mutlak

dibutuhkan oleh organisasi dalam berbagai bentuknya, seperti: perusahaan komersial, institusi pemerintah, organisasi publik, lembaga nirlaba, dan lain sebagainya.

6.5 MENYUSUN STRATEGI SOSIALISASI ORGANISASI

Pemahaman dan kesadaran mengenai pentingnya memperhatikan aspek-aspek keamanan informasi harus ditanamkan sedini mungkin oleh setiap organisasi terhadap seluruh jajaran manajemen dan karyawannya. Setiap individu yang berada di dalam organisasi memiliki tanggung jawab untuk melindungi keamanan informasi yang dimilikinya, sebagaimana layaknya memperlakukan hal yang sama terhadap aset-aset berharga lainnya. Dalam kaitan dengan hal ini, harus terdapat kebijakan menyangkut pemberian sanksi bagi mereka yang lalai memperhatikan hal ini maupun penghargaan bagi mereka yang berprestasi mempromosikan dan menerapkan keamanan informasi di organisasi terkait.

6.6 MENGIMPLEMENTASIKAN KEAMANAN INFORMASI

Tentunya proses keamanan informasi harus dimulai dari menjaga tempat-tempat atau fasilitas fisik dimana informasi beserta piranti/peralatan pendukungnya disimpan. Mengingat bahwa hampir seluruh fungsi dalam organisasi memiliki tanggung jawab dalam mengelola informasinya masing-masing, maka setiap individu dalam berbagai fungsi-fungsi tersebut harus secara aktif menjaga keamanan informasi. Dengan berkembangnya teknologi akses informasi dari jarak jauh melalui pemanfaatan jaringan komputer, maka ruang lingkup keamanan menjadi semakin besar dan kompleks, karena sudah tidak dibatasi lagi oleh sekat-sekat lingkungan fisik tertentu. Perkembangan internet yang telah membentuk sebuah dunia maya tempat berbagai individu maupun komunitas berinteraksi (tukar menukar informasi) secara elektronik memperlihatkan bagaimana kompleksnya keamanan area baik secara fisik maupun virtual – yang tentu saja akan sangat berpengaruh terhadap manajemen kontrol yang akan dipilih dan diterapkan.

6.7 MENERAPKAN SISTEM KEAMANAN INFORMASI

Untuk dapat membangun dan menerapkan sistem keamanan informasi yang baik, sebaiknya organisasi memulainya dari upaya melakukan kajian atau telaah terhadap resiko-resiko keamanan yang mungkin timbul. Kajian yang dimaksud dapat diterapkan dalam tingkatan organisasi, maupun pada tataran sub bagian atau fungsi organisasi tertentu, seperti sistem informasi, komponen, layanan, dan lain sebagainya – sesuai dengan skala prioritas yang ada.Kajian resiko yang dimaksud merupakan suatu pendekatan sistematis dari proses:

1. Identifikasi terhadap kejadian-kejadian apa saja yang dapat mengancam keamanan informasi perusahaan dan potensi dampak kerugian yang ditimbulkan jika tidak terdapat kontrol yang memadai; dan
2. Analisa tingkat kemungkinan (probabilitas) terjadinya hal-hal yang tidak diinginkan tersebut akibat adanya sejumlah kelemahan pada sistem yang tidak dilindungi dengan kontrol tertentu.

Hasil dari kajian tersebut akan menghasilkan arahan yang jelas bagi manajemen dalam menentukan prioritas dan mengambil sejumlah tindakan terkait dengan resiko keamanan informasi yang dihadapi. Dengan adanya prioritas yang jelas maka akan dapat didefinisikan kontrol-kontrol mana saja yang perlu diterapkan. Perlu diperhatikan bahwa langkah-langkah tersebut harus dilakukan secara kontinyu dan periodik, mengingat dinamika perubahan organisasi dan lingkungan eksternal yang sedemikian cepat. Langkah-langkah interaktif yang dimaksud meliputi:

1. Menganalisa perubahan kebutuhan dan prioritas organisasi yang baru sesuai dengan pertumbuhannya;
2. Mempelajari ancaman-ancaman atau kelamahan-kelemahan baru apa yang terjadi akibat perubahan yang ada tersebut; dan
3. Memastikan bahwa kendali-kendali yang dimiliki tetap efektif dalam menghadapi ancaman-ancaman kejadian terkait.

Perlu dicatat bahwa peninjauan berkala tersebut harus dilakukan pada bagian organisasi dengan tingkat kedalaman tertentu sesuai dengan hasil analisa resiko yang telah dilakukan sebelumnya. Karena keberadaan kontrol ini akan sangat berpengaruh terhadap kinerja sebuah organisasi, maka proses telaah resiko harus dimulai dari tingkat, agar mereka yang berwenang dapat menilainya berdasarkan tingkat kepentingan terteinggi (pendekatan *top down*).

6.8 MENETAPKAN STANDAR KEAMANAN INFORMASI

Keberadaan dan kepatuhan terhadap standar merupakan hal mutlak yang harus dimiliki oleh pihak manapun yang ingin menerapkan sistem keamanan informasi secara efektif. Sejumlah alasan utama mengapa standar diperlukan adalah untuk menjamin agar:

1. Seluruh pihak yang terlibat dalam proses keamanan informasi memiliki kesamaan pengertian, istilah, dan metodologi dalam melakukan upaya-upaya yang berkaitan dengan keamanan data;
2. Tidak terdapat aspek-aspek keamanan informasi yang terlupakan karena standar yang baik telah mencakup keseluruhan spektrum keamanan informasi

yang disusun melalui pendekatan komprehensif dan holistik (utuh dan menyeluruh);

3. Upaya-upaya untuk membangun sistem keamanan informasi dilakukan secara efektif dan efisien dengan tingkat optimalisasi yang tinggi, karena telah memperhatikan faktor-faktor perkembangan teknologi serta situasi kondisi yang berpengaruh terhadap organisasi;
4. Tingkat keberhasilan dalam menghasilkan sistem keamanan informasi yang berkualitas menjadi tinggi, karena dipergunakan standar yang sudah teruji kehandalannya.

6.9 MENYUSUN DOKUMEN STANDAR

Seperti yang telah dijelaskan sebelumnya, proses awal yang harus dilakukan setiap organisasi adalah melakukan kajian awal untuk mengidentifikasikan kebutuhan keamanan, mengingat setiap organisasi memiliki sifat uniknya masing-masing. Berdasarkan hasil tersebut, pilihlah kontrol-kontrol sesuai yang dapat diambil dalam dokumen standar ini, maupun dari sumber-sumber lain untuk melengkapinya manakala dibutuhkan. Setelah itu susunlah perencanaan program penerapan kontrol-kontrol yang dimaksud dengan melibatkan pihak internal maupun eksternal organisasi sesuai dengan kebutuhan. Perlu diperhatikan bahwa sejumlah kontrol sifatnya mutlak harus dimiliki oleh sebuah organisasi, sementara berbagai kontrol lainnya hakekatnya ditentukan oleh situasi dan kondisi organisasi yang bersangkutan. Disamping itu terdapat pula sejumlah kontrol yang harus diperhatikan secara sungguh-sungguh karena memiiki implikasi besar karena menyangkut kepentingan publik atau kontinuitas keberadaan organisasi.

6.10 MEMAHAMI SEPULUH ASPEK KEAMANAN INFORMASI

Berikut adalah penjabaran ringkas dari sepuluh domain atau aspek yang harus diperhatikan terkait dengan isu keamanan informasi dalam sebuah organisasi atau institusi.

1. **Kebijakan Keamanan**: untuk memberikan arahan dan dukungan manajemen keamanan informasi. Manajemen harus menetapkan arah kebijakan yang jelas dan menunjukkan dukungan, serta komitmen terhadap keamanan informasi melalui penerapan dan pemeliharaan suatu kebijakan keamanan informasi di seluruh tataran organisasi;
2. **Pengorganisasian Keamanan**: untuk mengelola keamanan informasi dalam suatu organisasi. Satu kerangka kerja manajemen harus ditetapkan untuk memulai dan mengkontrol penerapan keamanan informasi di dalam organisasi.Fora manajemen dengan kepemimpinan yang kondusif harus dibangun un-

tuk menyetujui kebijakan keamanan informasi, menetapkan peran keamanan dan mengkoordinir penerapan keamanan di seluruh tataran organisasi. Jika diperlukan, pendapat pakar keamanan informasi harus dipersiapkan dan tersedia dalam organisasi. Hubungan dengan pakar keamanan eksternal harus dibangun untuk mengikuti perkembangan industri, memonitor standar dan metode penilaian serta menyediakan penghubung yang tepat, ketika berurusan dengan insiden keamanan. Pendekatan multi-disiplin terhadap keamanan informasi harus dikembangkan, misalnya dengan melibatkan kerjasama dan kolaborasi di antara manajer, pengguna, administrator, perancang aplikasi, pemeriksa dan staf keamanan, serta keahlian di bidang asuransi dan manajemen resiko;

3. **Klasifikasi dan Kontrol Aset**: untuk memelihara perlindungan yang tepat bagi pengorganisasian aset.Semua aset informasi penting harus diperhitungkan keberadaannya dan ditentukan kepemilikannya. Akuntabilitas terhadap aset akan menjamin terdapatnya perlindungan yang tepat. Pemilik semua aset penting harus diidentifikasi dan ditetapkan tanggung jawabnya untuk memelihara sistem kontrol tersebut. Tanggungjawab penerapan sistem kontrol dapat didelegasikan. Akuntabilitas harus tetap berada pada pemilik aset;
4. **Pengamanan Personil**: untuk mengurangi resiko kesalahan manusia, pencurian, penipuan atau penyalahgunaan fasilitas.Tanggung jawab keamanan harus diperhatikan pada tahap penerimaan pegawai, dicakup dalam kontrak dan dipantau selama masa kerja pegawai. Penelitian khusus harus dilakukan terhadap calon pegawai khususnya di bidang tugas yang rahasia. Seluruh pegawai dan pengguna pihak ketiga yang menggunakan fasilitas pemrosesan informasi harus menanda-tangani perjanjian kerahasiaan (non-disclosure);
5. **Keamanan Fisik dan Lingkungan**: untuk mencegah akses tanpa otorisasi, kerusakan, dan gangguan terhadap tempat dan informasi bisnis. Fasilitas pemrosesan informasi bisnis yang kritis dan sensitif harus berada di wilayah aman, terlindung dalam perimeter keamanan, dengan rintangan sistem pengamanan dan kontrol masuk yang memadai. Fasilitas tersebut harus dilindungi secara fisik dari akses tanpa ijin, kerusakan dan gangguan. Perlindungan harus disesuaikan dengan identifikasi resiko. Disarankan penerapan kebijakan clear desk dan clear screen untuk mengurangi resiko akses tanpa ijin atau kerusakan terhadap kertas, media dan fasilitas pemrosesan informasi.
6. **Komunikasi dan Manajemen Operasi**: untuk menjamin bahwa fasilitas pemrosesan informasi berjalan dengan benar dan aman. Harus ditetapkan tanggungjawab dan prosedur untuk manajemen dan operasi seluruh fasilitas pemrosesan informasi. Hal ini mencakup pengembangan instruksi operasi yang tepat dan prosedur penanganan insiden. Dimana mungkin harus ditetapkan

pemisahan tugas, untuk mengurangi resiko penyalahgunaan sistem karena kecerobohan atau kesengajaan;

7. **Pengontrolan Akses**: untuk mencegah akses tanpa ijin terhadap sistem informasi. Prosedur formal harus diberlakukan untuk mengkontrol alokasi akses, dari pendaftaran awal dari pengguna baru sampai pencabutan hak pengguna yang sudah tidak membutuhkan lagi akses ke sistem informasi dan layanan. Perhatian khusus harus diberikan, jika diperlukan, yang dibutuhkan untuk mengkontrol alokasi hak akses istimewa, yang memperbolehkan pengguna untuk menembus sistem kontrol;
8. **Pengembangan dan Pemeliharaan Sistem**: untuk memastikan bahwa keamanan dibangun dalam sistem informasi. Persyaratan Keamanan sistem mencakup infrastruktur, aplikasi bisnis dan aplikasi yang dikembangkan pengguna. Disain dan implementasi proses bisnis yang mendukung aplikasi atau layanan sangat menentukan bagi keamanan. Persyaratan keamanan harus diidentifikasi dan disetujui sebelum pengembangan sistem informasi. Semua persyaratan keamanan sisitem informasi, termasuk kebutuhan pengaturan darurat, harus diidentifikasi pada fase persyaratan suatu proyek., dan diputuskan, disetujui serta didokumentasikan sebagai bagian dari keseluruhan kasus bisnis sebuah sistem informasi;
9. **Manajemen Kelangsungan Bisnis**: Untuk menghadapi kemungkinan penghentian kegiatan usaha dan melindungi proses usaha yang kritis dari akibat kegagalan atau bencana besar. Proses manajemen kelangsungan usaha harus diterapkan untuk mengurangi kerusakan akibat bencana atau kegagalan sistem keamanan (yang mungkin dihasilkan dari, sebagai contoh, bencana alam, kecelakaan, kegagalan alat dan keterlambatan) sampai ke tingkat yang dapat ditolerir melalui kombinasi pencegahan dan pemulihan kontrol. Konsekuensi dari bencana alam, kegagalan sistem keamanan dan kehilangan layanan harus dianalisa. Rencana darurat harus dikembangkan dan diterapkan untuk memastikan proses usaha dapat disimpan ulang dalam skala waktu yang dibutuhkan. Rencana semacam itu harus dijaga dan dipraktekkan untuk menjadi bagian integral keseluruhan proses manajemen. Manajemen kelangsungan bisnis harus mencakup kontrol untuk mengidentifikasi dan mengurangi resiko, membatasi konsekuensi kesalahan yang merusak, dan memastikan penyimpulan tahapan operasional yang penting; dan
10. **Kesesuaian**: Untuk menghindari pelanggaran terhadap hukum pidana maupun hukum perdata, perundangan, peraturan atau kewajiban kontrak serta ketentuan keamanan lainnya. Disain, operasional, penggunanan dan manajemenan sistem informasi adalah subyek dari perundangan, peraturan, dan perjanjian kebutuhan keamanan. Saran untuk kebutuhan legalitas yang

bersifat khusus harus dicari dari penasihat hukum organisasi, atau praktisi hukum yang berkualitas. Kebutuhan legalitas bervariasi dari negara ke negara dan bagi informasi yang dihasilkan dalam satu negara yang didistribusikan ke negara lain (contohnya arus data lintas batas).

-oo0oo-

~ 7 ~

FENOMENA HACTIVISM DAN BERBAGAI SELUK BELUK PERMASALAHANNYA

Capaian Pembelajaran (*Learning Outcomes*):

1. Menguraikan Fenomena dan Profil Hacker di Tanah Air
2. Memahami Hacktivism sebagai Sebuah Gerakan Komunitas
3. Menjelaskan Beragam Tipe Hacker

7.1 MENGURAIKAN FENOMENA DAN PROFIL HACKER DI TANAH AIR

Belakangan ini kehadiran dan aksi hacker mulai marak terjadi di dunia maya. Kontroversi mengenai definisi dan perilaku hacker telah pula menjadi sebuah wacana menarik bagi masyarakat moderen dalam era internet dewasa ini. Kehadiran buku-buku mengenai hacker dan berbagai kiat pekerjaannya telah pula mulai mewarnai ranah publik di Indonesia – terbukti dengan sangat lakunya publikasi tersebut dijual secara luas di pasar. Bahkan tidak tanggung-tanggung para praktisi teknologi informasi dan komunikasi dari negara tetangga seperti Malaysia, Brunei, dan Singapura tidak jarang berkunjung ke Indonesia untuk mendapatkan buku-buku tersebut. Hal ini disebabkan tidak semata-mata karena buku-buku tersebut dijual dengan harga relatif murah, namun juga karena telah begitu banyaknya koleksi referensi yang diperdagangkan secara bebas di toko-toko buku terkemuka dengan kualitas konten yang dianggap baik. Tidaklah heran jika dalam hitungan hari, jumlah hacker amatir maupun profesional di Indonesia bertambah secara cukup signifikan. Tidak saja dipandang dari segi kuantitas semata, namun ditinjau dari segi kualitas, mereka cukup baik menguasai berbagai ilmu "hacking" dan relatif aktif "berkarya" di dunia maya. Berikut adalah sekelumit seluk beluk kehidupan mereka.

7.2 MEMAHAMI HACKTIVISM SEBAGAI SEBUAH GERAKAN KOMUNITAS

Istilah "hacktivism" mengacu pada sebuah inisiatif dan kegiatan yang berfokus pada tindakan melakukan "hacking" karena atau untuk alasan tertentu. Alasan yang dimaksud dapat beraneka ragam.

Gambar 7.1 *Alasan Hacker Beraksi*

Dalam sejumlah referensi yang ada, paling tidak ada 4 (empat) alasan mengapa para hacker melakukan aksi "hacktivism"-nya. Pertama, adalah untuk mencari "sensasi diri". Perlu diperhatikan, generasi yang lahir setelah tahun 85-an telah terbiasa dengan keberadaan komputer di lingkungannya, berbeda dengan mereka yang

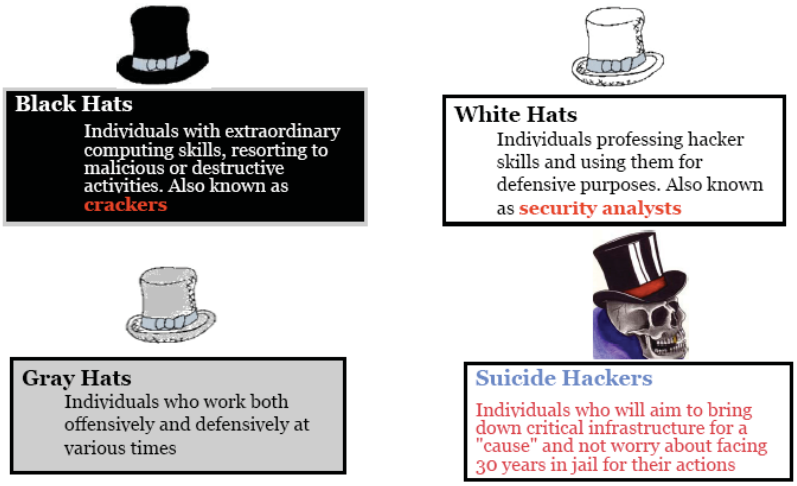
lahir di masa-masa sebelumnya. Jika generasi lama merasakan sebuah "sensasi diri" yang menyenangkan dengan cara bermain catur, mengisi teka teki silang, bermain kartu "truft", menyelesaikan misteri cerita detektif, dan lain sebagainya – maka generasi baru mendapatkan "sensasi diri" yang sama dengan cara "utak-atik" atau "ngoprek" komputer, bermain *game*, dan tentu saja melakukan kegiatan "hacking". Jika pada jaman dahulu pemain catur merasa tertantang jika harus "membunuh" raja dengan dua kuda, maka saat ini hacker merasa tertantang jika dapat masuk ke sebuah sistem tertentu yang dianggap sulit untuk dipenetrasi. Senang atau tidak senang, suka atau tidak suka, tindakan melakukan "hacking" tersebut telah berhasil menstimulus hormon-hormon dalam tubuh manusia masa kini yang memberikan sebuah sensasi tersendiri secara alami. Kedua, adalah untuk melakukan kejahatan. Bukan rahasia umum bahwa di negara-negara maju misalnya, telah banyak "berkeliaran" para hacker profesional yang tugasnya adalah melakukan kejahatan terorganisasi. Kejahatan yang dimaksud sifatnya beraneka ragam, mulai dari tindakan kriminal berlatar belakang ekonomi dan keuangan (seperti: perampokan bank, penipuan transaksi, pencucian uang, pencurian surat berharga, dan lain sebagainya), hingga yang bersifat kejahatan sosial (seperti: pencemaran nama baik, perusakan citra individu, pembunuhan karakter, pembohongan publik, dan lain sebagainya). Mereka ini biasanya dibayar mahal oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan tindakan kejahatan tersebut. Ketiga, adalah untuk menjalankan aktivitas terorisme. Di jaman moderen ini para teroris melihat bahwa internet dan dunia maya merupakan lahan dan media yang cukup efektif untuk melakukan aktivitas teror dimana-mana. Sasaran "terrorist hacker" biasanya adalah *critical infrastructure* alias obyek-obyek vitas sebuah negara seperti: perusahaan listrik, instalasi militer, pusat transportasi publik, sentra-sentra keamanan negara, jaringan keuangan perbankan, dan lain sebagainya. Karena kebanyakan organisasi-organisasi ini telah belibatkan teknologi informasi dan internet sebagai bagian tak terpisahkan dari aktivtas operasionalnya, maka penyerangan terhadap sistem jaringan dan komputer yang dimiliki akan mendatangkan dampak teror yang luar biasa. Dengan melakukan penyerangan terhadap obyek-obyek vital ini, maka pesan dibalik aksi terorisme yang dilakukan diharapkan dapat sampai ke pihak-pihak pemangku kepentingan yang menjadi sasaran. Keempat, adalah untuk alasan intelijen. Seperti diketahui bersama, setiap negara pasti memiliki jaringan intelijen di dalam dan di luar negeri untuk keperluan pertahanan dan keamanan nasional. Karena saat ini seluruh percakapan, interaksi, komunikasi, diskusi, kooperasi, transaksi, dan negosiasi dilakukan dengan memanfaatkan teknologi informasi dan intenet, maka kegiatan intelijen-pun mulai masuk ke ranah ini. Dalam konteks inilah maka dibutuhkan sejumlah hacker profesional yang dapat membantu melakukan kegiatan intelijen demi keutuhan negara ini. Lihatlah bagaimana Amerika dengan lembaga NSA

(National Security Agency) merekrut dan mendidik sedemikan banyak hacker dengan intelegensia dan keahlian tinggi untuk membantu mereka melaksanakan tugas kenegaraannya.

7.3 MENJELASKAN BERAGAM TIPE HACKER

Dengan berlatarbelakang penjelasan sebelumnya, dan dilihat dari sisi atau motivasi seorang hacker melakukan aktivitas yang menjadi bidang keahliannya, dunia internet kerap mengkategorikan hacker menjadi empat tipe, masing-masing adalah sebagai berikut:

1. *Black Hats* – merupakan kumpulan dari individu dengan keahlian tinggi di bidang keamanan komputer yang memiliki motivasi untuk melakukan tindakan-tindakan destruktif terhadap sistem komputer tertentu yang menjadi sasarannya demi mendapatkan sejumlah "imbalan" tertentu (dalam dunia kejahatan internet hacker ini dikenal sebagai *crackers*);
2. *White Hats* – merupakan kumpulan dari profesional yang memiliki keahlian di bidang internet yang bertugas untuk menjaga keamanan sebuah sistem komputer agar terhindar dari tindakan yang merugikan dari pihak-pihak yang menyerangnya (dalam dunia internet hacker ini dikenal sebagai *security analysts*);
3. *Gray Hats* – merupakan kumpulan dari orang-orang yang terkadang melakukan kegiatan yang bersifat *offensive* namun di lain waktu melakukan kegiatan yang bersifat *deffensive* terkait dengan keamanan sebuah jaringan komputer; dan
4. *Suicide Hackers* – merupakan kumpulan dari mereka yang dengan sengaja memiliki visi utama menyerang obyek-obyek vital kenegaraan untuk tujuan tertentu dan tidak khawatir terhadap ancaman perdata maupun pidana yang mengincarnya.



Gambar 7.2 *Empat Tipe Hacker*

Dengan berkaca pada berbagai seluk beluk hacker ini, dapat diambil kesimpulan bahwa sebenarnya istilah "hacker" di mata praktisi teknologi informasi dan internet tersebut sebenarnya bersifat netral. Namun kesalahpahaman definisi yang menjadi persepsi masyarakat menempatkan istilah "hacker" pada suatu pengertian yang bernuansa negatif, sehingga sering kali kegiatan "hacktivism" dianggap sebagai tindakan kriminal yang senantiasa melawan hukum. Melalui sosialisasi yang tepat dan strategi yang baik, keberadaan para individu hacker yang berkembang di masyarakat dapat dijadikan sebagai sebuah kesempatan untuk meningkatkan kinerja keamanan beraneka ragam sistem komputer yang dimiliki oleh masyarakat Indonesia agar tidak terhindar dari serangan dan penetrasi pihak luar yang dapat merugikan bangsa dan negara.

-oo0oo-

~ 8 ~

EMPAT DOMAIN KERAWANAN SISTEM

Capaian Pembelajaran (*Learning Outcomes*):

1. Mendeteksi Kerawanan dan Serangan pada Sistem Operasi
2. Mendeteksi Kerawanan dan Kualitas Aplikasi
3. Mendeteksi Kerawanan pada Modul Program
4. Mendeteksi Kerawanan Akibat Konfigurasi Standar

Bagaimana caranya mengetahui suatu sistem aman atau tidak? Cara yang paling mudah adalah menugaskan individu atau mereka yang memiliki keahlian di bidang keamanan sistem informasi untuk melakukan audit dan uji coba penetrasi (baca: *penetration test*) terhadap sistem terkait. Dari berbagai hasil uji coba yang ada, terlihat ada sejumlah cara yang biasa dipergunakan penyerang untuk masuk dan mengambil alih sistem. Keberhasilan penyerang ini adalah karena yang bersangkutan sanggup mengeksploitasi sejumlah kelemahan yang ada pada sistem. Berbagai studi memperlihatkan bahwa ada empat lubang kerawanan pada sistem yang paling sering dimanfaatkan oleh penyerang dalam melakukan serangan, masing-masing terkait dengan: (i) Sistem Operasi; (ii) Aplikasi; (iii) Modul Program; dan (iv) Konfigurasi. Berikut adalah pemaparan singkat terhadap aspek yang dimaksud.

Gambar 8.1 *Empat Jenis Lubang Kerawanan dan Potensi Serangan*

8.1 MENDETEKSI KERAWANAN DAN SERANGAN PADA SISTEM OPERASI

Seperti diketahui bersama, piranti lunak sistem operasi moderen sangatlah kompleks struktur maupun arsitekturnya. Begitu banyaknya kebutuhan dan beranekaragamnya fungsi serta kapabilitas yang diharapkan membuat sebuah sistem operasi harus dibangun dari beratus-ratus bahkan beribu-ribu sub-modul program untuk melayani berbagai jenis *services, ports,* maupun model akses yang berbeda-beda. Dengan demikian maka diharapkan pengguna dapat melakukan instalasi sistem operasi sesuai dengan spesifikasi keinginannya, melalui penyesuaian terhadap berbagai parameter yang tersedia. Namun di sini pulalah letak kerawanannya. Seorang pengguna atau *user* misalnya, sering sekali dalam melakukan instalasi sistem memilih mode “standard”, alias tanpa melakukan kustomisasi terhadap sejumlah parameter terkait, yang diantaranya menyangkut dengan masalah tingkat keamanan[1]. Tentu saja hal ini berakibat tidak terkonfigurasinya proteksi keamanan terhadap sejumlah *services* maupun

1 Untuk memudahkan proses instalasi, sering kali tanpa membaca arahan terlebih dahulu, sang pengguna langsung memilih tombol “YES” untuk mempercepat proses.

ports terkait, sehingga memudahkan penyerang untuk melakukan penyusupan dengan memanfaatkan lubang-lubang kerawanan tersebut.

Alasan berikutnya mengapa banyak terdapat kerawanan pada sistem operasi adalah karena begitu banyaknya modul-modul serta sub-sub modul pembentuknya, mengakibatkan sering kali sebuah perusahaan pembuat sistem informasi "tidak sempat" melakukan uji coba keamanan terhadap seluruh kombinasi dan/atau permutasi dari keseluruhan modul dan sub-modul pembentuk sistem operasi yang dimaksud[2].

Namun terdapat pula lubang kerawanan yang sifatnya "tak terhindarkan" karena merupakan bagian dari *trade-off* kinerja yang diharapkan dari sebuah sistem operasi – sehingga harus dilakukan sebuah desain atau rancangan piranti lunak yang sedemikian rupa. Lihatlah fenomena *buffer overflow* yang sebenarnya merupakan dampak dari mekanisme *memory swap* yang pada dasarnya merupakan solusi dari permasalahan sistem operasi klasik. Atau masalah penentuan tingkat keamanan yang dapat diubah-ubah parameternya oleh pengguna sesuai dengan profil resiko yang ingin diadopsi[3].

Hal lainnya yang juga mengemuka adalah begitu banyaknya aplikasi yang berfungsi sebagai "tambal sulam" (baca: *patches*) terhadap lubang-lubang sistem operasi yang belum mengalami tes uji coba secara holistik. Sifatnya yang *ad-hoc* dan lebih bersifat reaktif dan jangka pendek terkadang menimbulkan sebuah kerawanan baru yang tanpa disadari tertanam dalam sistem operasi terkait.

8.2 MENDETEKSI KERAWANAN DAN KUALITAS APLIKASI

Dalam kenyataan sehari-hari, ada tiga jenis piranti lunak aplikasi yang biasa dipergunakan. Jenis pertama adalah aplikasi siap pakai yang dibeli di pasar *software* dan langsung diterapkan, jenis kedua merupakan aplikasi yang dibangun sendiri oleh perusahaan yang bersangkutan, dan jenis ketiga yaitu aplikasi yang merupakan kombinasi dari keduanya[4]. Terlepas dari perbedaan ketiga jenis tersebut, keseluruhannya merupakan sebuah karya intelektual dari seorang atau sekelompok orang yang memiliki kompetensi terkait dengan pengembangan atau rekayasa sebuah piranti lunak (baca: *software engineering*). Dari sinilah cerita terciptanya kerawanan bermula.

---

2 Inilah salah satu alasan utama mengapa terkadang sistem operasi berbasis open source memiliki tingkat dan model keamanan yang jauh lebih baik dari proprietary adalah karena banyaknya pihak serta sumber daya yang setiap hari bekerjasama atau "keroyokan" melihat beragam kombinasi interaksi antar modul dan sub-modul guna mencari dan menambal segera lubang-lubang kerawanan yang ditemui.

3 Akibat adanya prinsip "keamanan" yang berbanding terbalik dengan "kenyamanan".

4 Biasanya merupakan aplikasi yang merupakan hasil kustomisasi dari modul-modul atau obyek-obyek program yang siap pakai dan dapat dirangkai satu dengan lainnya untuk membangun sebuah fungsi aplikasi yang lebih besar.

Pertama, pekerjaan pembuatan sebuah piranti lunak aplikasi biasanya memiliki target dan durasi penyelesaian tertentu, karena pengembangannya dilakukan melalui sebuah proses aktivitas berbasis proyek. Hal ini berarti bahwa setiap praktisi pengembang aplikasi, memiliki waktu yang sangat terbatas. Dalam kondisi ini sangat wajar jika terjadi sejumlah "kecerobohan" atau "kekurang-hati-hatian" karena dikejar atau diburu-buru target "waktu tayang" alias penyelesaian. Jadwal yang ketat ini secara teknis dan psikologis sangat berpengaruh terhadap terciptanya sebuah piranti aplikasi yang terbebas dari berbagai lubang-lubang kerawanan yang ada.

Kedua, mengingat begitu banyaknya modul dan objek program pembentuk sebuah aplikasi, dimana pada saatnya nanti *software* tersebut akan diinstalasi di berbagai jenis dan ragam lingkungan piranti keras serta jejaring komputer yang berbeda, akan teramat sulit untuk melakukan uji coba aplikasi yang mencakup seluruh kemungkinan konfigurasi sistem yang ada. Artinya adalah bahwa sang pengembang tidak memiliki data atau informasi yang lengkap dan utuh mengenai kinerja sistem secara keseluruhan dalam berbagai kemungkinan konfigurasi sistem.

Ketiga, masih begitu banyaknya *programmer* jaman sekarang yang memikirkan aspek keamanan sebagai sesuatu yang *additional* atau bersifat *afterthought consideration* – alias dipikirkan kemudian sebagai sebuah "pertimbangan tambahan" setelah sebuah piranti aplikasi dibangun. Padahal sifat dan karakteristik keamanan yang holistik haruslah dipikirkan sejalan dengan kode program dibuat dan dikembangkan. Belakangan ini mulai terlihat marak diperkenalkan teknologi yang terkait dengan *secured programming* untuk mengatasi berbagai jenis kerawanan akibat aktivitas pembuatan program konvensional yang tidak memperhatikan aspek penting ini.

Keempat, pengetahuan "pas-pasan" dari pengembang piranti lunak tidak jarang membuat kualitas keamanan dari sebuah aplikasi sedemikian buruk dan rendahnya. Hal ini disebabkan karena kebanyakan pemilik dan pengguna aplikasi hanya menilai efektivitas serta kinerja sebuah program dari segi kelengkapan fungsionalitas dan *user interface* saja, tanpa memikirkan mengenai kebutuhan berbagai jenis pengamanan yang diperlukan.

8.3 MENDETEKSI KERAWANAN PADA MODUL PROGRAM

Seperti diketahui bersama, metodologi dan konsep pengembangan aplikasi moderen adalah dengan menggunakan pendekatan objek. Artinya adalah kebanyakan pengembang piranti lunak tidak selalu membuat fungsi, prosedur, modul, atau sub-program dari nol atau "from scratch", tetapi terlebih dahulu mencari apakah telah ada objek program yang telah dibuat orang lain dan dapat dipergunakan

(baca: *reusable*). Kebiasaan ini mendatangkan sejumlah keuntungan, terutama terkait dengan faktor kecepatan proses dan penghematan biaya pengembangan aplikasi. Namun segi negatifnya adalah begitu banyaknya pengembang yang "pasrah" percaya saja menggunakan sebuah objek tanpa tahu kualitas keamanan dari "penggalan" program tersebut. Contohnya adalah penggunaan modul-modul semacam *libraries, scripts, drivers,* dan lain sebagainya. Pada kenyataannya, begitu banyak ditemukan modul atau objek program yang sangat rawan karena tidak dibangun dengan memperhatikan faktor keamanan – karena sebagian besar dari objek tersebut dibangun hanya dengan memperhatikan unsur fungsionalitasnya semata.

8.4 MENDETEKSI KERAWANAN AKIBAT KONFIGURASI STANDAR

Sebuah sistem informasi terdiri dari sejumlah piranti lunak dan piranti keras. Agar bekerja sesuai dengan kebutuhan, perlu diperhatikan sungguh-sungguh proses instalasi dan konfigurasi keseluruhan piranti yang dimaksud. Namun yang terjadi pada kenyataannya, tidak semua organisasi memiliki sumber daya manusia yang berpengetahuan dan berkompetensi memadai untuk melakukan hal tersebut. Akibatnya adalah tidak jarang dari mereka hanya mencari mudahnya saja, alias melakukan instalasi dan konfigurasi sistem secara standar, tanpa memperhatikan kebutuhan khusus dari organisasi yang bersangkutan. Misalnya adalah dalam hal melakukan konfigurasi *firewalls* dimana *port-port* yang seharusnya ditutup karena alasan keamanan menjadi terbuka karena sesuai dengan *set up* standar pabrik. Atau pada saat menginstalasi *software anti virus* dimana tingkat keamanan yang "dipasang" adalah *low* sehingga tidak berfungsi maksimal dalam melindungi sistem. Hal-hal semacam inilah yang menyebabkan "terciptanya" lubang-lubang kerawanan tanpa disadari.

Berdasarkan keempat jenis aspek kerawanan tersebut, ada baiknya sebuah organisasi menjalankan strategi khusus untuk menghindari diri dari kemungkinan dieskploitasi oleh pihak-pihak tidak bertanggung jawab, misalnya adalah dengan cara:

- Sebelum membeli atau mengadakan sebuah modul objek atau aplikasi, dilakukan penelitian terlebih dahulu mengenai kinerja program yang dimaksud, terutama dilihat dari segi atau aspek keamanannya;
- Pada saat mengembangkan sistem, dilibatkan *programmer* atau pihak-pihak yang paham benar dan memiliki kompetensi dalam ilmu *secured programming*, sehingga produk modul maupun aplikasi yang dibangun telah mempertimbangkan aspek keamanan yang dimaksud;

- Jika tidak memiliki sumber daya yang memiliki kometensi dan keahlian dalam mengkonfigurasi sebuah sistem, bekerjasamalah dengan konsultan atau ahli di bidang piranti tersebut agar dapat melakukan instalasi parameter keamanan dalam sistem yang dimaksud; dan lain sebagainya.

-oo0oo-

~ 9 ~

RAGAM JENIS SOFTWARE JAHAT

Capaian Pembelajaran (*Learning Outcome*):

1. Menjelaskan Jenis-Jenis Malicious Software
2. Web Defacement
3. Denial of Services (DoS)
4. Botnet
5. Phishing
6. SQL Injection
7. Cross-Site Scripting

Dewasa ini terdapat banyak sekali tipe dan jenis serangan yang terjadi di dunia maya. Sesuai dengan sifat dan karakteristiknya, semakin lama model serangan yang ada semakin kompleks dan sulit dideteksi maupun dicegah. Berikut adalah berbagai jenis model serangan yang kerap terjadi menerpa dunia maya, terutama yang dikenal luas di tanah air.

9.1 MENJELASKAN JENIS-JENIS MALICIOUS SOFTWARE

Malware merupakan program yang dirancang untuk disusupkan ke dalam sebuah sistem (baca: target penyerangan) dengan tujuan untuk melakukan beraneka ragam aktivitas yang bersifat merugikan pemilikinya. Merugikan dalam arti kata dampak negatif yang ditimbulkan dapat berkisar mulai dari sekedar memperlambat kinerja sistem hingga merusak bahkan menghancurkan data penting yang tersimpan dalam sistem dimaksud. Ada tiga jenis malware klasik yang paling banyak ditemui, yaitu: Virus, Worm, dan Trojan Horse.

Virus

Sejak kemunculannya pertama kali pada pertengahan tahun 1980-an, virus komputer telah mengundang berbagai kontroversi akibat aksinya yang beraneka ragam. Seiring dengan perkembangan teknologi komputer, virus menemukan berbagai cara-cara baru untuk menyebarkan dirinya melalui berbagai modus operandi. Pada dasarnya, virus merupakan program komputer yang bersifat "malicious" (memiliki tujuan merugikan maupun bersifat mengganggu pengguna sistem) yang dapat menginfeksi satu atau lebih sistem komputer melalui berbagai cara penularan yang dipicu oleh otorasisasi atau keterlibatan "user" sebagai pengguna komputer. Fenomena yang mulai ditemukan pada awal tahun 1980-an ini memiliki beribu-ribu macam atau jenis sejalan dengan perkembangan teknologi komputer dewasa ini – terutama setelah dikembangkannya teknologi jaringan dan internet. Jenis kerusakan yang ditimbulkan virus pun menjadi bermacam-macam. Mulai dari yang sekedar mengganggu seperti menampilkan gambar-gambar yang tidak sepantasnya, hingga sampai yang bersifat mendatangkan kerugian ekonomis seperti memformat hard disk atau bahkan merusak file-file sistem operasi sehingga mengganggu komputer yang bersangkutan. Ditinjau dari cara kerjanya, virus dapat dikelompokkan menjadi:

a. *Overwriting Virus* – merupakan penggalan program yang dibuat sedemikian rupa untuk menggantikan program utama (baca: host) dari sebuah program besar sehingga menjalankan perintah yang tidak semestinya;
b. *Prepending Virus* – merupakan tambahan program yang disisipkan pada bagian awal dari program utama atau "host" sehingga pada saat dieksekusi,

program virus akan dijalankan terlebih (bereplikasi) dahulu sebelum program yang sebenarnya;

c. *Appending Virus* – merupakan program tambahan yang disisipkan pada bagian akhir dari program host sehingga akan dijalankan setelah program sebenarnya tereksekusi;
d. *File Infector Virus* – merupakan penggalan program yang mampu memiliki kemampuan untuk melekatkan diri (baca: attached) pada sebuah file lain, yang biasanya merupakan file "executable", sehingga sistem yang menjalankan file tersebut akan langsung terinfeksi;
e. *Boot Sector Virus* – merupakan program yang bekerja memodifikasi program yang berada di dalam boot sector pada cakram penyimpan (baca: disc) atau disket yang telah diformat. Pada umumnya, sebuah boot sector virus akan terlebih dahulu mengeksekusi dirinya sendiri sebelum proses "boot-up" pada komputer terjadi, sehingga seluruh "floppy disk" yang digunakan pada komputer tersebut akan terjangkiti pula (perhatikan bahwa dewasa ini, modus operandi sejenis terjadi dengan memanfaatkan media penyimpan USB);
f. *Multipartite Virus* – merupakan kombinasi dari Infector Virus dan Boot Sector Virus dalam arti kata ketika sebuah file yang terinfeksi oleh virus jenis ini dieksekusi, maka virus akan menjangkiti boot sector dari hard disk atau partition sector dari komputer tersebut, dan sebaliknya; dan
g. *Macro Virus* - menjangkiti program "macro" dari sebuah file data atau dokumen (yang biasanya digunakan untuk "global setting" seperti pada template Microsoft Word) sehingga dokumen berikutnya yang diedit oleh program aplikasi tersebut akan terinfeksi pula oleh penggalan program macro yang telah terinfeksi sebelumnya.

Perlu diperhatikan bahwa virus hanya akan aktif menjangkiti atau menginfeksi sistem komputer lain apabila ada campur tangan manusia atau "user" sebagai pengguna. Campur tangan yang dimaksud misalnya dilakukan melalui: penekanan tombol pada keyboard, penekanan tombol pada mouse, "pemasukan" USB pada komputer, pengiriman file via email, dan lain sebagainya.

Worms

Istilah "worms" yang tepatnya diperkenalkan kurang lebih setahun setelah "virus" merupakan program malicious yang dirancang terutama untuk menginfeksi komputer-komputer yang berada dalam sebuah sistem jaringan. Walaupun sama-sama sebagai sebuah penggalan program, perbedaan prinsip yang membedakan worms dengan pendahulunya virus yaitu yang bersangkutan tidak memerlukan campur tangan manusia atau pengguna dalam melakukan penularan atau penyebarannya. Worms merupakan program yang dibangun dengan algoritma

tertentu sehingga yang bersangkutan mampu untuk mereplikasikan dirinya sendiri pada sebuah jaringan komputer tanpa melalui intervensi atau bantuan maupun keterlibatan pengguna. Pada mulanya worms diciptakan dengan tujuan tunggal yaitu untuk mematikan sebuah sistem atau jaringan komputer. Namun belakangan ini telah tercipta worms yang mampu menimbulkan kerusakan luar biasa pada sebuah sistem maupun jaringan komputer, seperti merusak file-file penting dalam sistem operasi, menghapus data pada hard disk, memacetkan aktivitas komputer (baca: hang), dan hal-hal destruktif lainnya.

Karena karakteristiknya yang tidak melibatkan manusia, maka jika sudah menyebar sangat sulit untuk mengontrol atau mengendalikannya. Usaha penanganan yang salah justru akan membuat pergerakan worms menjadi semakin liar tak terkendali dan "mewabah". Untuk itulah dipergunakan penanganan khusus dalam menghadapinya.

Trojan Horse

Istilah "Trojan Horse" atau Kuda Troya diambil dari sebuah taktik perang yang digunakan untuk merebut kota Troy yang dikelilingi benteng nan kuat. Pihak penyerang membuat sebuah patung kuda raksasa yang di dalamnya memuat beberapa prajurit yang nantinya ketika sudah berada di dalam wilayah benteng akan keluar untuk melakukan penyerangan dari dalam. Adapun bentuk kuda dipilih sebagaimana layaknya sebuah hasil karya seni bagi sang Raja agar dapat dengan leluasa masuk ke dalam benteng yang dimaksud.

Ide ini mengilhami sejumlah hacker dan cracker dalam membuat virus atau worms yang cara kerjanya mirip dengan fenomena taktik perang ini, mengingat pada waktu itu bermuncukan Anti Virus Software yang dapat mendeteksi virus maupun worms dengan mudah untuk kemudian dilenyapkan. Dengan menggunakan prinsip ini, maka penggalan program malicious yang ada dimasukkan ke dalam sistem melalui sebuah program atau aktivitas yang legal – seperti: melalui proses instalasi perangkat lunak aplikasi, melalui proses "upgrading" versi software yang baru, melalui proses "download" program-program freeware, melalui file-file multimedia (seperti gambar, lagu, dan video), dan lain sebagainya.

Berdasarkan teknik dan metode yang digunakan, terdapat beberapa jenis Trojan Horse, antara lain:

- *Remote Access Trojan* - kerugian yang ditimbulkan adalah komputerkorban serangan dapat diakses secara remote;
- *Password Sending Trojan* - kerugian yang ditimbulkan adalah password yang diketik oleh komputer korban akan dikirimkan melalui email tanpa sepengetahuan dari korban serangan;

- *Keylogger* - kerugian yang ditimbulkan adalah ketikan atau input melalui keyboard akan dicatat dan dikirimkan via email kepada hacker yang memasang keylogger;
- *Destructive Trojan* – kerugian yang ditimbulkan adalah file-file yang terhapus atau hard disk yang terformat;
- *FTP Trojan* – kerugian yang terjadi adalah dibukanya port 21 dalam sistem komputer tempat dilakukannya download dan upload file;
- *Software Detection Killer* – kerugiannya dapat program-program keamanan seperti zone alarm, anti-virus, dan aplikasi keamanan lainnya; dan
- *Proxy Trojan* – kerugian yang ditimbulkan adalah di-"settingnya" komputer korban menjadi "proxy server" agar digunakan untuk melakukan "anonymous telnet", sehingga dimungkinkan dilakukan aktivitas belanja online dengan kartu kredit curian dimana yang terlacak nantinya adalah komputer korban, bukan komputer pelaku kejahatan.

9.2 WEB DEFACEMENT

Serangan dengan tujuan utama merubah tampilah sebuah website – baik halaman utama maupun halaman lain terkait dengannya – diistilahkan sebagai "Web Defacement". Hal ini biasa dilakukan oleh para "attacker" atau penyerang karena merasa tidak puas atau tidak suka kepada individu, kelompok, atau entitas tertentu sehingga website yang terkait dengannya menjadi sasaran utama[1]. Pada dasarnya deface dapat dibagi menjadi dua jenis berdasarkan dampak pada halaman situs yang terkena serangan terkait.

Jenis pertama adalah suatu serangan dimana penyerang merubah (baca: men-deface) satu halaman penuh tampilan depan alias file index atau file lainnya yang akan diubah secara utuh.Artinya untuk melakukan hal tersebut biasanya seorang 'defacer' harus berhubungan secara 'langsung' dengan mesin komputer terkait. Hal ini hanya dapat dilakukan apabila yang bersangkutan sanggup mendapatkan hak akses penuh (baca: priviledge) terhadap mesin, baik itu "root account" atau sebagainya yang memungkinkan defacer dapat secara interaktif mengendalikan seluruh direktori terkait. Hal ini umumnya dimungkinkan terjadi dengan memanfaatkan kelemahan pada sejumlah "services" yang berjalan di sistem komputer.

Jenis kedua adalah suatu serangan dimana penyerang hanya merubah sebagian atau hanya menambahi halaman yang di-deface.Artinyayang bersangkutan men-deface suatu situs tidak secara penuh, bisa hanya dengan menampilkan beberapa kata, gambar atau penambahan "script" yang mengganggu. Dampaknya

1 Seperti halnya mencoret-coret tembok atau grafiti dalam dunia nyata.

biasanya adalah menghasilkan tampilan yang kacau atau mengganggu. Hal ini dapat dilakukan melaluipenemuan celah kerawanan padamodel scripting yang digunakan, misalnya dengan *XSS injection*, *SQL* atau *database injection,*atau memanfaatkan sistem aplikasi manajemen website yang lemah (baca: CMS = Content Management System).

9.3 DENIAL OF SERVICES (DOS)

Serangan yang dikenal dengan istilah DoS dan DDoS (Distributed Denial of Services) ini pada dasarnya merupakan suatu aktivitas dengan tujuan utama menghentikan atau meniadakan layanan (baca: services) sistem atau jaringan komputer - sehingga sang pengguna tidak dapat menikmati fungsionalitas dari layanan tersebut – dengan cara mengganggu ketersediaan komponen sumber daya yang terkait dengannya. Contohnya adalah dengan cara memutus koneksi antar dua sistem, membanjiri kanal akses dengan jutaan paket, menghabiskan memori dengan cara melakukan aktivitas yang tidak perlu, dan lain sebagainya.

Dengan kata lain, DOS dan/atau DDoS merupakan serangan untuk melumpuhkan sebuah layanan dengan cara menghabiskan sumber daya yang diperlukan sistem komputer untuk melakukan kegiatan normalnya. Adapun sumber daya yang biasa diserang misalnya: kanal komunikasi (baca: bandwidth), kernel tables, swap space, RAM, cache memories, dan lain sebagainya. Berikut adalah sejumlah contoh tipe serangan DoS/DDoS:

1. *SYN-Flooding*: merupakan serangan yang memanfaatkan lubang kerawanan pada saat koneksi TCP/IP terbentuk.
2. *Pentium 'FOOF' Bug*: merupakan serangan terhadap prosessor yang menyebabkan sistem senantiasa melakukan "re-booting". Hal ini tidak bergantung terhadap jenis sistem operasi yang digunakan tetapi lebih spesifik lagi terhadap prosessor yang digunakan.
3. *Ping Flooding*: merupakan aktivitas "brute force" sederhana, dilakukan oleh penyerang dengan bandwidth yang lebih baik dari korban, sehingga mesin korban tidak dapat mengirimkan paket data ke dalam jaringan (network). Hal ini terjadi karena mesin korban dibanjiri (baca: flood) oleh peket-paket ICMP.

Yang membedakan antara DDoS dengan DoS adalah pada DDoS serangan dilakukan serempak oleh beberapa komputer sekaligus, sehingga hal ini sangat ampuh dalam membuat sistem atau jaringan komputer tertentu lumpuh dalam waktu cepat.

9.4 BOTNET

Salah satu jenis serangan yang paling banyak dibicarakan belakangan ini dan menjadi trend di negara-negara maju adalah "botnet" yang merupakan singkatan dari "Robot Network". Pada dasarnya aktivitas botnet dipicu dari disusupkannya program-program kecil – bersifat seperti virus, worms, maupun trojan horse – ke dalam berbagai sistem komputer server yang ada dalam jejaring internet tanpa sepengatahuan pemiliknya. Program malicious yang disusupkan dan ditanamkan pada server ini pada mulanya bersifat pasif, alias tidak melakukan kegiatan apa-apa yang mengganggu. Karena karakteristik inilah makanya sering dinamakan sebagai "zombies". Yang menarik adalah bahwa pada saatnya nanti, si penyerang yang diistilahkan sebagai "Master Refer" secara "remote" akan mengendalikan keseluruhan zombies yang berada di bawah "kekuasannya" untuk melakukan penyerangan secara serentak dan simultan ke suatu target tertentu. Pada saat inilah maka seluruh zombies yang jumlahnya dapat mencapai puluhan ribu bahkan jutaan tersebut langsung bersifat aktif melakukan kegiatan sesuai yang diinginkan oleh "master"-nya.

Dengan melakukan aktivasi terhadap zombies ini maka serangan botnet dapat dilakukan secara serempak dengan beragam skenario yang memungkinkan, seperti: melakukan DDoS secara masif, mematikan sistem komputer secara simultan, menularkan virus dan worms secara serentak, menginfeksi puluhan ribu server dengan trojan horse dalam waktu singkat, dan lain sebagainya.

Tingkat kesulitan untuk menangani botnet dikenal sangat tinggi dan kompleks, karena karakteristiknya yang mendunia membuat koordinasi multi-lateral harus dilakukan secara intensif dan sesering mungkin. Disamping itu tidak mudah untuk mendeteksi adanya beraneka ragam jenis zombies yang dalam keadaan non aktif atau "tidur" tersebut; apalagi mencoba untuk mengalokasikan dimana posisi sang Master Refer sebagai dalang pengendali serangan botnet terkait.

9.5 PHISHING

Phishing merupakan sebuah proses "pra-serangan" atau kerap dikatakan sebagai "soft attack" dimana sang penyerang berusaha mendapatkan informasi rahasia dari target dengan cara menyamar menjadi pihak yang dapat dipercaya – atau seolah-olah merupakan pihak yang sesungguhnya. Contohnya adalah sebuah email yang berisi suatu informasi yang mengatakan bahwa sang pengirim adalah dari Divisi Teknologi Informasi yang sedang melakukan "upgrading" sistem; dimana untuk memperlancar tugasnya, sang penerima email diminta untuk segera mengirimkan kata kunci "password" dari "user name" yang dimilikinya. Atau situs sebuah bank

palsu yang memiliki tampilan sama persis dengan situs aslinya namun memiliki alamat URL yang mirip-mirip, sehingga diharapkan sang nasabah akan khilaf dan secara tidak sadar memasukkan kata kunci rahasianya untuk mengakses rekening yang dimaksud.

Serangan "phishing" ini kerap dikategorikan sebagai sebuah usaha "social engineering", yaitu memanfaatkan pendekatan sosial dalam usahanya untuk mendapatkan informasi rahasia sebagai alat untuk melakukan penyerangan di kemudian hari. Modus operandi yang paling banyak ditemui saat ini adalah usaha phishing melalui SMS pada telepon genggam, dimana sudah banyak korban yang harus kehilangan uangnya karena diminta untuk melakukan transfer ke rekening tertentu dengan berbagai alasan yang seolah-olah masuk akal sehingga berhasil menjebak sang korban.

9.6 SQL INJECTION

Pada dasarnya SQL Injection merupakan cara mengeksploitasi celah keamanan yang muncul pada level atau "layer" database dan aplikasinya. Celah keamanan tersebut ditunjukkan pada saat penyerang memasukkan nilai "string" dan karakter-karakter contoh lainnya yang ada dalam instruksi SQL; dimana perintah tersebut hanya diketahui oleh sejumlah kecil individu (baca: hacker maupun cracker) yang berusaha untuk mengeksploitasinya. Karena tipe data yang dimasukkan tidak sama dengan yang seharusnya (sesuai dengan kehendak program), maka terjadi sebuah aktivitas "liar" yang tidak terduga sebelumnya[2] - dimana biasanya dapat mengakibatkan mereka yang tidak berhak masuk ke dalam sistem yang telah terproteksi menjadi memiliki hak akses dengan mudahnya. Dikatakan sebagai sebuah "injeksi" karena aktivitas penyerangan dilakukan dengan cara "memasukkan" string (kumpulan karakter) khusus untuk melewati filter logika hak akses pada website atau sistem komputer yang dimaksud.

Contoh-contoh celah kerawanan yang kerap menjadi korban SQL Injection adalah:

- Karakter-karakter kendali, kontrol, atau filter tidak didefinisikan dengan baik dan benar (baca: Incorrectly Filtered Escape Characters);
- Tipe pemilihan dan penanganan variabel maupun parameter program yang keliru (baca: Incorrect Type Handling);
- Celah keamanan berada dalam server basis datanya (baca: Vulnerabilities Inside the Database Server);
- Dilakukan mekanisme penyamaran SQL Injection (baca: Blind SQL Injection); dan lain sebagainya.

2 Kerawanan sistem ini merupakan bagian tak terpisahkan dari desain program yang dimaksud (baca: embedded vulnerable) sehingga sangat sulit mengatasinya.

9.7 CROSS-SITE SCRIPTING

Cross Site Scripting (CSS) adalah suatu serangan dengan menggunakan mekanisme "injection" pada aplikasi web dengan memanfaatkan metode HTTP GET atau HTTP POST. Cross Site Scripting biasa digunakan oleh pihak-pihak yang berniat tidak baik dalam upaya mengacaukan konten website dengan memasukkan naskah program (biasanya java script) sebagai bagian dari teks masukan melalui formulir yang tersedia.

Apabila tidak diwaspadai, script ini dapat begitu saja dimasukkan sebagai bagian dari teks yang dikirim ke web setiap pengunjung, misalnya melalui teks masukan buku tamu atau forum diskusi yang tersedia bagi semua pengunjung website. Script yang menyisip di teks yang tampil ini dapat memberi efek dramatis pada tampilan website mulai dari menyisipkan gambar tidak senonoh sampai mengarahkan tampilan ke website lain.

CSS memanfaatkan lubang kelemahan keamanan yang terjadi pada penggunaan teknologi "dynamic page". Serangan jenis ini dapat diakibatkan oleh kelemahan yang terjadi akibat ketidakmampuan server dalam memvalidasi input yang diberikan oleh pengguna – misalnya algoritma yang digunakan untuk pembuatan halaman yang diinginkan tidak mampu melakukan penyaringan terhadap masukkan tersebut. Hal ini memungkinkan halaman yang dihasilkan menyertakan perintah yang sebenarnya tidak diperbolehkan.

Serangan CSS ini populer dilakukan oleh berbagai kalangan. Namun sayangnya, banyak penyedia layanan yang tidak mengakui kelemahan tersebut dan mau melakukan perubahan pada sistem yang mereka gunakan. Citra penyedia layanan merupakan harga yang dipertaruhkan ketika mereka mengakui kelemahan tersebut. Sayangnya dengan tindakan ini konsumen atau pengguna menjadi pihak yang dirugikan.

Dari sisi kerapuhan dan keamanan, CSS dapat bekerja bak penipu dengan kedok yang mampu mengelabui orang yang tidak waspada. Elemen penting dari keberhasilan CSS adalah "social engineering" yang efektif dari sisi penipu. CSS memampukan seseorang yang tidak bertanggungjawab melakukan penyalahgunaan informasi penting.

Sebelum sampai pada proses penyalahgunaan tersebut, penyerang biasanya mengambil langkah-langkah awal terlebih dahulu dengan mengikuti pola tertentu. Langkah pertama, penyerang melakukakan pengamatan untuk mencari web-web yang memiliki kelemahan yang dapat dieksploitasi dengan CSS. Langkah kedua, sang penyerang mencari tahu apakah web tersebut menerbitkan informasi yang dapat digunakan untuk melakukan pencurian infomasi lebih lanjut. Informasi

tersebut biasanya berupa “cookie”. Langkah kedua ini tidak selalu dijalankan. Langkah ketiga, sang penyerang membujuk korban untuk mengikuti sebuah link yang mengandung kode, ditujukan untuk mendapatkan informasi yang telah disebutkan sebelumnya. Kemampuan melakukan “social engineering” dari sang penyerang diuji disini. Setelah mendapatkan informasi tersebut, sang penyerang melakukan langkah terakhir, pencurian maupun pengubahan informasi vital.

Pada kenyataannya, masih banyak sekali ditemukan jenis-jenis serangan seperti yang dikemukakan di atas, seperti: *Land Attack*, *Man-in-the-Middle Attack*, *Packet Spoofing*, *Password Cracking*, *Sessions Hijacking*, dan lain sebagainya. Pada intinya keseluruhan jenis serangan itu bervariasi berdasarkan tipe-tipe kerawanan atau “vulnerabilities” yang terdapat pada sistem terkait yang kurang dijaga keamanannya.

-oo0oo-

~ 10 ~

SELUK BELUK SERANGAN MELALUI TEKNIK SOCIAL ENGINEERING

Capaian Pembelajaran (*Learning Outcomes*):

1. Mendeteksi Kelemahan Manusia
2. Menjelaskan Tipe Social Engineering
3. Mendeteksi Social Engineering Menggunakan Teknik Komunikasi
4. Mendeteksi Social Engineering Menggunakan Medium Komputer
5. Mendteksi Jenis Social Engineering Lainnya
6. Mengidentifikasi Target Korban Social Engineering
7. Menetapkan Solusi Menghindari Resiko

Ada prinsip dalam dunia keamanan jaringan yang berbunyi “kekuatan sebuah rantai tergantung dari atau terletak pada sambungan yang terlemah” atau dalam bahasa asingnya “the strength of a chain depends on the weakest link”. Apa atau siapakah “the weakest link” atau “komponen terlemah” dalam sebuah sistem jaringan komputer? Ternyata jawabannya adalah: manusia. Walaupun sebuah sistem telah dilindungi dengan piranti keras dan piranti lunak canggih penangkal serangan seperti firewalls, anti virus, IDS/IPS, dan lain sebagainya – tetapi jika manusia yang mengoperasikannya lalai, maka keseluruhan peralatan itu tidaklah ada artinya. Para kriminal dunia maya paham betul akan hal ini sehingga kemudian mereka mulai menggunakan suatu kiat tertentu yang dinamakan sebagai “social engineering” untuk mendapatkan informasi penting dan krusial yang disimpan secara rahasia oleh manusia.

10.1 MENDETEKSI KELEMAHAN MANUSIA

Menurut definisi, “social engineering” adalah suatu teknik ‘pencurian’ atau pengambilan data atau informasi penting/krusial/rahasia dari seseorang dengan cara menggunakan pendekatan manusiawi melalui mekanisme interaksi sosial. Atau dengan kata lain social engineering adalah suatu teknik memperoleh data/ informasi rahasia dengan cara mengeksploitasi kelemahan manusia. Contohnya kelemahan manusia yang dimaksud misalnya:

- Rasa Takut – jika seorang pegawai atau karyawan dimintai data atau informasi dari atasannya, polisi, atau penegak hukum yang lain, biasanya yang bersangkutan akan langsung memberikan tanpa merasa sungkan;
- Rasa Percaya – jika seorang individu dimintai data atau informasi dari teman baik, rekan sejawat, sanak saudara, atau sekretaris, biasanya yang bersangkutan akan langsung memberikannya tanpa harus merasa curiga; dan
- Rasa Ingin Menolong – jika seseorang dimintai data atau informasi dari orang yang sedang tertimpa musibah, dalam kesedihan yang mendalam, menjadi korban bencana, atau berada dalam duka, biasanya yang bersangkutan akan langsung memberikan data atau informasi yang diinginkan tanpa bertanya lebih dahulu.

10.2 MENJELASKAN TIPE SOCIAL ENGINEERING

Pada dasarnya teknik social engineering dapat dibagi menjadi dua jenis, yaitu: berbasis interaksi sosial dan berbasis interaksi komputer. Berikut adalah sejumlah teknik social engineering yang biasa dipergunakan oleh kriminal, musuh, penjahat, penipu, atau mereka yang memiliki intensi tidak baik.

10.3 MENDETEKSI SOCIAL ENGINEERING MENGGUNAKAN TEKNIK KOMUNIKASI

Dalam skenario ini yang menjadi sasaran penipuan adalah individu yang bekerja di divisi teknologi informasi perusahaan. Modus operandinya sama, yaitu melalui medium telepon.

Skenario 1 (Kedok sebagai User Penting)

Seorang penipu menelpon help desk bagian divisi teknologi informasi dan mengatakan hal sebagai berikut *"Halo, di sini pak Abraham, Direktur Keuangan. Saya mau log in tapi lupa password saya. Boleh tolong beritahu sekarang agar saya dapat segera bekerja?"*. Karena takut – dan merasa sedikit tersanjung karena untuk pertama kalinya dapat berbicara dan mendengar suara Direktur Keuangan perusahaannya – yang bersangkutan langsung memberikan password yang dimaksud tanpa rasa curiga sedikitpun. Si penipu bisa tahu nama Direktur Keuangannya adalah Abraham karena melihat dari situs perusahaan.

Skenario 2 (Kedok sebagai User yang Sah)

Dengan mengaku sebagai rekan kerja dari departemen yang berbeda, seorang wanita menelepon staf junior teknologi informasi sambil berkata *"Halo, ini Iwan ya? Wan, ini Septi dari Divisi Marketing, dulu kita satu grup waktu outing kantor di Cisarua. Bisa tolong bantu reset password-ku tidak? Dirubah saja menjadi tanggal lahirku. Aku takut ada orang yang tahu passwordku, sementara saat ini aku di luar kantor dan tidak bisa merubahnya. Bisa bantu ya?"*. Sang junior yang tahu persis setahun yang lalu merasa berjumpa Septi dalam acara kantor langsung melakukan yang diminta rekan sekerjanya tersebut tanpa melakukan cek dan ricek. Sementara kriminal yang mengaku sebagai Septi mengetahui nama-nama terkait dari majalah dinding "Aktivitas" yang dipajang di lobby perusahaan – dan nomor telepon Iwan diketahuinya dari Satpam dan/atau receptionist.

Skenario 3 (Kedok sebagai Mitra Vendor)

Dalam hal ini penjahat yang mengaku sebagai mitra vendor menelepon bagian operasional teknologi informasi dengan mengajak berbicara hal-hal yang bersifat teknis sebagai berikut: *"Pak Aryo, saya Ronald dari PT Teknik Alih Daya Abadi, yang membantu outsource file CRM perusahaan Bapak. Hari ini kami ingin Bapak mencoba modul baru kami secara cuma-cuma. Boleh saya tahu username dan password Bapak agar dapat saya bantu instalasi dari tempat saya? Nanti kalau sudah terinstal, Bapak dapat mencoba fitur-fitur dan fasilitas canggih dari program CRM versi terbaru."* Merasa mendapatkan kesempatan, kepercayaan,

dan penghargaan, yang bersangkutan langsung memberikan username dan passwordnya kepada si penjahat tanpa merasa curiga sedikitpun. Sekali lagi sang penjahat bisa tahu nama-nama yang bersangkutan melalui berita-berita di koran dan majalah mengenai produk/jasa PT Teknik Alih Daya Abadi dan nama-nama klien utamanya.

Skenario 4 (Kedok sebagai Konsultan Audit)

Kali ini seorang penipu menelpon Manajer Teknologi Informasi dengan menggunakan pendekatan sebagai berikut: *"Selamat pagi Pak Basuki, nama saya Roni Setiadi, auditor teknologi informasi eksternal yang ditunjuk perusahaan untuk melakukan validasi prosedur. Sebagai seorang Manajer Teknologi Informasi, boleh saya tahu bagaimana cara Bapak melindungi website perusahaan agar tidak terkena serangan defacement dari hacker?"*. Merasa tertantang kompetensinya, dengan panjang lebar yang bersangkutan cerita mengenai struktur keamanan website yang diimplementasikan perusahaannya. Tentu saja sang kriminal tertawa dan sangat senang sekali mendengarkan bocoran kelemahan ini, sehingga mempermudah yang bersangkutan dalam melakukan serangan.

Skenario 5 (Kedok sebagai Penegak Hukum)

Contoh terakhir ini adalah peristiwa klasik yang sering terjadi dan dipergunakan sebagai pendekatan penjahat kepada calon korbannya: *"Selamat sore Pak, kami dari Kepolisian yang bekerjasama dengan Tim Insiden Keamanan Internet Nasional. Hasil monitoring kami memperlihatkan sedang ada serangan menuju server anda dari luar negeri. Kami bermaksud untuk melindunginya. Bisa tolong diberikan perincian kepada kami mengenai topologi dan spesifikasi jaringan anda secara detail?"*. Tentu saja yang bersangkutan biasanya langsung memberikan informasi penting tersebut karena merasa takut untuk menanyakan keabsahan atau keaslian identitas penelpon.

10.4 MENDETEKSI SOCIAL ENGINEERING MENGGUNAKAN MEDIUM KOMPUTER

Sementara itu untuk jenis kedua, yaitu menggunakan komputer atau piranti elektronik/digital lain sebagai alat bantu, cukup banyak modus operandi yang sering dipergunakan seperti:

Skenario 1 (Teknik Phishing – melalui Email)

Strategi ini adalah yang paling banyak dilakukan di negara berkembang seperti Indonesia. Biasanya si penjahat menyamar sebagai pegawai atau karyawan sah

yang merepresentasikan bank. Email yang dimaksud berbunyi misalnya sebagai berikut:

"Pelanggan Yth. Sehubungan sedang dilakukannya upgrade sistem teknologi informasi di bank ini, maka agar anda tetap mendapatkan pelayanan perbankan yang prima, mohon disampaikan kepada kami nomor rekening, username, dan password anda untuk kami perbaharui. Agar aman, lakukanlah dengan cara me-reply electronic mail ini. Terima kasih atas perhatian dan koordinasi anda sebagai pelanggan setia kami.

Wassalam,

Manajer Teknologi Informasi"

Bagaimana caranya si penjahat tahu alamat email yang bersangkutan? Banyak cara yang dapat diambil, seperti: melakukan searching di internet, mendapatkan keterangan dari kartu nama, melihatnya dari anggota mailing list, dan lain sebagainya.

Skenario 2 (Teknik Phishing – melalui SMS)

Pengguna telepon genggam di Indonesia naik secara pesat. Sudah lebih dari 100 juta nomor terjual pada akhir tahun 2008. Pelaku kriminal kerap memanfaatkan fitur-fitur yang ada pada telepon genggam atau sejenisnya untuk melakukan social engineering seperti yang terlihat pada contoh SMS berikut ini:

"Selamat. Anda baru saja memenangkan hadiah sebesar Rp 25,000,000 dari Bank X yang bekerjasama dengan provider telekomunikasi Y. Agar kami dapat segera mentransfer uang tunai kemenangan ke rekening bank anda, mohon diinformasikan user name dan passoword internet bank anda kepada kami. Sekali lagi kami atas nama Manajemen Bank X mengucapkan selamat atas kemenangan anda…"

Skenario 3 (Teknik Phishing – melalui Pop Up Windows)

Ketika seseorang sedang berselancar di internet, tiba-tiba muncul sebuah "pop up window" yang bertuliskan sebagai berikut:

"Komputer anda telah terjangkiti virus yang sangat berbahaya. Untuk membersihkannya, tekanlah tombol BERSIHKAN di bawah ini."

Tentu saja para awam tanpa pikir panjang langsung menekan tombol BERSIHKAN yang akibatnya justru sebaliknya, dimana penjahat berhasil mengambil alih komputer terkait yang dapat dimasukkan virus atau program mata-mata lainnya.

10.5 MENDETEKSI JENIS SOCIAL ENGINEERING LAINNYA

Karena sifatnya yang sangat "manusiawi" dan memanfaatkan interaksi sosial, teknik-teknik memperoleh informasi rahasia berkembang secara sangat variatif. Beberapa contoh adalah sebagai berikut:

- Ketika seseorang memasukkan password di ATM atau di PC, yang bersangkutan "mengintip" dari belakang bahu sang korban, sehingga karakter passwordnya dapat terlihat;
- Mengaduk-ngaduk tong sampah tempat pembuangan kertas atau dokumen kerja perusahaan untuk mendapatkan sejumlah informasi penting atau rahasia lainnya;
- Menyamar menjadi "office boy" untuk dapat masuk bekerja ke dalam kantor manajemen atau pimpinan puncak perusahaan guna mencari informasi rahasia;
- Ikut masuk ke dalam ruangan melalui pintu keamanan dengan cara "menguntit" individu atau mereka yang memiliki akses legal;
- Mengatakan secara meyakinkan bahwa yang bersangkutan terlupa membawa ID-Card yang berfungsi sebagai kunci akses sehingga diberikan bantuan oleh satpam;
- Membantu membawakan dokumen atau tas atau notebook dari pimpinan dan manajemen dimana pada saat lalai yang bersangkutan dapat memperoleh sejumlah informasi berharga;
- Melalui chatting di dunia maya, si penjahat mengajak ngobrol calon korban sambil pelan-pelan berusaha menguak sejumlah informasi berharga darinya;
- Dengan menggunakan situs social networking – seperti facebook, myspace, friendster, dsb. – melakukan diskursus dan komunikasi yang pelan-pelan mengarah pada proses "penelanjangan" informasi rahasia; dan lain sebagainya.

10.6 MENGIDENTIFIKASI TARGET KORBAN SOCIAL ENGINEERING

Statistik memperlihatkan, bahwa ada 4 (empat) kelompok individu di perusahaan yang kerap menjadi korban tindakan social engineering, yaitu:

1. *Receptionist* dan/atau *Help Desk* sebuah perusahaan, karena merupakan pintu masuk ke dalam organisasi yang relatif memiliki data/informasi lengkap mengenai personel yang bekerja dalam lingkungan dimaksud;
2. Pendukung teknis dari divisi teknologi informasi – khususnya yang melayani pimpinan dan manajemen perusahaan, karena mereka biasanya memegang kunci akses penting ke data dan informasi rahasia, berharga, dan strategis;

3. Administrator sistem dan pengguna komputer, karena mereka memiliki otoritas untuk mengelola manajemen password dan account semua pengguna teknologi informasi di perusahaan;
4. Mitra kerja atau vendor perusahaan yang menjadi target, karena mereka adalah pihak yang menyediakan berbagai teknologi beserta fitur dan kapabilitasnya yang dipergunakan oleh segenap manajemen dan karyawan perusahaan; dan
5. Karyawan baru yang masih belum begitu paham mengenai prosedur standar keamanan informasi di perusahaan.

10.7 MENETAPKAN SOLUSI MENGHINDARI RESIKO

Setelah mengetahui isu social engineering di atas, timbul pertanyaan mengenai bagaimana cara menghindarinya. Berdasarkan sejumlah pengalaman, berikut adalah hal-hal yang biasa disarankan kepada mereka yang merupakan pemangku kepentingan aset-aset informasi penting perusahaan, yaitu:

- Selalu hati-hati dan mawas diri dalam melakukan interaksi di dunia nyata maupun di dunia maya. Tidak ada salahnya perilaku "ekstra hati-hati" diterapkan di sini mengingat informasi merupakan aset sangat berharga yang dimiliki oleh organisasi atau perusahaan;
- Organisasi atau perusahaan mengeluarkan sebuah buku saku berisi panduan mengamankan informasi yang mudah dimengerti dan diterapkan oleh pegawainya, untuk mengurangi insiden-insiden yang tidak diinginkan;
- Belajar dari buku, seminar, televisi, internet, maupun pengalaman orang lain agar terhindar dari berbagai penipuan dengan menggunakan modus social engineering;
- Pelatihan dan sosialisasi dari perusahaan ke karyawan dan unit-unit terkait mengenai pentingnya mengelola keamanan informasi melalui berbagai cara dan kiat;
- Memasukkan unsur-unsur keamanan informasi dalam standar prosedur operasional sehari-hari – misalnya "clear table and monitor policy" - untuk memastikan semua pegawai melaksanakannya; dan lain sebagainya.

Selain usaha yang dilakukan individu tersebut, perusahaan atau organisasi yang bersangkutan perlu pula melakukan sejumlah usaha, seperti:

- Melakukan analisa kerawanan sistem keamanan informasi yang ada di perusahaannya (baca: *vulnerability analysis*);
- Mencoba melakukan uji coba ketangguhan keamanan dengan cara melakukan "penetration test";
- Mengembangkan kebijakan, peraturan, prosedur, proses, mekanisme, dan standar yang harus dipatuhi seluruh pemangku kepentingan dalam wilayah organisasi;

- Menjalin kerjasama dengan pihak ketiga seperti vendor, ahli keamanan informasi, institusi penanganan insiden, dan lain sebagainya untuk menyelenggarakan berbagai program dan aktivitas bersama yang mempromosikan kebiasaan perduli pada keamanan informasi;
- Membuat standar klasifikasi aset informasi berdasarkan tingkat kerahasiaan dan nilainya;
- Melakukan audit secara berkala dan berkesinambungan terhadap infrastruktur dan suprastruktur perusahaan dalam menjalankan keamanan informasi; dan lain sebagainya.

-oo0oo-

~ 11 ~

MANAJEMEN PASSWORD

Capaian Pembelajaran (*Learning Outcomes*):

1. Menguraikan Seluk Beluk Manajemen Password
2. Menjelaskan Teknik Membuat Password
3. Menyusun Strategi Melindungi Keamanan Password
4. Menjelaskan Kiat Memelihara Password

Terlepas dari beraneka-ragamnya keberadaan sistem dan model keamanan informasi berbasis teknologi yang canggih yang ada di pasaran, pada tataran penggunaannya – terutama untuk user awam dan kebanyakan – kata kunci atau yang dikenal sebagai "password" merupakan pendekatan keamanan yang paling lumrah dipakai. Mulai dari cara mengoperasikan ATM, internet banking, email account, dan sistem operasi sampai dengan mengendalikan mobil, mengakses kamera keamanan, menjalankan robot, dan mengkonfigurasi sistem, password merupakan hal yang sangat krusial dalam menjaga keamanan hak aksesnya.

Namun statistik memperlihatkan bahwa kasus kejahatan yang terjadi dengan cara "membobol password" jumlahnya makin lama semakin banyak belakangan ini. Dan uniknya, modus operasi kejahatan keamanan informasi yang terkenal sangat klasik dan konvensional ini belakangan menjadi sebuah trend yang menggejala kembali. Apakah yang sebenarnya terjadi? Hasil riset dan pengamatan sejumlah lembaga independen memperlihatkan bahwa penyebab utama kasus kejahatan meningkat karena buruknya manajemen password dari pengguna atau user komputer.

11.1 MENGURAIKAN SELUK BELUK MANAJEMEN PASSWORD

Manajemen password merupakan suatu tata cara mengelola kata kunci oleh pengguna agar fungsinya sebagai gerbang keamanan informasi dapat secara efektif berperan. Dalam mengelola password ini ada sejumlah hal yang perlu untuk diperhatikan sungguh-sungguh. Berikut adalah beberapa hal penting yang patut untuk dimengerti dan dipertimbangkan sungguh-sungguh oleh semua pengguna password.

Memilih Password yang Baik

Kriteria password yang baik sebenarnya cukup sederhana, hanya dibatasi oleh dua syarat, yaitu: mudah diingat oleh pemiliknya, dan pada saat yang sama sulit ditebak oleh orang lain atau mereka yang tidak berhak mengetahuinya. Dalam prakteknya, persyaratan tersebut merupakan sesuatu yang susah-susah mudah untuk diterapkan. Kebanyakan password yang mudah diingat oleh pemiliknya cenderung mudah ditebak oleh orang lain. Sementara sebuah password yang dinilai aman karena sulit diterka oleh mereka yang tidak berhak, cenderung sulit diingat oleh yang memilikinya. Oleh karena itulah maka diperlukan suatu teknik khusus untuk memilih password agar di satu pihak aman karena terdiri dari susunan karakter yang sulit ditebak, namun di sisi lain mudah bagi sang pemilik untuk mengingatnya.

Kriteria Password Ideal

Password yang baik disarankan memiliki sejumlah karakteristik sebagai berikut:

- Terdiri dari minimum 8 karakter – dimana pada prinsipnya adalah makin banyak karakternya semakin baik, direkomendasikan password yang relatif aman jika terdiri dari 15 karakter;
- Pergunakan campuran secara random dari berbagai jenis karakter, yaitu: huruf besar, huruf kecil, angka, dan simbol;
- Hindari password yang terdiri dari kata yang dapat ditemukan dalam kamus bahasa;
- Pilih password yang dengan cara tertentu dapat mudah mengingatnya; dan
- Jangan pergunakan password yang sama untuk sistem berbeda.

Dalam menentukan password tersebut, ada sejumlah hal yang sebaiknya dihindari karena karakteristik password berikut ini telah banyak "diketahui" variasinya oleh para kriminal, yaitu:

- Jangan menambahkan angka atau simbol setelah atau sebelum kata-kata yang biasa dikenal, seperti: pancasila45, nusantara21, 17agustus45, dan lain-lain;
- Jangan menggunakan pengulangan dari kata-kata, seperti: rahasiarahasia, racunracun, ayoayoayo, dan lain-lain;
- Jangan hanya membalikkan karakter dari sebuah kata yang lazim, seperti: gnudih, adamra, kumayn, dan lain-lain;
- Jangan merupakan sebuah kata yang dihilangkan huruf vokalnya, seperti: ndns (dari kata 'indonesia'), pncsl (dari kata 'pancasila'), pnsrn (dari kata 'penasaran'), dan lain-lain;
- Jangan menggunakan susunan karakter yang merupakan urutan penekanan pada tombol-tombok keyboard, seperti: qwerty, asdfghjk, mnbvcxz, dan lain-lain; dan
- Jangan hanya sekedar menggantikan karakter huruf dengan angka seperti halnya nomor cantik pelat mobil tanpa melakukan sejumlah improvisasi, seperti: s3l4m4t, g3dungt1ngg1, 5ul4we5i, dan lain-lain.

11.2 MENJELASKAN TEKNIK MEMBUAT PASSWORD

Berdasarkan prinsip-prinsip yang telah dipaprkan sebelumnya, berikut adalah sejumlah trik dalam mendesain atau menentukan password yang baik. Ada sejumlah pendekatan yang dipergunakan, yang pada intinya bertumpu pada bagaimana cara mengingat sebuah password yang aman.

Trik #1: Berbasis Kata

Katakanlah Donny seorang pemain basket ingin menentukan sebuah password yang aman dan sekaligus mudah diingat. Hal-hal yang dilakukannya mengikuti langkah-langkah sebagai berikut:

1. Memilih sebuah kata yang sangat kerap didengar olehnya dalam kapasistasnya sebagai pemain basket, misalnya adalah: **JORDAN**.
2. Merubah huruf "O" dengan angka "0" dan merubah huruf "A" dengan angka "4" sehingga menjadi: **J0RD4N**.
3. Merubah setiap huruf konsonan kedua, keempat, keenam, dan seterusnya menjadi huruf kecil, sehingga menjadi: **J0rD4n**.
4. Memberikan sebuah variabel simbol tambahan di antaranya; karena Donny terdiri dari 5 huruf, maka yang bersangkutan menyelipkan suatu variabel simbol pada urutan huruf yang kelima, menjadi: **J0rD%4n**.

Trik #2: Berbasis Kalimat

Ani adalah seorang karyawan perusahaan yang memiliki hobby bernyanyi, untuk itulah maka yang bersangkutan akan menggunakan kegemarannya tersebut sebagai dasar pembuatan password aman yang mudah diingat. Berikut adalah urutan pelaksanaannya:

1. Mencari kalimat pertama sebuah lagu yang disenangi, misalnya adalah: "Terpujilah Wahai Engkau Ibu Bapak Guru, Namamu Akan Selalu Hidup Dalam Sanubariku", dimana kumpulan huruf pertama setiap kata akan menjadi basis password menjadi: **TWEIBGNASHDS**.
2. Ubahlah setiap huruf kedua, keempat, keenam, dan seterusnya menjadi huruf kecil, sehingga menjadi: **TwEiBgNaShDs**.
3. Untuk sisa huruf konsonan, ubahlah menjadi angka, seperti: **Tw3i8gNa5hDs**.
4. Kemudian untuk huruf kecil, ubahlan dengan simbol yang mirip dengannya: **Tw3!8gN@5hDs**.

Kedua trik di atas hanyalah sejumlah contoh pendekatan yang dapat dipergunakan oleh siapa saja yang ingin menentukan atau menyusun password yang mudah diingat dan relatif aman seperti yang disyaratkan dalam paparan terdahulu.

11.3 MENYUSUN STRATEGI MELINDUNGI KEAMANAN PASSWORD

Setelah memiliki password yang baik, hal selanjutnya yang perlu diperhatikan adalah bagaiaman menjaga dan melindunginya. Ada sejumlah hal yang perlu dilakukan, misalnya:

- Jangan sekali-kali menyimpan password di dalam piranti elektronik seperti komputer, telepon genggam, personal digital assistant, dsb. kecuali dalam keadaan ter-enkripsi (password yang telah disandikan sehingga menjadi sebuah karakter acak);
- Dilarang memberitahukan password anda kepada siapapun, termasuk "system administrator" dari sistem terkait;
- Hindari tawaran fitur "save password" dalam setiap aplikasi browser atau program lainnya yang memberikan tawaran kemudahan ini;
- Hindari memanfaatkan menu yang bisa membantu melihat password ketika sedang dimasukkan;
- Ketika sedang memasukkan password, pastikan tidak ada orang yang berada di sekitar, pastikan tidak terdapat pula kamera CCTV di belakang pundak; dan
- Jika karena suatu hal harus menuliskan password di kertas sebelum memasukkannya ke dalam sistem, pastikan bahwa setelah digunakan, kertas tersebut dihancurkan sehingga tidak mungkin direkonstruksi lagi.

Ada sebuah hal yang perlu diperhatikan, terutama ketika seseorang telah berhasil masuk ke dalam sistem dengan menggunakan password yang dimaksud:

- Lakukan "log out" setelah sistem selesai dipergunakan atau pada saat yang bersangkutan harus jeda sebentar melakukan sesuatu hal (misalnya: dipanggil bos, pergi ke toilet, menerima telepon, dan lain sebagainya);
- Jangan biarkan seseorang melakukan interupsi di tengah-tengah yang bersangkutan berinteraksi dengan sistem yang ada;
- Ada baiknya "protected automatic screen saver" diaktifkan jika dalam kurun waktu 15-30 detik tidak terdapat interaksi pada keyboard maupun mouse;
- Pastikan dalam arti kata lakukan cek-and-ricek terhadap kondisi komputer dan aplikasi agar benar-benar telah berada pada level aman sebelum meninggalkan perimeter; dan
- Biasakan memeriksa meja tempat mengoperasikan komputer untuk memastikan tidak ada bekas-bekas maupun torehan yang dapat mengarah atau menjadi petunjuk bagi aktivitas pembobolan password oleh mereka yang tidak berhak.

11.4 MENJELASKAN KIAT MEMELIHARA PASSWORD

Walaupun terlihat aman, adalah sangat bijaksana untuk mengganti password secara berkala, misalnya sebulan sekali atau seminggu sekali tergantung kebutuhan dan konteksnya. Password yang kerap diganti akan menyulitkan seorang kriminal untuk membobolnya. Dalam prakteknya, ada pula individu yang kerap mengganti passwordnya setiap kali kembali dari perjalanan dinas ke luar kota dan/atau ke luar negeri, hanya untuk memastikan bahwa tidak terdapat hal-hal mengandung

resiko yang dibawanya atau diperolehnya selama yang bersangkutan bepergian. Hal yang perlu diperhatikan pula adalah hindari menggunakan password yang sama untuk sistem yang berbeda, karena disamping akan meningkatkan resiko, juga akan mempermudah kriminal dalam menjalankan aksinya. Intinya adalah bahwa setiap kali seseorang merasa bahwa password yang dimilikinya sudah terlampau lama dipergunakan, dan/atau yang bersangkutan merasa sudah banyak orang di sekelilingnya yang terlibat dengannya dengan kemungkinan ada satu atau dua di antara mereka yang tertarik untuk mengetahui password terkait, tidak perlu ragu-ragu untuk segera mengganti password tersebut. Perhatian khusus perlu ditujukan bagi mereka yang aktif berwacana atau berinteraksi di media jejaring sosial seperti Facebook, Friendster, MySpace, dan Twitter – pastikan tidak ada kata atau kalimat yang secara langsung maupun tidak langsung dapat menjadi petunjuk bagi kriminal dalam melakukan kegiatannya. Ingat, cara klasik yang kerap dipergunakan oleh para pembobol password adalah:

- Menebak-nebak password dengan menggunakan analisa mengenai profil dan/atau karakteirstik pemiliknya;
- Menggunakan “brute force attack” alias mencoba segala bentuk kemungkinan kombinasi karakter yang bisa dipergunakan dalam password;
- Menggunakan referensi kata-kata pada kamus sebagai bahan dasar pembobolannya;
- Melakukan teknik “social engineering” kepada calon korban pemilik password;
- Melakukan pencurian terhadap aset-aset yang mengarah pada informasi penyimpanan password; dan lain sebagainya.

Perlu diperhatikan, bahwa teknik-teknik di atas saat ini dilakukan secara otomatis – alias menggunakan teknologi, tidak seperti dahulu yang bersifat manual, sehingga tidak diperlukan waktu lama untuk melaksanakannya (walaupun lama sekalipun tidak akan berpengaruh karena yang mengerjakannya adalah mesin komputer). Statistik memperlihatkan bahwa dari hari ke hari, waktu untuk mengeksploitasi keamanan komputer semakin bertambah singkat.

-oo0oo-

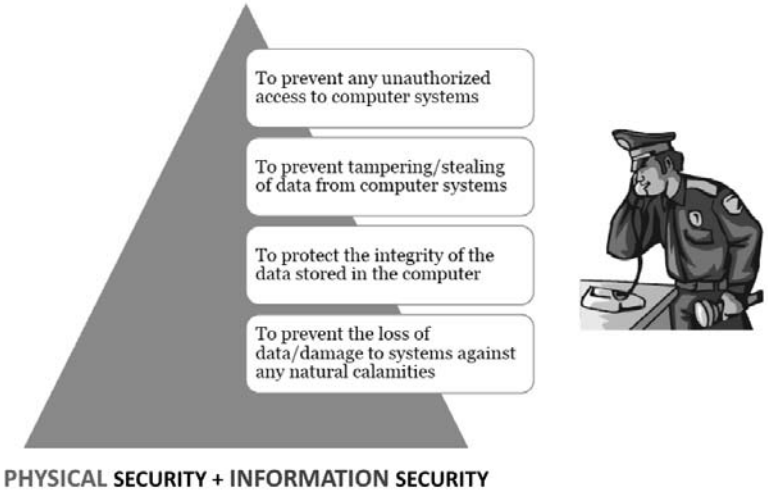
~ 12 ~

STRATEGI ORGANISASI MENGAMANKAN DIRI

Capaian Pembelajaran (*Learning Outcomes*):

1. Menjelaskan Aspek Keamanan pada Lingkungan Fisik
2. Mengembangkan Strategi Pengamanan Informasi

"Budaya aman" belumlah menjadi suatu perilaku sehari-hari dari kebanyakan karyawan atau pegawai dalam sebuah perusahaan atau organisasi. Pengalaman membuktikan bahwa kebanyakan insiden keamaman informasi terjadi karena begitu banyaknya kecorobohan yang dilakukan oleh staf organisasi maupun karena kurangnya pengetahuan dari yang bersangkutan terkait dengan aspek-aspek keamanan yang dimaksud.



Gambar 12.1 *Tujuan Keamanan Informasi*

Tujuan utama dari kebijakan keamanan informasi dari sebuah perusahaan atau organisasi secara prinsip ada 4 (empat) buah, yaitu masing-masing:

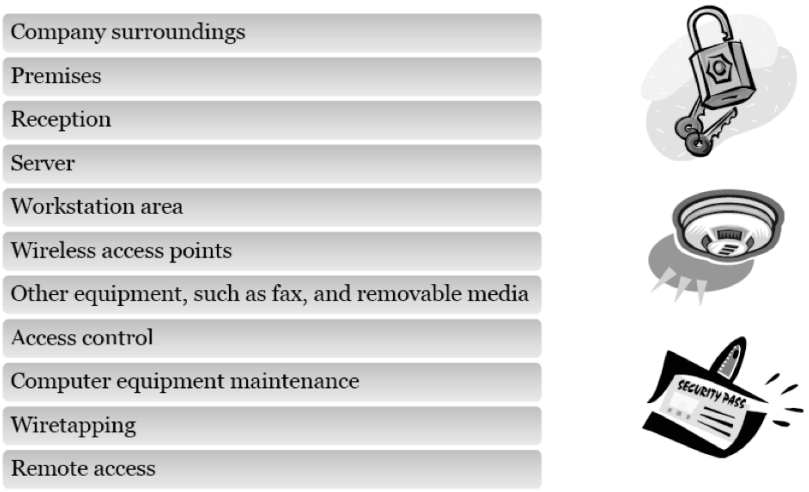
- Mencegah adanya pihak-pihak yang tidak berhak dan berwenang melakukan akses ke sistem komputer atau teknologi informasi milik organisasi;
- Mencegah terjadinya pencurian data dari sebuah sistem komputer atau media penyimpanan data yang ada dalam teritori organisasi;
- Melindungi keutuhan dan integritas data yang dimiliki organisasi agar tidak dirubah, diganti, atau diganggu keasilannya; dan
- Menghindari diri dari dirusaknya sistem komputer karena berbagai tindakan kerusakan yang dilakukan secara sengaja maupun tidak.

Untuk dapat mencapai tujuan ini, setiap individu dalam organisasi haruslah benar-benar mengimplementasikan "budaya aman", yaitu suatu kebiasaan atau perilaku menjaga keamanan dengan memperhatikan dua aspek penting, yaitu: lingkungan fisik dan keamanan informasi.

12.1 MENJELASKAN ASPEK KEAMANAN PADA LINGKUNGAN FISIK

Paling tidak ada 11 (sebelas) hal terkait dengan lingkungan fisik yang harus benar-benar diperhatikan oleh staf karyawan maupun manajemen yang bekerja dalam

organisasi atau perusahaan. Berikut adalah penjelasan dari masing-masing aspek yang dimaksud.



Gambar 12.2 *Menjaga Keamanan Lingkungan Fisik*

Akses Masuk Organisasi

Hal pertama yang harus diperhatikan adalah memastikan diperhatikannya faktor keamanan pada seluruh pintu atau akses masuk ke dalam perusahaan, mulai dari pintu gerbang masuk ke dalam komplek usaha sampai dengan seluruh jalan atau pintu masuk ke setiap ruangan yang perlu dilindungi. Karena pintu-pintu ini merupakan jalan akses masuk ke dalam lingkungan perusahaan secara fisik, perlu dipastikan bahwa hanya mereka yang memiliki otoritas atau hak saja yang boleh masuk ke dalam lingkungan yang dimaksud. Oleh karena itu, perlu diterapkan sejumlah fasilitas dan prosedur keamanan di titik-titik ini, seperti: pemanfaatan kartu identitas elektronik untuk masuk melalui gerbang otomatis, pengecekan identitas individu oleh satuan petugas keamanan (satpam), penukaran kartu identitas dengan kartu akses teritori perusahaan, penggunaan sidik jari dan retina mata sebagai bukti identitas untuk membuka pintu, dan lain sebagainya.

Lingkungan Sekitar Organisasi

Walaupun sekilas nampak bahwa pintu masuk adalah satu-satunya jalan akses menuju perusahaan, namun pada kenyataannya terdapat sejumlah area yang dapat dimanfaatkan oleh pelaku kejahatan dalam menjalankan aksinya. Katakanlah akses masuk ke lingkungan perusahaan dapat melalui pagar yang dapat dipajat dan dilompati, atau melalui jendela yang dapat dibuka dengan mudah, atau melalui dinding kaca yang dapat dijebol, atau atap gedung yang mudah dirombak, atau lubang alat pendingan yang dapat dibongkar, dan lain sebagainya. Cara melindungi titik-titik penting ini antara lain dilakukan dengan menggunakan kamera CCTV,

atau memasang sistem alarm, atau memelihara anjing pelacak, atau mengaliri pagar dengan tegangan listrik, dan cara-cara lainnya.

Daerah Pusat Informasi (Reception)

Banyak perusahaan tidak sadar, bahwa daerah "receptionist" merupakan sebuah titik rawan yang harus diperhatikan keamanannya. Ada sejumlah alasan dibalik pernyataan ini. Pertama, karena fungsi dan tugasnya sebagai sumber informasi, maka biasanya di meja seorang *receptionist* dapat ditemukan berbagai data dan informasi berharga, seperti: nama pegawai dan nomor telpon ekstensionnya, detail lokasi unit dan pimpinannya, daftar pengunjung individu atau unit tertentu, informasi kehadiran karyawan perusahaan, dan lain sebagainya. Kedua, daerah di sekitar *receptionist* adalah wilayah yang paling ramai dan sibuk karena yang bersangkutan harus berhadapan dengan tamu perusahaan yang keluar masuk. Tentu saja jumlah yang tidak imbang ini membuat sulitnya mengamati dan mengawasi perilaku semua tamu yang berada di sekitarnya. Ketiga, karena sifatnya sebagai "penerima tamu", seorang *receptionist* biasanya cenderung memiliki perilaku yang ramah dan berfikir positif terhadap keberadaan semua tamu. Oleh karena itu, mudah sekali bagi pelaku kejahatan dalam melakukan tindakan social engineering terhadap seorang *receptionist*. Oleh karena itulah perlu dilakukan sejumlah tindakan pengamanan seperti: menghindari bercecernya catatan, dokumen, atau kertas-kertas berisi informasi di meja receptionist, mendesain meja receptionist agar tidak ada sisi yang memungkinkan kontak langsung dengan tamu, memposisikan monitor komputer sedemikian rupa agar tidak mudah diintip oleh orang lain, mengunci secara fisik seluruh peralatan yang dipergunakan dalam bertugas, dan lain sebagainya.

Ruang Server

Server adalah "jantung dan otaknya" perusahaan, karena selain terkoneksi dengan pusat-pusat penyimpanan data, entitas ini merupakan penggerak dan pengatur lalu lintas data serta informasi yang ada di perusahaan. Oleh karena itulah maka secara fisik keberadaannya harus dijaga dengan sebaik-baiknya. Pertama adalah ruangan server harus tersedia dengan kondisi ruangan sesuai dengan persyaratan teknis yang berlaku. Kedua tidak boleh sembarang orang masuk ke ruang server tersebut, kecuali yang memiliki otoritas dan hak akses. Ketiga, pastikan server tersebut "terkunci" dan "terpasung" kuat di tempatnya, tidak berpindah-pindah dari satu tempat ke tempat lain. Keempat, set konfigurasi server dengan baik sehingga tidak memungkinkan adanya pintu akses ke dalamnya, misalnya dengan cara mematikan semua saluran atau port media eksternal, mempartisi sistem operasi sesuai dengan hak akses dan tingkat keamanan, dan lain sebagainya.

Area Workstation

Ini merupakan tempat dimana kebanyakan karyawan bekerja, yaitu terdiri dari sejumlah meja dengan komputer dan/atau notebook di atasnya. Dalam konteks ini, perusahaan perlu membuat kebijakan dan peraturan yang harus disosialisasikan kepada karyawannya, terutama terkait dengan masalahan keamanan informasi ditinjau dari sisi keamanan fisik. Salah satu kebiasaan yang baik untuk disosialisasikan dan diterapkan adalah "clear table and clean monitor policy" – yaitu suatu kebiasaan membersihkan meja dan "mematikan" monitor komputer setiap kali karyawan sebagai pengguna hendak meninggalkan meja – baik sementara atau pun sebelum pulang ke rumah.

Wireless Access Points

Hampir semua lingkungan perusahaan sekarang diperlengkapi dengan Wireless Access Points atau Hot Spot. Selain murah dan praktis dalam penggunaannya, medium komunikasi "wireless" ini dianggap dapat menjawab berbagai kebutuhan berkomunikasi antar para pemangku kepentingan perusahaan. Yang perlu untuk diperhatikan adalah mengenai keamanannya, karena kerap kali perusahaan lalai dalam melakukannya. Bayangkan saja, jika seorang penyusup berhasil masuk via WAP atau Hot Spot ini, berarti yang bersangkutan berhasil masuk ke dalam sistem perusahaan. Oleh karena itulah perlu diperhatikan sejumlah hal terkait dengan keamanannya, seperti: terapkan enkripsi pada WEP, jangan memberitahu SSID kepada siapapun, untuk masuk ke WAP harus menggunakan password yang sulit, dan lain sebagainya.

Faksimili dan Media Elektronik Lainnya

Dalam satu hari, sebuah perusahaan biasanya menerima berpuluh-puluh fax dari berbagai tempat, dimana data atau informasi yang dikirimkan dapat mengandung sejumlah hal yang sangat penting dan bersifat rahasia. Oleh karena itulah perlu diperhatikan pengamanan terhadap mesin faksimili ini, terutama dalam proses penerimaan dan pendistribusiannya ke seluruh unit perusahaan terkait. Demikian pula dengan berbagai media elektronik terkait seperti: modem, printer, eksternal drive, flash disk, CD-ROM, dan lain sebagainya. Jangan sampai beragam media elektronik ini berserakan tanpa ada yang mengelola dan bertanggung jawab, karena jika berhasil diambil oleh yang tidak berhak dapat mengakibatkan berbagai insiden yang tidak diinginkan.

Entitas Kendali Akses

Di sebuah perusahaan moderen dewasa ini sering kali diterapkan manajemen identitas dengan menggunakan berbagai entitas yang sekaligus berfungsi

sebagai kunci akses terhadap berbagai fasilitas perusahaan. Misalnya adalah kartu identitas, modul biometrik, token RFID, sensor wajah dan suara, dan lain sebagainya. Mengingat bahwa keseluruhan entitas ini adalah kunci akses ke berbagai sumber daya yang ada, maka keberadaan dan keamanannya harus dijaga sungguh-sungguh. Sebagai pemegang kartu identitas misalnya, jangan menaruh kartu tersebut di sembarang tempat sehingga dapat dicuri orang; atau untuk model token RFID, pastikan bahwa token yang ada selalu berada dalam posesi yang bersangkutan; dan lain sebagainya.

Pengelolaan Aset Komputer

Hal ini merupakan sesuatu yang sederhana namun jarang dilakukan oleh sebuah organisasi semacam perusahaan, yaitu pemeliharaan aset komputer. Seperti diketahui bersama, karyawan mengalami proses promosi, mutasi, dan demosi – dimana yang bersangkutan dapat berpindah-pindah unit kerjanya. Di setiap penugasannya, biasanya yang bersangkutan mendapatkan akses ke komputer tertentu. Permasalahan timbul ketika sebelum pindah jabatan, yang bersangkutan lupa menghapus seluruh file penting, baik milik pribadi maupun perusahaan. Akibat kelupaan tersebut, penggantinya dengan leluasa dapat mengakses file-file yang dimaksud. Masalah yang lebih besar lagi adalah ketika perusahaan berniat untuk mengganti seluruh komputer-komputer yang sudah usang dengan yang baru. Karena alasan biaya dan waktu, banyak perusahaan yang tidak melakukan proses format ulang atau bahkan pemusnahan terhadap data yang masih tersimpan di hard disk komputer usang tersebut. Perlu pula dijaga dengan hati-hati jika perusahaan menyerahkan kepada pihak ketiga untuk melakukan pemeliharaan sistem komputer yang dimaksud, misalnya dalam hal: pemutakhiran program anti virus, proses penataan ulang file dalam hard disk (defragmentation), dan lain sebagainya.

Penyadapan

Sudah bukan rahasia umum lagi, dengan dipicu oleh semakin berkembangnya kemajuan teknologi informasi dan komunikasi dewasa ini, harga peralatan untuk melakukan penyadapan terhadap media komunikasi menjadi sangat murah. Siapa saja dapat membelinya dan menginstalnya untuk keperluan positif maupun untuk tindakan kriminal. Perlu diingat bahwa di Indonesia, hanya penegak hukum yang boleh melakukan penyadapan; dalam arti kata, seluruh kegiatan penyadapan dalam bentuk apa pun tidaklah sah atau merupakan suatu tindakan kejahatan. Oleh karena itu, perusahaan perlu melakukan aktivitas untuk menyapu bersih kemungkinan adanya alat-alat sadap di sekitar daerah atau lokasi yang penting, seperti: telepon direktur, ruang rapat manajemen, koneksi ke/dari server pusat, dan

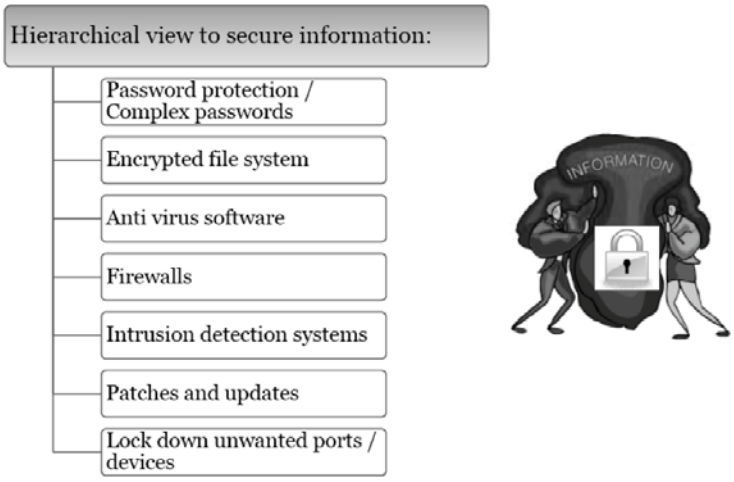
lain sebagainya. Inspeksi dan audit yang teliti perlu dilakuan untuk memastikan tidak terjadi kegiatan penyadapan dalam perusahaan.

Remote Access

"Remote Access" adalah cara termudah bagi pegawai atau karyawan untuk bekerja di luar teritori perusahaan, seperti di rumah, di kendaraan, di tempat publik, dan lain-lain. Walaupun ditinjau dari segi bisnis hal tersebut sangatlah menguntungkan dan memberikan nilai tambah, namun ditinjau dari aspek keamanan informasi hal tersebut mendatangkan sejumlah resiko baru. Karena sifatnya yang "remote" atau "kendali jauh", maka terdapat banyak sekali titik-titik dimana pelaku kejahatan dapat melakukan aksi penetrasi dan eksploitasinya. Oleh karena itu saran yang baik untuk dilakukan adalah melakukan enkripsi atau penyandian terhadap data dan/atau informasi yang dikirimkan agar tidak dapat dibaca oleh mereka yang mencoba untuk menyadap atau memanipulasinya.

12.2 MENGEMBANGKAN STRATEGI PENGAMANAN INFORMASI

Setelah mengamankan lingkungan fisik, hal berikut yang disarankan untuk dilakukan adalah mengamankan konten dari data dan/atau informasi itu sendiri. Paling tidak ada 7 (tujuh) hal yang dapat dilakukan terkait dengan hal ini seperti yang dipaparkan di bawah ini.



Gambar 12.3 *Skala Prioritas Mengamankan Informasi*

Proteksi Password

Memproteksi akses ke beberapa file dan program dengan menggunakan password merupakan cara lumrah yang paling banyak dipergunakan. Dalam kaitan ini sang

pengguna harus paham benar cara mengelola password yang baik, mulai dari menentukan password yang aman hingga memelihara dan memperbaharuinya. Password yang aman biasanya minimum terdiri dari 6 (enam) buah karakter yang merupakan campuran dari huruf besar dan kecil, angka, serta simbol. Dan paling tidak setiap 3 (tiga) bulan sekali password tersebut diganti dan diperbaharui.

Enkripsi File

Jika memang data dan/atau informasi yang dimiliki dan didistribusikan sedemikian pentingnya, ada baiknya file-file elektronik tersebut dienkripsi atau disandikan; sehingga jika ada pelaku kejahatan berhasil menyadap atau memperoleh data/informasi yang dimaksud, yang bersangkutan mengalami kesulitan dalam membacanya. Kebiasaan melakukan enkripsi terhadap file-file penting di perusahaan harus mulai disosialisasikan dan dibudayakan, terutama oleh kalangan manajemen yang berhubungan erat dengan informasi rahasia dan penting.

Software Anti Virus

Program anti virus ada baiknya diinstal pada server atau komputer yang di dalamnya terdapat data atau informasi penting. Perlu diperhatikan bahwa efektivitas sebuah program atau software anti virus terletak pada proses pemutakhiran atau "upgrading" file-file library terkait dengan jenis-jensi virus yang baru. Tanpa adanya aktivitas pemutakhiran, maka anti virus tidak akan banyak membantu karena begitu banyaknya virus-virus baru yang diperkenalkan setiap harinya. Dalam konteks ini jelas terlihat bahwa tidak ada gunanya menginstal program anti virus bajakan, karena selain bertentangan dengan HAKI, juga tidak bisa dilakukan aktivitas pemutakhiran. Banyak orang belakangan ini yang meremehkan kemampuan virus. Statistik memperlihatkan bahwa semakin banyak virus-virus baru yang bersifat destruktif terhadap file dan sistem komputer dewasa ini; belum lagi kemampuan virus dalam mengendalikan atau mengakses sistem komputer yang dapat menyebabkan perilaku kriminal dan dapat terjerat undang-undang terkait dengan "cyber law".

Firewalls

Perangkat ini merupakan program atau piranti keras (baca: hardware) yang memiliki fungsi utama untuk melindungi jejaring sistem komputer internal dari lingkungan luar. Tugas utamanya adalah menjadi filter terhadap trafik data dari luar, dimana jika dipandang aman, data yang datang dari luar akan diteruskan ke dalam jejaring internal, namun jika ditemukan hal-hal yang mencurigakan atau yang tidak diinginkan, maka data yang dimaksud akan ditolak. Selain data, segala

bentuk akses dari luar ke jejaring komputer juga dapat diseleksi oleh firewalls. Dengan diinstalasinya firewalls ini paling tidak data yang ada di dalam internal perusahaan dapat terlindung dari akses luar.

Intrusion Detection System

IDS atau Intrusion Detection System adalah sebuah piranti lunak atau keras yang memililki fungsi utama untuk mendeteksi terjadinya aktivitas "penyusupan" pada jejaring sistem internal perusahaan. Cara kerja sistem ini adalah menganalisa paket-paket trafik data yang ada; jika terdapat jenis paket yang mencurigakan atau tidak normal, maka IDS akan memberikan peringatan kepada administrator sistem. Paket yang tidak normal dapat berisi macam-macam jenis serangan terhadap data maupun sistem yang ada, misalnya dalam bentuk DOS/DDOS, botnet, SQL injection, dan lain sebagainya.

Pemutakhiran Patches

Tidak ada program atau aplikasi yang dibangun dengan sempurna atau bebas dari kesalahan (baca: error). Untuk itu biasanya produsen yang bersangkutan menyediakan program tambalan atau "patches" untuk menutup lubang-lubang kesalahan atau kerawanan yang ditemukan pada program, software, atau aplikasi tertentu. Dengan selalu dimutakhirkannya sistem dengan berbagai patches, maka paling tidak lubang-lubang kerawanan yang dapat dieksploitasi oleh pelaku kejahatan untuk mengambil dan merusak data dalam perusahaan dapat dihindari.

Penutupan Port dan Kanal Akses

Sistem komputer dihubungkan dengan entitas luar melalui port. Dengan kata lain, port merupakan jalan yang dapat dipergunakan oleh pihak luar untuk menyusup atau masuk ke dalam komputer. Seperti halnya pintu dan jendela dalam sebuah rumah, sistem komputer memiliki pula beberapa port; ada yang secara aktif dibuka untuk melayani berbagai kebutuhan input dan output, dan ada pula yang dibiarkan terbuka tanpa fungsi apa-apa. Sangatlah bijaksana untuk "menutup" saja seluruh port yang terbuka dan tanpa fungsi tersebut untuk mencegah adanya pihak yang tidak bertanggung jawab masuk ke sistem komputer melalui kanal tersebut.

-oo0oo-

~ 13 ~

MENYUSUN KEBIJAKAN KEAMANAN INFORMASI DAN INTERNET

Capaian Pembelajaran (*Learning Outcomes*):

1. Memahami Pentingnya Dokumen Kebijakan Keamanan
2. Menguraikan Elemen Kunci Kebijakan Keamanan
3. Menjelaskan Peranan dan Tujuan Keberadaan Kebijakan Keamanan
4. Menyebutkan Klasifikasi Jenis Kebijakan Keamanan
5. Menyusun Panduan Rancangan Konten Dokumen Kebijakan Keamanan
6. Menyusun Strategi Implementasi Kebijakan Keamanan
7. Memberikan Contoh Model Kebijakan Keamanan

13.1 MEMAHAMI PENTINGNYA DOKUMEN KEBIJAKAN KEAMANAN

Keberadaan dokumen "Kebijakaan Keamanan" atau "Security Policies" merupakan sebuah infrastruktur keamanan yang harus dimiliki oleh sebuah organisasi atau perusahaan yang ingin melindungi aset informasi terpentingnya. Dokumen ini secara prinsip berisi berbagai cara (baca: kendali) yang perlu dilakukan untuk mengontrol manajemen, mekanisme, prosedur, dan tata cara dalam mengamankan informasi, baik secara langsung maupun tidak langsung. Karena berada pada tataran kebijakan, maka dokumen ini biasanya berisi hal-hal yang bersifat prinsip dan strategis. Dengan adanya kebijakan ini, selain akan membantu organisasi dalam mengamankan aset pentingya, juga menghindari adanya insiden atau tuntutan hukum akibat organisasi terkait lalai dalam melakukan pengelolaan internal terhadap aset informasi atau hal-hal terkait dengan tata kelola informasi yang berada dalam lingkungannya. Kebijakan yang dimaksud juga bersifat teknologi netral, artinya tidak tergantung atau spesifik terhadap penggunaan merek teknologi tertentu.

13.2 MENGURAIKAN ELEMEN KUNCI KEBIJAKAN KEAMANAN

EC-Council melihat ada 7 (tujuh) elemen kunci yang harus diperhatikan dalam menyusun kebijakan keamanan, masing-masing adalah:

1. Komunikasi yang jelas mengenai arti dan pentingnya sebuah kebijakan keamanan untuk disusun dan ditaati oleh seluruh pemangku kepentingan perusahaan;
2. Definisi yang jelas dan ringkas mengenai aset informasi apa saja yang harus diprioritaskan untuk dilindungi dan dikelola dengan sebaik-baiknya;
3. Penentuan ruang lingkup pemberlakukan kebijakan yang dimaksud dalam teritori kewenangan yang ada;
4. Jaminan adanya sanksi, perlindungan, dan penegakan hukum terhadap para pelaku yang terkait dengan manajemen informasi sesuai dengan peraturan dan undang-undang yang berlaku;
5. Adanya pembagian tugas dan tanggung jawab yang jelas terhadap personel atau SDM yang diberikan tugas untuk melakukan kegiatan pengamanan informasi;
6. Penyusunan dokumen atau referensi panduan bagi seluruh pemangku kepentingan dan pelaku manajemen keamanan informasi untuk menjamin penerapan yang efektif; dan

7. Partisipasi aktif dan intensif dari manajemen atau pimpinan puncak organisasi untuk mensosialisasikan dan mengawasi implementasi kebijakan dimaksud.

13.3 MENJELASKAN PERANAN DAN TUJUAN KEBERADAAN KEBIJAKAN KEAMANAN

Secara prinsip paling tidak ada 2 (dua) peranan penting dari sebuah dokumen kebijakan keamanan, yaitu:

1. Untuk mendefinisikan dan memetakan secara detail aset-aset informasi apa saja yang harus dilindungi dan dikelola dengan baik keamanannya; dan
2. Untuk mereduksi atau mengurangi resiko yang dapat ditimbulkan karena:
   - Adanya penyalahgunaan sumber daya atau fasilitas perusahaan yang terkait dengan manajemen pengelolaan data dan informasi;
   - Adanya insiden yang menyebabkan hilangnya data penting, tersebarnya informasi rahasia, dan pelanggaran terhadap hak cipta (HAKI); dan
   - Adanya pelanggaran terhadap hak akses pengguna informasi tertentu sesuai dengan hak dan wewenangnya.

Oleh karena itulah maka perlu didefinisikan dan ditentukan serangkaian mekanisme atau protokol yang berfungsi sebagai panduan strategis dan operasional dalam hal semacam: (i) bagaiaman setiap karyawan harus dan dapat berinteraksi dengan sistem informasi; (ii) bagaimana setiap sistem informasi harus dikonfigurasi; (iii) apa yang harus dilakukan jika terjadi insiden keamanan; (iv) bagaimana cara mendeteksi adanya kerawanan keamanan sistem yang terjadi; dan lain sebagainya. Sementara tujuan dari adanya Kebijakan Keamanan adalah:

- Memproteksi dan melindungi sumber daya sistem dan teknologi informasi organisasi dari penyalahgunaan wewenang akses;
- Menangkis serangan atau dakwaan hukum dari pihak lain terkait dengan insiden keamanan; dan
- Memastikan integritas dan keutuhan data yang bebas dari perubahan dan modifikasi pihak-pihak tak berwenang.

13.4 MENYEBUTKAN KLASIFIKASI JENIS KEBIJAKAN KEAMANAN

Dilihat dari segi peruntukkan dan kontennya, dokumen kebijakan keamanan dapat dikategorisasikan menjadi beberapa jenis, yaitu:

1. *User Policy* – berisi berbagai kebijakan yang harus dipatuhi oleh seluruh pengguna komputer dan sistem informasi organisasi, terutama menyangkut masalah hak akses, proteksi keamanan, tanggung jawab pengelolaan aset teknologi, dan lain sebagainya;

2. *IT Policy* – diperuntukkan secara khusus bagi mereka yang bekerja di departemen atau divisi teknologi informasi untuk memastikan adanya dukungan penuh terhadap pelaksanaan tata kelola keamanan informasi, seperti: mekanisme back-up, tata cara konfigurasi teknologi, dukungan terhadap pengguna, manajemen help desk, penanganan insiden, dan lain sebagainya;
3. *General Policy* – membahas masalah-masalah umum yang menjadi tanggung jawab bersama seluruh pemangku kepentingan organisasi, misalnya dalam hal mengelola keamanan informasi pada saat terjadi: manajemen krisis, serangan penjahat cyber, bencana alam, kerusakan sistem, dan lain sebagainya; dan
4. *Partner Policy* – kebijakan yang secara khusus hanya diperuntukkan bagi level manajemen atau pimpinan puncak organisasi semata.

13.5 MENYUSUN PANDUAN RANCANGAN KONTEN DOKUMEN KEBIJAKAN KEAMANAN

Untuk setiap dokumen kebijakan keamanan yang disusun dan dikembangkan, terdapat sejumlah hal yang harus diperhatikan sebagai panduan, yaitu:

- Terdapat penjelasan detail mengenai deskripsi kebijakan yang dimaksud, terutama berkaitan dengan isu-isu keamanan informasi dalam organisasi;
- Adanya deskripsi mengenai status dokumen kebijakan yang disusun dan posisinya dalam tata peraturan organisasi dimaksud;
- Ruang lingkup pemberlakuan dokumen terkait dalam konteks struktur serta lingkungan organisasi yang dimaksud – terutama dalam hubungannya dengan unit serta fungsi struktur organisasi yang bersangkutan; dan
- Konsekuensi atau hukuman bagi mereka yang tidak taat atau melanggar kebijakan yang dimaksud.

Dipandang dari sisi konten, perlu disampaikan dalam dokumen kebijakan keamanan sejumlah aspek sebagai berikut:

- Pendahuluan mengenai alasan dibutuhkannya suatu kebijakan keamanan dalam konteks berorganisasi, terutama dalam kaitannya dengan definisi, ruang lingkup, batasan, obyektif, serta seluk beluk keamanan informasi yang dimaksud;
- Pengantar mengenai posisi keberadaan dokumen kebijakan yang disusun, serta struktur pembahasannya, yang telah fokus pada proses pengamanan aset-aset penting organisasi yang terkait dengan pengelolaan data serta informasi penting dan berharga;
- Definisi mengenai peranan, tugas dan tanggung jawab, fungsi, serta cara penggunaan kebijakan keamanan yang dideskripsikan dalam dokumen formal terkait; dan

- Mekanisme kendali dan alokasi sumber daya organisasi yang diarahkan pada proses institutionalisasi kebijakan keamanan yang dipaparkan dalam setiap pasal atau ayat dalam dokumen kebijakan ini.

13.6 MENYUSUN STRATEGI IMPLEMENTASI KEBIJAKAN KEAMANAN

Belajar dari pengalaman organisasi yang telah berhasil menerapkan dokumen kebijakan keamanan secara efektif, ada sejumlah prinsip yang harus dimengerti dan diterapkan secara sungguh-sungguh, yaitu:

1. Mekanisme pengenalan dan "enforcement" harus dilaksanakan dengan menggunakan pendekatan "top down", yang dimulai dari komitmen penuh pimpinan puncak yang turun langsung mensosialisasikannya kepada segenap komponen organisasi;
2. Bahasa yang dipergunakan dalam dokumen kebijakan keamanan tersebut haruslah yang mudah dimengerti, dipahami, dan dilaksanakan oleh setiap pemangku kepentingan;
3. Sosialisasi mengenai pemahaman cara melaksanakan setiap pasal dalam kebijakan kemanan haruslah dilaksanakan ke segenap jajaran manajemen organisasi;
4. Tersedianya "help desk" yang selalu bersedia membantu seandainya ada individu atau unit yang mengalami permasalahan dalam menjalankan kebijakan yang ada; dan
5. Secara konsisten diberikannya sanksi dan hukuman terhadap setiap pelanggaran kebijakan yang terjadi, baik yang sifatnya sengaja maupun tidak sengaja.

13.7 MEMBERIKAN CONTOH MODEL KEBIJAKAN KEAMANAN

Dipandang dari segi prinsip, paradigma, dan pendekatan dalam menyusun strategi keamanan, dokumen kebijakan yang disusun dapat dikategorikan menjadi sejumlah model, antara lain:

Primiscuous Policy

Merupakan kebijakan untuk tidak memberikan restriksi apa pun kepada para pengguna dalam memanfaatkan internet atau sistem informasi yang ada. Kebebasan yang mutlak ini biasanya sering diterapkan oleh organisasi semacam media atau pers, konsultan, firma hukum, dan lain sebagainya – yang menerapkan prinsip-prinsip kebebasan dalam berkarya dan berinovasi.

Permissive Policy

Pada intinya kebijakan ini juga memberikan keleluasaan kepada pengguna untuk memanfaatkan sistem informasi sebebas-bebasnya tanpa kendali, namun setelah dilakukan sejumlah aktivitas kontrol, seperti: (i) menutup lubang-lubang kerawanan dalam sistem dimaksud; (ii) menonaktifkan port atau antar muka input-output yang tidak dipergunakan; (iii) mengkonfigurasian server dan firewalls sedemikian rupa sehingga tidak dimungkinkan adanya akses dari eksternal organisasi ke dalam; dan lain sebagainya.

Prudent Policy

Kebalikan dengan dua model kebijakan sebelumnya, jenis ini organisasi benar-benar menggunakan prinsip kehati-haian dalam mengelola keamanan informasinya. Dalam lingkungan ini, hampir seluruh sumber daya informasi "dikunci" dan "diamankan". Untuk menggunakannya, setiap user harus melalui sejumlah aktivitas pengamanan terlebih dahulu. Prinsip ekstra hati-hati ini biasanya cocok untuk diterapkan pada organisasi semacam instalasi militer, bursa efek, perusahaan antariksa, dan lain sebagainya.

Paranoid Policy

Pada model ini, kebanyakan individu dalam organisasi yang tidak memiliki relevansi sama sekali dengan kebutuhan informasi benar-benar ditutup kemungkinannya untuk dapat mengakses internet maupun sistem informasi apa pun yang ada dalam lingkungan organisasi. Seperti selayaknya orang yang sedang "paranoid", organisasi benar-benar "tidak percaya" kepada siapapun, termasuk karyawannya sendiri, sehingga akses terhadap hampir semua sistem informasi benar-benar ditutup secara ketat.

Acceptable-Use Policy

Dalam lingkungan kebijakan ini, organisasi menentukan hal-hal apa saja yang boleh dilakukan maupun tidak boleh dilakukan oleh sejumlah pengguna dalam organisasi – terkait dengan akses dan hak modifikasi informasi tertentu. Hasil pemetaan inilah yang kan dipakai untuk memberikan tingkat atau level hak akses keamanannya.

User-Account Policy

Ini merupakan kebijakan yang paling banyak diterapkan di organisasi kebanyakan. Dalam konteks ini, setiap pengguna, sesuai dengan tupoksi dan tanggung jawabnya, ditetapkan hak aksesnya terhadap masing-masing jenis informasi yang ada di

organisasi. Dengan kata lain, wewenang akses yang dimiliki tersebut melekat pada struktur atau unit organisasi tempatnya bekerja dan beraktivitas.

Remote-Access Policy

Kebijakan ini erat kaitannya dengan manajemen hak akses terhadap sumber daya sistem informasi organisasi yang dapat dikendalikan dari jarak jauh (baca: remote). Hal ini menjadi tren tersendiri mengingat semakin banyaknya organisasi yang memperbolehkan karyawannya untuk bekerja dari rumah atau ranah publik lainnya sejauh yang bersangkutan memiliki akses ke internet. Karena sifatnya inilah maka perlu dibuat kebijakan khsus mengenai hak akses kendali jarak jauh.

Information-Protection Policy

Jika dalam kebijakan sebelumnya fokus lebih ditekankan pada hak akses pengguna terhadap sumber daya teknologi yang ada, dalam kebijakan ini fokus kendali atau perlindungan ada pada aset informasi itu sendiri. Dimulai dari definisi informasi apa saja yang dianggap bernilai tinggi dan perlu diprioritaskan untuk dijaga, hingga model pencegahan penguasaan orang lain yang tidak berhak dengan cara melakukan enkripsi, perlindungan penyimpanan, model akses, dan lain sebagainya.

Firewall-Management Policy

Sesuai dengan namanya, kebijakan ini erat kaitannya dengan prinsip dan mekanisme konfigurasi firewalls yang harus diterapkan dalam organisasi. Karena sifatnya yang holistik, biasanya kebijakan ini menyangkut mulai dari perencanaan, pengadaan, pengkonfigurasian, penginstalan, pemasangan, penerapan, hingga pada tahap pengawasan dan pemantauan kinerja.

Special-Access Policy

Disamping kebijakan yang bersifat umum, dapat pula diperkenalkan kebijakan yang secara khusus mengatur hal-hal yang diluar kebiasaan atau bersifat ad-hoc (maupun non-rutin). Misalnya adalah hak akses terhadap sumber daya teknologi yang diberikan kepada penegak hukum ketika terjadi proses atau insiden kejahatan kriminal; atau wewenang akses terhadap pihak eksternal yang sedang melakukan aktivitas audit teknologi informasi; atau hak khusus bagi pemilik perusahaan atau pemegang saham mayoritas yang ingin melihat kinerja organisasi atau perusahaan yang dimilikinya.

Network-Connection Policy

Seperti diketahui bersama, terdapat banyak sekali cara untuk dapat menghubungkan sebuah komputer atau notebook ke jejaring komputer maupun dunia maya (baca: internet), antara lain melalui: (i) hot spot secara langsung; (ii) wireless dengan perantara komputer lain sebagai host; (iii) modem; (iv) telepon genggam; (v) sambungan fisik teritorial; dan lain sebagainya. Agar aman, perlu dikembangkan sebuah kebijakan keamanan terkait dengan aturan dan mekanisme kebijakan menghubungkan diri ke dunia maya.

Business-Partner Policy

Sebagai pihak yang berada di luar lingkungan internal perusahaan, mitra bisnis perlu pula diberikan akses terhadap sejumlah informasi yang relevan untuknya. Dalam kaitan ini maka perlu dikembangkan kebijakan keamanan khusus yang mengatur hak dan tanggung jawab akses informasi dari mitra bisnis.

Other Policies

Setiap organisasi memiliki karakteristik, budaya, dan kebutuhannya masing-masing. Oleh karena itu, maka akan berkembang sejumlah kebijakan sesuai dengan kebutuhan yang ada. Beberapa di antaranya yang kerap dikembangkan oleh organisasi di negara berkembang seperti Indonesia adalah:

- Kebijakan mengenai manajemen pengelolaan kata kunci atau password;
- Kebijakan dalam membeli dan menginstalasi software baru;
- Kebijakan untuk menghubungkan diri ke dunia maya (baca: internet);
- Kebijakan terkait dengan penggunaan flash disk dalam lingkungan organisasi;
- Kebijakan yang mengatur tata cara mengirimkan dan menerima email atau berpartisipasi dalam mailing list; dan lain sebagainya.

-oo0oo-

~ 14 ~

PROSEDUR PENANGANAN INSIDEN KEAMANAN DUNIA SIBER

Capaian Pembelajaran (*Learning Outcomes*):

1. Menjelaskan Prinsip Penanganan Insiden
2. Menetapkan Kerangka Dasar Fungsi Penanganan Insiden
3. Menguraikan Siklus dan Prosedur Baku Penanganan Insiden
4. Menjelaskan Aktivitas Triage
5. Menjelaskan Aktivitas Handling
6. Menjelaskan Aktivitas Announcement
7. Menjelaskan Aktivitas Feedback

14.1 MENJELASKAN 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.

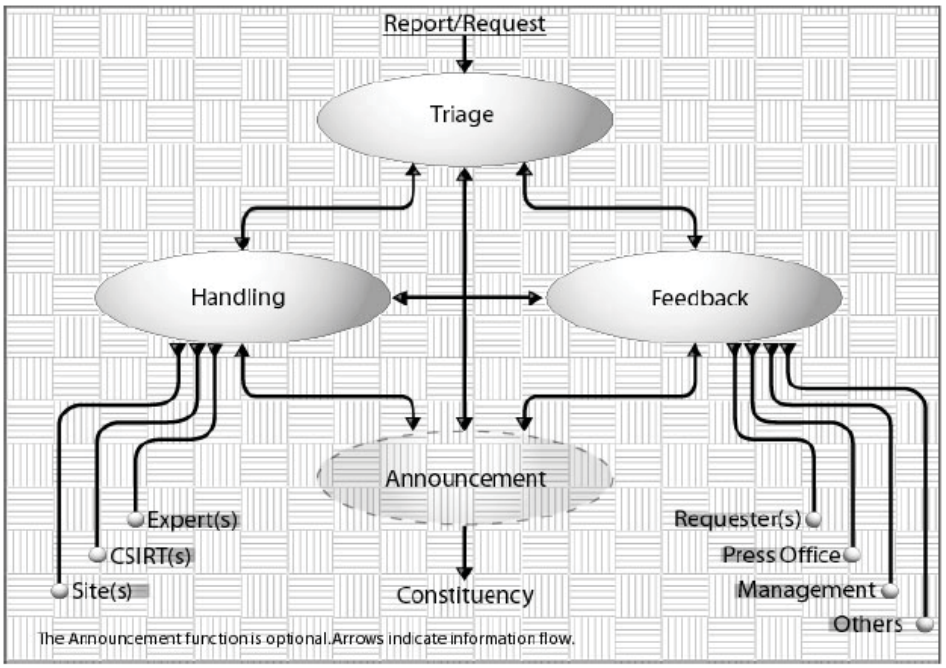
14.2 MENETAPKAN KERANGKA DASAR FUNGSI PENANGANAN INSIDEN

CERT/CC melalui publikasinya "Handbook for CSIRTs" menggambarkan kerangka fungsi penanganan insiden yang terdiri dari sejumlah entitas atau komponen seperti yang diperlihatkan dalam gambar 14.1.

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.



Gambar 14.1 *Fungsi Penanganan Insiden*

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

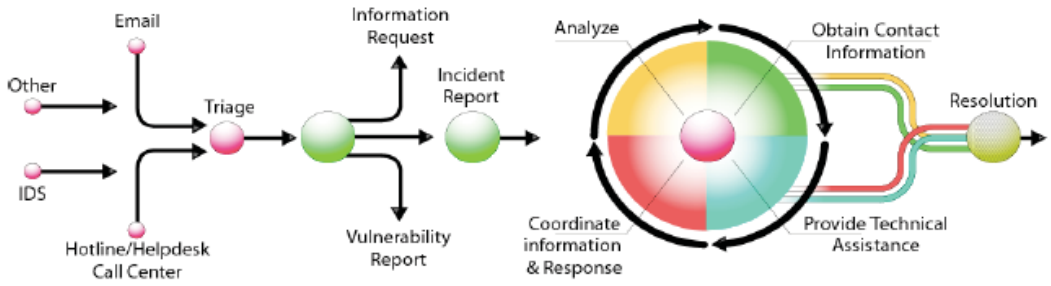
agar seluruh pihak yang berkepentingan dapat saling berpartisipasi dan berkoordinasi secara efektif sesuai dengan porsi tugas dan tanggung jawabnya masing-masing.

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.

14.3 MENGURAIKAN 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.



Gambar 14.2 *Siklus Penanganan Insiden*

Dalam gambar ini terlihat jelas tahap-tahap yang dimaksud, yaitu:

- 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.

14.4 MENJELASKAN 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.

14.5 MENJELASKAN 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.

14.6 MENJELASKAN 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.

14.7 MENJELASKAN 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.

-oo0oo-

~ 15 ~

PERANAN KRIPTOLOGI DALAM PENGAMANAN INFORMASI

Capaian Pembelajaran (*Learning Outcomes*):

1. Memahami Fenomena Perang Dunia Informasi
2. Menyebutkan Berbagai Kejahatan Dunia Maya
3. Menyebutkan Langkah-Langkah Pengamanan Informasi
4. Mengidentifikasi Permasalahan yang Dihadapi
5. Menerapkan Kriptologi dan Prinsip Keamanan Informasi
6. Menguraikan Budaya Penyandian dalam Masyarakat Indonesia
7. Menjelaskan Dampak dan Resiko Perang di Dunia Maya
8. Mendukung Gerakan Nasional Penerapan Kriptografi
9. Mengidentifikasi Kunci Sukses Gerakan Pengamanan

15.1 MEMAHAMI FENOMENA PERANG DUNIA INFORMASI

Sudah merupakan suatu kenyataan bahwa saat ini tengah terjadi "perang dunia" informasi antar negara dalam berbagai konteks kehidupan yang dipicu oleh fenomena globalisasi dunia. Lihatlah bagaimana lihainya para pemimpin dunia senantiasa melakukan penjagaan terhadap pencitraan dengan memanfaatkan media massa sebagai salah satu bentuk pertahanan politik yang ampuh. Atau fenomena pengembangan opini publik melalui media interaksi sosial di dunia maya seperti Facebook, Twitters, dan Friendster yang telah menunjukkan taring kejayaannya. Belum lagi terhitung sengitnya perang budaya melalui beragam rekaman multimedia yang diunggah dan dapat diunduh dengan mudah oleh siapa saja melalui situs semacam You Tube atau iTunes. Sebagaimana halnya pisau bermata dua, teknologi informasi dan komunikasi yang dipergunakan sebagai medium bertransaksi dan berinteraksi ini pun memiliki dua sisi karakteristik yang berbeda. Di satu pihak keberadaan teknologi ini mampu meningkatkan kualitas kehidupan manusia melalui aplikasi semacam e-government, e-business, e-commerce, e-society, dan e-education; sementara di sisi lainnya secara simultan teknologi memperlihatkan pula sisi negatifnya, seperti kejahatan ekonomi internet, pembunuhan karakter via dunia maya, penipuan melalui telepon genggam, penculikan anak dan remaja lewat situs jejaring sosial, penyadapan terselubung oleh pihak yang tidak berwenang, dan sejumlah hal mengemuka lainnya belakangan ini. Mau tidak mau, suka tidak suka, harus ada suatu usaha dari segenap masyarakat untuk melakukan sesuatu agar dampak teknologi yang positif dapat senantiasa diakselerasi penggunaannya, bersamaan dengan usaha untuk menekan sedapat mungkin pengaruh negatif yang berpotensi berkembang dan berdampak merugikan komunitas luas.

15.2 MENYEBUTKAN BERBAGAI KEJAHATAN DUNIA MAYA

Semenjak diperkenalkan dan berkembangnya teknologi internet di penghujung abad 21, statistik memperlihatkan pertumbuhan pengguna teknologi informasi dan komunikasi ini meningkat secara sangat pesat (baca: eksponensial). Pada saat ini diperkirakan 1 dari 5 penduduk dunia telah terhubung ke dunia maya melalui teknologi yang sangat digemari khususnya oleh para generasi muda dewasa ini. Selain sebagai sarana berkomunikasi dan berinteraksi antar berbagai individu maupun beragam kelompok komunitas, internet dipergunakan pula sebagai medium melakukan transaksi dan kolaborasi. Di industri perbankan dan keuangan misalnya, internet dipakai sebagai medium efektif dalam menjalankan transaksi perbankan seperti: transfer uang, lihat saldo, bayar listrik, beli saham, dan lain-lain. Contoh lain adalah di dunia pendidikan, dimana internet

dengan variasi teknologi informasi dan komunikasi lainnya dipakai untuk hal-hal semacam: pembelajaran jarak jauh, pencarian referensi belajar, pelaksanaan riset, penyelenggaraan tutorial, dan lain sebagainya. Demikian pula di sektor militer dan pertahanan keamanan, sudah sangat jamak pemanfaatan jejaring internet dan dunia maya untuk melakukan aktivitas seperti: pengiriman pesan rahasia, pemantauan dinamika masyarakat, pengendali peralatan dan fasilitas pertahanan keamanan, penerapan intelijen dan kontera intelijen, dan beragam kegiatan strategis lainnya. Dengan kata lain, pemanfaatan internet serta teknologi informasi dan komunikasi telah masuk ke seluruh aspek kehidupan masyarakat, tanpa terkecual - terutama pada sektor yang sangat vital bagi kelangsungan hidup bermasyarakat dan bernegara, seperti: telekomunikasi, transportasi, distribusi, keuangan, pendidikan, manufaktur, pemerintahan, dan kesehatan.

Seperti halnya pada dunia nyata, dalam dunia nyata pun terjadi berbagai jenis kejahatan yang dilakukan oleh para kriminal dengan beragam latar belakang dan obyektifnya. Statistik memperlihatkan bahwa sejalan dengan perkembangan pengguna internet, meningkat frekuensi terjadinya kejahatan, insiden, dan serangan di dunia maya. Lihatlah beraneka modus operandi yang saat ini tengah menjadi “primadona” sorotan masyarakat seperti:

penipuan berkedok penyelenggara atau pengelola institusi yang sah melalui SMS, email, chatting, dan website sehingga korban secara tidak sadar mengirimkan atau menyerahkan hak maupun informasi rahasia miliknya (seperti: password, nomor kartu kredit, tanggal lahir, nomor KTP, dan lain sebagainya) kepada pihak kriminal yang selanjutnya nanti dipergunakan untuk merampok harta miliknya via ATM, internet banking, e-comerce, dan lain-lain;

- penyerangan secara intensif dan bertubi-tubi pada fasilitas elektronik milik sebuah institusi - dengan menggunakan virus, botnet, trojan horse, dan program jahat lainnya - sehingga berakibat pada tidak berfungsinya peralatan terkait, dimana pada akhirnya nanti fungsi-fungsi vital seperti perbankan, pasar saham, radar penerbangan, lalu lintas transportas, atau instalasi militer menjadi tidak berfungsi atau pun malfungsi;
- perusakan atau pun perubahan terhadap data atau informasi dengan tujuan jahat seperti memfitnah, merusak citra individu atau institusi, membohongi pihak lain, menakut-nakuti, menyesatkan pengambil keputusan, merintangi transparansi, memutarbalikkan fakta, membentuk persepsi/opini keliru, memanipulasi kebenaran, dan lain sebagainya;
- penanaman program jahat (baca: malicious software) pada komputer-komputer milik korban dengan tujuan memata-matai, menyadap, mencuri data, merubah informasi, merusak piranti, memindai informasi rahasia, dan lain-lain; serta

- penyebaran faham-faham atau pengaruh jahat serta negatif lainnya ke khalayak, terutama yang berkaitan dengan isu pornografi, komunisme, eksploitasi anak, aliran sesat, pembajakan HAKI, terorisme, dan berbagai hal lainnya yang mengancam kedamaian hidup manusia.

15.3 MENYEBUTKAN LANGKAH-LANGKAH PENGAMANAN INFORMASI

Memperhatikan berbagai fenomena ancaman yang ada, reaksi beragam diperlihatkan oleh sejumlah pihak seperti pemerintah, swasta, akademisi, politisi, praktisi, komunitas swadaya, dan kelompok-kelompok masyarakat lainnya. Pada level nasional misalnya, hampir seluruh negara mendirikan apa yang dinamakan sebagai CERT (Computer Emergency Response Team) atau CSIRT (Computer Security Incident Response Team) - sebuah lembaga pengawas dan pengelola insiden berskala nasional jika terjadi serangan pada tingkat nasional. Bahkan di sejumlah negara maju seperti Amerika Serikat dan Jepang, dikembangkan institusi yang sangat berpengaruh dan memegang otoritas tinggi - yang disebut sebagai NSA (National Security Agency) atau NISC (National Information Security Council) - dengan tugas dan tanggung jawab utama menjaga keamanan informasi pada tataran kenegaraan dan lembaga vital negara yang berpengaruh terhadap kelangsungan hidup masyarakatnya. Di Indonesia institusi serupa bernama ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure).

Pada tataran swasta, proses pengamanan informasi dilakukan pada sektor hulu - yaitu industri telekomunikasi - terutama yang berperan sebagai penyedia jasa penyelenggara koneksi internet (baca: ISP=Internet Service Provider). Berbagai usaha dilakukan oleh perusahaan-perusahaan ini, mulai dari menginstalasi piranti keras seperti sensor, firewalls, Intrusion Prevention System (IPS), dan Intrusion Detection System (IDS), hingga membentuk divisi keamanan internet atau informasi dalam struktur organisasi ISP terkait (baca: internal CERT). Sementara itu tumbuh pula sejumlah perusahaan swasta yang bergerak di bidang jasa konsultasi, pelatihan, dan pendampingan di bidang keamanan informasi.

Sektor pendidikan pun nampak tidak mau kalah berperan. Terbukti dengan mulai ditawarkannya beraneka ragam program, pelatihan, penelitian, seminar, lokakarya, sertifikasi, serta pelayanan dengan kurikulum atau konten utama terkait dengan manajemen keamanan informasi dan internet. Secara serius terlihat bagaimana lembaga pendidikan yang dimotori perguruan tinggi ini berkolaborasi dengan perusahaan swasta berskala nasional, regional, dan internasional dalam menyemaikan kompetensi - terkait dengan ilmu penetration test, malware analysis,

ethical hacking, traffic monitoring, secured programming, security governance, dan lain sebagainya - pada peserta didik atau partisipan terkait.

Sementara itu secara giat berbagai praktisi maupun kelompok komunitas pun bertumbuhan di tanah air, dengan visi dan misi utama untuk mempromosikan dan meningkatkan kewaspadaan mengenai pentingnya keperdulian terhadap berinternet secara sehat dan aman. Penggiat komunitas ini berasal dari berbagai kalangan, seperti: praktisi teknologi informasi, lembaga swadaya masyarakat, organisasi politik, penggerak industri internet, pengusaha/vendor teknologi, dan lain sebaga

Terlepas dari berbagai bentuk, karakteristik, dan pendekatan aktivitas yang dilakukan, keseluruhan komponen organisasi tersebut di atas memiliki cita-cita dan obyektif yang sama, yaitu menyediakan lingkungan berinternet yang sehat dan aman.

15.4 MENGIDENTIFIKASI PERMASALAHAN YANG DIHADAPI

Terlepas dari begitu banyaknya usaha yang telah dilakukan secara kolektif tersebut, ada satu prinsip permasalahan keamanan informasi yang masih dihadapi dunia internet Indonesia. Kebanyakan aktivitas dan kegiatan yang dilakukan berbagai lembaga tersebut lebih fokus menggunakan pendekatan mengamankan infrastruktur jaringan internet dibandingkan dengan melakukan pengamanan terhadap data atau informasi yang mengalir pada infrastruktur jaringan tersebut. Kerawanan ini menimbulkan sejumlah potensi ancaman yang cukup serius sebagai berikut:

- kesulitan mengetahui tingkat integritas dan keaslian data yang diperoleh seandainya fasilitas pengaman jaringan gagal mendeteksi adanya modifikasi atau fabrikasi terhadap data yang dikirim (misalnya karena kualitas pengamanan yang buruk, anti virus yang tidak ter-update secara mutakhir, kecanggihan model penyerangan para kriminal, dan lain sebagainya);
- kemudahan pihak kriminal dalam mengerti data atau pesan yang dikirimkan setelah proses penyadapan, pengintaian, pengambilan, dan penduplikasian berhasil dilaksanakan terhadap informasi yang mengalir dalam sebuah jejaring internet yang aman maupun tidak aman (karena data atau pesan yang ada masih dalam bentuk asli tanpa dilakukan proses penyandian sama sekali);
- keleluasaan pihak kriminal dalam melakukan kegiatan kejahatannya seperti mencuri data dan informasi karena sebagian besar aset berharga tersebut masih tersimpan dalam bentuk plain file di dalam media penyimpanan semacam hard disk, CD ROM, flash disk, dan lain sebagainya;

- keterbukaan berbagai konten atau pesan komunikasi baik melalui media teknologi informasi maupun komunikasi seperti telepon genggam, Personal Digital Assistant, smart phone, communicator, blackberry, netbook, atau piranti gadget lainnya dalam bentuk SMS (Short Message Services), chatting, electronic mail, mailing list, newsgroup, dan lain-lain; serta
- kebiasaan individu atau masyarakat yang dengan mudahnya memberikan berbagai data dan informasi diri tanpa berpikir panjang terlebih dahulu karena kurang pahamnya mengenai potensi kejahatan yang dapat timbul di kemudian hari seperti yang ditunjukkan selama ini dalam berbagai konteksi seperti ketika berpartisipasi dalam jejaring sosial internet, bertransaksi jual beli melalui situs e-commerce, beraktivitas menjadi anggota mailing list, bermain game berbasis jaringan, dan lain sebagainya.

15.5 MENERAPKAN KRIPTOLOGI DAN PRINSIP KEAMANAN INFORMASI

Dipandang dari sudut keamanan informasi berbasis digital atau data elektronik, sebagaimana layaknya uang bersisi dua (baca: two sides of a coin), ada dua aspek yang secara simultan harus diperhatikan secara sungguh-sungguh, yaitu keamanan fisik dan keamanan informasi. Yang dimaksud dengan keamanan fisik adalah terkait segala sesuatu yang berkaitan dengan usaha untuk mengamankan data dan informasi melalui mekanisme dan prosedur yang berhubungan dengan sumber daya yang dapat dilihat secara kasat mata (baca: fisik). Misalnya adalah bagaimana melakukan tindakan pengamanan terhadap fasilitas fisik seperti: kamera pengaman (baca: CCTV atau kamera surveillance), sensor jaringan, pintu pengaman pada data center, perimeter lokasi akses, penguncian port, alarm pengaman, kartu akses identifikasi, dan lain sebagainya.

Sementara untuk mengamankan informasi, berbagai cara pun kerap dipergunakan seperti: manajemen password, aplikasi anti virus, sistem deteksi terjadinya intrusi, pemutakhiran patches, dan lain sebagainya. Dari berbagai cara yang ada, ada satu mekanisme atau pendekatan yang sangat efektif dan efisien untuk dapat diadopsi secara mudah, murah, dan masif - yaitu dengan memanfaatkan Kriptologi atau Ilmu Persandian - diambil dari bahasa Latin yang terdiri dari kata ‘kriptos’ (rahasia) dan ‘logos’ (ilmu). Dengan kata lain, kriptologi adalah ilmu atau seni yang mempelajari semua aspek tulisan rahasia.

Dalam tataran implementasinya, kriptologi dibagi menjadi dua, yaitu kriptografi dan kriptoanalisis. Kriptografi adalah cara, sistem, atau metode untuk mengkonstruksi pesan, berita, atau informasi sehingga menjadi tata tulisan yang berlainan dan tidak bermakna. Sementara kriptoanalisis adalah usaha untuk mendapatkan teks

bermakna atau teks terang dari suatu teks dandi yang tidak diketahui sistem serta kunci-kuncinya. Dengan kata lain, kriptologi dapat dianggap sebagai sebuah ilmu atau seni untuk menjaga kerahasiaan berita - melalui penerapan sejumlah teknik-teknik matematika yang berhubungan dengan aspek keamanan data dan/atau informasi. Dari kedua hal ini, keberadaan kriptografi sangatlah dibutuhkan dalam konteks menjaga keamanan informasi di tanah air tercinta ini.

Paling tidak ada empat tujuan mendasar dari diberlakukannya kriptografi ini yang sangat erat kaitannya dengan aspek keamanan informasi, yaitu:

- Kerahasiaan Data - memastikan bahwa data atau informasi yang ada hanya dapat diakses oleh pihaki yang memiliiki otoritas atau wewenang, dengan cara menggunakan kunci rahasia yang menjadi miliknya untuk membuka dan/atau mengupas informasi yang telah disandi;
- Integritas Data - meyakinkan bahwa data atau informasi tertentu adalah utuh dan asli alias tidak terjadi aktivitas manipulasi data pihak-pihak yang tidak berhak, baik dalam bentuk pengubahan, penyisipan, penambahan, pengurangan, penghapusan, maupun pensubtitusian;
- Autentifikasi - memastikan bahwa data atau informasi yang dihasilkan memang benar-benar berasal dari pihak yang sebenarnya memiliki kewenangan untuk menciptakan atau berinteraksi dengan data/informasi tersebut; dan
- Non Repudiasi - meyakinkan bahwa benar-benar telah terjadi proses ataupun mekanisme tertentu yang terkait dengan keberadaan data/informasi dari pihak-pihak yang berhubungan sehingga terhindar dari segala bentuk penyangkalan yang mungkin terjadi.

Teknik kriptografi atau lebih sederhananya dikenal sebagai proses penyandian ini dilakukan dengan menggunakan sejumlah algoritma matematik yang dapat memiliki kemampuan serta kekuatan untuk melakukan:

- konfusi atau pembingungan - merekonstruksi teks yang terang atau mudah dibaca menjadi suatu format yang membingungkan, dan tidak dapat dikembalikan ke bentuk aslinya tanpa menggunakan algoritma pembalik tertentu; dan
- difusi atau peleburan - melakukan mekanisme tertentu untuk menghilangkan satu atau sejumlah karakteristik dari sebuah teks yang terang atau mudah dibaca.

Sejumlah studi memperlihatkan bahwa di dunia nyata, kehandalan sebuah algoritma bukan terletak pada kerahasiaan algoritma itu sendiri, namun berada pada kuncinya. Secara prinsip algoritma yang dimaksud hanya melakukan dua proses transformasi, yaitu: enkripsi (proses transformasi mengubah teks terang atau plain text menjadi teks sandi atau cipher text) dan dekripsi (proses

transformasi sebaliknya, yaitu merubah teks sandi menjadi teks terang). Adapun kunci yang dimaksud biasa dikenal sebagai istilah sederhana 'password', yang dalam implementasinya dapat berupa serangkaian campuran antara huruf, angka, dan simbol - hingga yang berbentuk biometrik seperti sidik jari, retina mata, karakter suara, suhu tubuh, dan berbagai kombinasi lainnya. Berbagai algoritma yang telah dikenal secara luas adalah Data Encryption Standard (DES), Blowfish, Twofish, MARS, IDEA, 3DES, dan AES (untuk tipe altoritma sandi kunci-simetris); atau Rivert-Shamir-Adelman (RSA), Knapsack, dan Diffie-Heillman (untuk tipe algoritma sandi kunci-asimetris).

Di samping itu, untuk semakin meningkatkan tingkat keamanan informasi, diperkenalkan pula sebuah fungsi hash Kriptologi seperti tipe MD4, MD5, SHA-0, SHA-1, SHA-256, dan SHA-512.

15.6 MENGURAIKAN BUDAYA PENYANDIAN DALAM MASYARAKAT INDONESIA

Kenyataan memperlihatkan - setelah dilakukan berbagai penelitian dan pengamatan - bahwa keperdulian masyarakat Indonesia tentang pentingnya menjaga kerahasiaan informasi masih sangatlah rendah. Ada sejumlah hal yang melatarbelakangi masih rendahnya keperdulian yang dimaksud. Pertama adalah masalah sosial budaya. Indonesia dikenal sebagai bangsa yang ramah tamah, terutama dalam hal melayani orang-orang yang bertamu ke lokasi tempat tinggalnya - baik berasal dari dalam negeri maupun luar negeri. Disamping itu masyarakat Indonesia juga dikenal dengan kehidupan kolegialnya, dimana masing-masing individu memiliki hubungan kedekatan yang sangat kental - dengan fenomena utama saling bergantung, siap selalu memberikan bantuan, serta kerap merasa senasib sepenganggungan - dalam lingkungan komunitas berkeluarga, bertetangga, berorganisasi, berusaha, dan bermasyarakat. Demikian pula kecenderungan untuk memiliki banyak sahabat, tempat yang bersangkutan mencurahkan segenap permasalahan, isi hati, pendapat, ajakan, maupun ketidaksetujuan menunjukkan adanya budaya 'trust' atau kepercayaan yang tinggi pada orang lain. Hal inilah yang menyebabkan timbulnya kebiasaan untuk senang menyebarkan berita, membagi informasi, menyerahkan data, menitipkan pesan, serta perilaku terbuka lainnya tanpa adanya upaya filterisasi maupun penyandian - karena hal tersebut dianggap menyalahi prinsip keterbukaan dan keterpercayaan yang telah dibangun selama ini.

Kedua adalah masalah pendidikan. Tidak banyak orang yang mengerti dan memahami betapa pentingnya nilai dari sebuah aset yang bernama data atau informasi dewasa ini. Hanya segelintir masyarakat yang pernah membaca,

mendengar, melihat, membahas, dan mensinyalir adanya peristiwa buruk dalam kehidupan akibat dari berbagai permasalahan terkait dengan keterbukaan data dan informasi. Banyak yang lupa atau kurang paham, bahwa fenomena dis-informasi dan mis-informasi misalnya dapat mengakibatkan terjadinya kerusuhan, kekacauan, bahkan ke-arnakisan di kalangan masyarakat akar rumput. Prinsip 'perception is reality' merupakan kata kunci yang kerap dipergunakan oleh pihak yang tidak bertanggung jawab dalam mencoba mempengaruhi dan membentuk opini serta persepsi masyarakat melalui pengrusakan atau penyesatan informasi - dengan cara menyadap, merubah, merusak, mengganti, memodifikasi, mengkonstruksi ulang, bahkan menghilangkan hal-hal yang seharusnya sangat bernilai dan diperlukan oleh pihak-pihak tertentu dan masyarakat. Masalah pendidikan ini wajar adanya, karena memang selain Indonesia masih merupakan sebuah negara berkembang yang sedang berjuang keluar dari kemiskinan dan kebodohan, teknologi informasi dan komunikasi tumbuh berkembang sedemikian pesatnya, yang membutuhkan kemauan dan kemampuan dari masyarakat moderen untuk dapat mengerti dampak negatif yang mungkin ditimbulkan dan mencari cara mengatasinya. Begitu banyak masyarakat moderen yang terbuai dengan berbagai kemajuan dan perubahan dinamika dunia global yang terjadi, tanpa sempat memikirkan kemungkinan terjadinya dampak negatif di kemudian hari.

Ketiga adalah masalah teknis. Ada dua aspek yang berkaitan dengan hal ini. Pertama adalah kemampuan, dalam arti kata telah cukup banyak masyarakat golongan menengah yang tahu akan pentingnya menjaga kerahasiaan data melalui mekanisme kriptografi. Namun pada saat bersamaan, yang bersangkutan tidak tahu bagaimana cara melakukannya. Misalnya adalah pemakai setia email dan SMS, yang tidak tahu bagaimana melakukan aktivitas enkripsi maupun dekripsi walaupun komputer atau piranti telepon genggamnya menyediakan hal tersebut. Demikian pula halnya dengan pemakai blackberry, mailing list, Facebook, Twitters, Friendsters, dan lain sebagainya. Kedua adalah kemauan untuk melakukan hal tersebut, karena selain dipandang rumit, proses enkripsi dan dekripsi memerlukan aktivitas tambahan yang lumayan memakan waktu dan usaha. Sangat sulit dirasakan untuk menanamkan kesadaran, keperdulian, dan motivasi individu agar dengan kesadarannya menggunakan ilmu Kriptologi untuk mengamankan transaksi, komunikasi, dan interaksi mereka. Konsep 'tahu, mau, dan bisa' nampaknya harus senantiasa ditanamkan kepada setiap individu yang tidak ingin menjadi korban kejahatan.

Keempat adalah masalah hukum. Walaupun hingga kini telah ada seperangkat peraturan dan perundang-undangan yang secara langsung maupun tidak langsung mengatur hukuman bagi siapa saja yang melakukan kejahatan keamanan informasi

seperti UU Telekomunikasi dan UU Informasi dan Transaksi Elektronik misalnya, namun belum ada cukup aturan yang mengharuskan pihak-pihak tertentu untuk menjalankan aktivitas penyandian dalam berbagai aktivitas kegiatannya. Contohnya adalah aturan yang mengikat dan tegas terhadap perlunya dilakukan proses penyandian dalam berbagai tingkatan interaksi pada setiap institusi atau obyek vital kenegaraan, seperti: instalasi militer, pusat pertambangan, bandara udara, simpul transaksi keuangan, pembangkit listrik, dan lain sebagainya. Tidak adanya keharusan atau peraturan yang mengatur sering diartikan dengan tidak adanya urgensi untuk melakukan hal yang dimaksud.

Selain empat masalah besar yang mendominasi tersebut, masih banyak terdapat isu-isu lainnya yang kerap menghambat terbentuknya budaya kriptografi atau penyandian di tengah-tengah masyarakat Indonesia, seperti misalnya: masalah kebiasaan, masalah insentif, masalah kepercayaan, masalah kepasrahan, masalah perilaku, masalah kemalasan, masalah keengganan dan lain sebagainya. Secara tidak langsung hal ini memperlihatkan bahwa masyarakat Indonesia masih merupakan komunitas berbudaya 'risk taker' atau berani menghadapi resiko apa pun yang mungkin terjadi di masa mendatang akibat kecerobohan dalam mengamankan informasi.

15.7 MENJELASKAN DAMPAK DAN RESIKO PERANG DI DUNIA MAYA

Banyak orang tidak tahu bahwa sebenarnya saat ini 'perang besar' di dunia maya tengah terjadi akibat globalisasi dan perkembangan teknologi informasi dan komunikasi. Selama tahun 2009 contohnya, ID-SIRTII mencatat bahwa setiap harinya, paling tidak terdapat rata-rata satu setengah juta percobaan serangan yang diarahkan untuk melumpuhkan internet Indonesia dengan berbagai modus kejahatan yang dilakukan baik dari luar negeri maupun dari dalam negeri sendiri. Jenis kajahatan yang dilakukan pun sangatlah beragam, yang secara kategori dapat dibagi menjadi empat jenis:

- Intersepsi - yang merupakan usaha untuk melakukan penyadapan terhadap sejumlah pesan, berita, data, atau informasi yang mengalir di dalam pipa transmisi internet Indonesia oleh pihak yang tidak berwenang dengan jenis serangan semacam sniffing dan eavesdropping;
- Interupsi - yang merupakan usaha untuk mengganggu hubungan komunikasi antar sejumlah pihak melalui berbagai cara seperti serangan bertipe DOS (Denial Of Services), DDOS (Distributed Denial Of Services), botnet, package flooding, dan lain sebagainya;

- Modifikasi - yang merupakan usaha melakukan perubahan terhadap pesan, berita, data, atau informasi yang mengalir pada pipa transmisi untuk memfitnah, mengelabui, membohongi, atau menyebarkan hal-hal yang tidak baik melalui mekanisme serangan semacam web defacement, SQL injection, cross scripting, dan beragam variasi lainnya; serta
- Fabrikasi - yang merupakan usaha untuk mengelabui pihak lain melalui beragam proses penyamaran terselubung dengan seolah-olah menjadi pihak yang memiliki wewenang atau hak akses yang sah, misalnya dengan menggunakan pendekatan serangan seperti phishing atau spoofing.

Seperti halnya perang di dunia fisik, perang di dunia maya telah banyak menelan korban dengan angka kerugian yang besarnya berkali-kali lipat dibandingkan dengan perang konvensional. Namun anehnya, karena kebanyakan sifatnya yang intangible, banyak masyarakat Indonesia yang tidak merasa telah kehilangan sesuatu atau merasa telah mengalami kerugian yang berarti. Cobalah lihat sejumlah peristiwa yang mungkin akan atau telah terjadi selama ini, seperti:

- Berapa banyak aset dokumen berharga berisi resep, formula, rahasia dagang, karya cipta, temuan, rancangan teknis, maupun paten produk yang telah jatuh ke tangan pihak asing karena dicuri melalui internet atau mekanisme lain di dunia maya;
- Seberapa banyak informasi rahasia seperti password, nomor kartu kredit, nama ibu kandung, nomor rekening, data kesehatan, profil pribadi, dan lain-lain yang telah bocor dan dikoleksi oleh para kriminal untuk selanjutnya diperjual-belikan di pasar hitam 'underground economy';
- Berapa banyak percakapan rahasia, dokumen penting, interaksi tertutup, maupun kegiatan intelijen yang berhasil diketahui dengan mudah oleh pihak yang tidak berwenang karena kemahiran mereka dalam menembus pertahanan jaringan pengaman sistem tempat disimpannya data penting atau terjadinya interaksi yang bersifat rahasia; dan
- Seberapa banyak aset tangible yang akhirnya harus direlakan untuk menjadi milik asing atau negara lain akibat sering kalahnya Indonesia dalam menghadapi perang citra di dunia maya karena banyaknya pihak-pihak yang melakukan aktivitas semacam kontra intelijen, mata-mata, negative marketing, public relations, dan black campaign.

Kalau hal ini terus dibiarkan terjadi, dimana aset yang paling berharga di era globalisasi ini - yaitu informasi dan pengetahuan - dibiarkan menjadi sebuah entitas yang 'telanjang' dan 'terang benderang' karena tidak dibalut dengan keamanan informasi melalui teknik persandian - maka perlahan namun pasti, tidak mustahil Indonesia akan menjadi layaknya kapal raksasa Titanic yang perlahan tenggelam.

15.8 MENDUKUNG GERAKAN NASIONAL PENERAPAN KRIPTOGRAFI

Mempelajari semua hal di atas, tidak ada jalan lain bagi bangsa Indonesia untuk dapat tetap bertahan di tengah persaingan global yang serba terbuka ini untuk segera melindungi dirinya dari berbagai serangan yang terjadi setiap hari di dunia maya. Harus ada sebuah usaha yang sistematik, berskala nasional dan bersifat masif, untuk menyadarkan seluruh masyarakat akan pentingnya menjaga keamanan informasi melalui penerapan kriptografi. Lembaga Sandi Negara sebagai sebuah institusi yang memiliki kewenangan, kekuatan, kompetensi, keahlian, dan kepiawaian di bidang kriptologi haruslah dapat menjadi lokomotif terdepan dalam memimpin gerakan ini. Prinsip dalam dunia keamanan informasi yang mengatakan bahwa 'your security is my security' memberikan arti bahwa gerakan sosialisasi keperdulian dan penyadaran akan pentingnya menerapkan kriptografi tersebut harus menyentuh seluruh lapisan hidup masyarakat, tanpa mengenal usia, latar belakang, status ekonomi, faksi politik, dan perbedaan-perbedaan lainnya. Gerakan tersebut harus mengakar dalam setiap kehidupan masyarakat moderen, dimana kelak akan menjadi sebuah budaya yang menyatu dengan kebiasaan, perilaku, serta tindakan individu-individu di tanah air.

Agar efektif, maka gerakan yang dimaksud harus dilakukan secara simultan dengan menggunakan pendekatan top-down dan bottom-up sebagai berikut:

- Pendekatan Top Down - berupa usaha pemerintah dan negara dalam mensosialisasikan secara tiada henti, konsisten, persistence, dan berkesinambungan terhadap pentingnya setiap individu dan komponen kehidupan masyarakat dalam melakukan pengamanan terhadap aset data maupun informasi yang dimiikinya - misalnya adalah dengan melakukan teknik kriptografi. Khusus untuk institusi atau organisasi yang bertanggung jawab terhadap kelangsungan operasional obyek-obyek vital negara - yang secara langsung menyangkut hajat hidup orang banyak - perlu diberlakukan peraturan yang ketat berisi keharusan dalam menerapkan kriptografi dalam aktivitas kegiatannya sehari-hari. Mekanisme 'reward and punishment' perlu secara tegas dikembangkan dan diterapkan dalam konteks ini; yang tentu saja berjalan dengan proses penegakan hukum yang adil dan berwibawa.
- Pendekatan Bottom Up - merupakan akumulasi dari kegiatan kolektif komunitas basis akar rumput, akademisi, industri swasta, maupun organisasi non profit lainnya dalam membangun kesadaran akan pentingnya menjaga kemanan informasi sesuai dengan konteks dan peranannya masing-masing. Melalui program edukatif semacam seminar, lokakarya, workshop, pelatihan, diskusi, dan tanya jawab hingga yang bersifat komersil seperti proyek pengembangan

sistem pengamanan, konsultasi standar keamanan informasi, jual beli alat-alat produk keamanan, riset dan pengembangan algoritma kriptografi, pengalihdayaan (baca: outsourcing) jasa keamanan informasi, dan lain sebagainya - masyarakat berperan secara aktif membentuk lingkungan yang kondusif dalam mengembangkan budaya dan ekosistem keamanan informasi.

Dengan bertemunya kedua sisi 'demand' dan 'supply' di atas - yaitu antar kebutuhan yang diciptakan melalui pendekatan 'top down' dan ketersediaan yang dipicu melalui penekatan 'bottom up' - maka nischaya akan terbentuk dan terbangun ekosistem keamanan informasi dan internet yang tangguh di tanah air tercinta ini.

15.9 MENGIDENTIFIKASI KUNCI SUKSES GERAKAN PENGAMANAN

Pada akhirnya, hakekat dari keamanan informasi itu melekat pada diri masing-masing individu. Topologi atau postur internet yang menghubungkan beribu-ribu bahkan berjuta-juta titik koneksi secara eksplisit memperlihatkan bahwa 'the stength of a chain depends on the weakest link' atau dalam bahasa Indonesianya 'kekuatan sebuah rantai terletak pada mata sambungan yang paling lemah'. Artinya adalaah bahwa tidak ada gunanya jika hanya sebagian kecil masyarakat saja yang paham dan perduli akan keamanan informasi, sementara masih banyak pihak lain yang tidak mau tahu mengenai pentingnya usaha bersama untuk mengamankan diri.

Perlu diingat, bahwa tidak ada negara di dunia ini yang meluangkan waktunya atau mengalokasikan sumber dayanya untuk melindungi keamanan informasi dari negara lain. Keamanan ekosistem internet Indonesia sepenuhnya terletak pada masyarakat Indonesia itu sendiri - yang pada akhirnya ditentukan oleh 'budaya aman' dari setiap insan atau individu manusia nusantara yang tersebar dari Sabang sampai Merauke, tanpa kecuali.

-oo0oo-

~ 16 ~

TEKNIK ANALISA MALWARE

Capaian Pembelajaran (*Learning Outcomes*):

1. Menjelaskan Arti dari Malware
2. Mengkaji Beragam Model Analisa
3. Menjelaskan Model Kajian Surface Analysis
4. Menjelaskan Model Kajian Runtime Analysis
5. Menjelaskan Model Kajian Static Analysis
6. Membahas Hasil Analisa Malware

16.1 MENJELASKAN ARTI DARI MALWARE

Modus operandi kejahatan di dunia siber sangatlah beragam dan bervariasi. Teknik yang dipergunakan oleh para kriminal pun semakin lama semakin mutakhir dan kompleks. Berdasarkan kejadian-kejadian terdahulu, hampir seluruh serangan melibatkan apa yang disebut sebagai "malicious software" atau "malware" – yang dalam terjemahan bebasnya adalah program jahat (karena sifatnya yang merusak atau bertujuan negatif).

Analisa malware adalah suatu aktivitas yang kerap dilakukan oleh sejumlah praktisi keamanan teknologi informasi untuk mendeteksi ada atau tidaknya komponen sub-program atau data yang bertujuan jahat dalam sebuah file elektronik. Analisa atau kajian ini sangat penting untuk dilakukan karena:

- Malware sering diselundupkan melalui file-file umum dan popular seperti aplikasi (.exe), pengolah kata (.doc), pengolah angka (.xls), gambar (.jpg), dan lain sebagainya – sehingga jika pengguna awam mengakses dan membukanya, akan langsung mejadi korban program jahat seketika;
- Malware sering diselipkan di dalam kumpulan file yang dibutuhkan untuk menginstalasi sebuah program atau aplikasi tertentu – sehingga jika sang pengguna melakukan instalasi terhadap aplikasi dimaksud, seketika itu juga malware diaktifkan;
- Malware sering disamarkan dengan menggunakan nama file yang umum dipakai dalam berbagai keperluan, seperti driver (.drv), data (.dat), library (.lib), temporary (.tmp), dan lain-lain – sehingga pengguna tidak sadar akan kehadirannya di dalam komputer yang bersangkutan;
- Malware sering dikembangkan agar dapat menularkan dirinya ke tempat-tempat lain, dengan cara kerja seperti virus atau worms – sehingga komputer pengguna dapat menjadi sarang atau sumber program jahat yang berbahaya;
- Malware sering ditanam di dalam sistem komputer tanpa diketahui oleh sang pengguna – sehingga sewaktu-waktu dapat disalahgunakan oleh pihak yang tidak berwenang untuk melakukan berbagai tindakan kejahatan; dan lain sebagainya.

16.2 MENGKAJI BERAGAM MODEL ANALISA

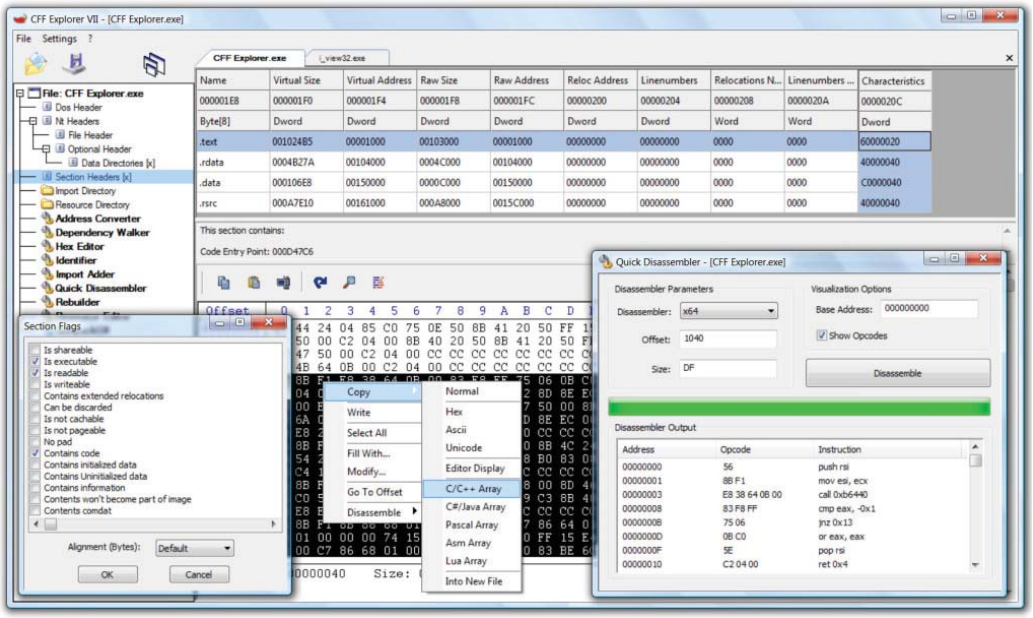
Pada dasarnya malware adalah sebuah program, yang disusun berdasarkan tujuan tertentu dengan menggunakan logika dan algoritma yang relevan dengannya. Oleh karena itulah maka model analisa yang biasa dipergunakan untuk mengkaji malware sangat erat kaitannya dengan ilmu dasar komputer, yaitu: bahasa pemrograman, algoritma, struktur data, dan rekayasa piranti lunak.

Secara umum, ada 3 (tiga) jenis analisa terhadap sebuah program untuk mendeteksi apakah yang bersangkutan merupakan malware atau bukan. Ketiga pendekatan dimaksud akan dijelaskan dalam masing-masing paparan sebagai berikut.

16.3 MENJELASKAN MODEL KAJIAN SURFACE ANALYSIS

Sesuai dengan namanya, "surface analysis" adalah suatu kajian pendeteksian malware dengan mengamati sekilas ciri-ciri khas sebuah file program tanpa harus mengeksekusinya. Untuk melihat ciri khas tersebut dapat dilakukan dengan menggunakan bantuan software atau perangkat aplikasi pendudukung. Analisa ini memiliki ciri-ciri sebagai berikut:

- Program yang dikaji tidak akan dijalankan, hanya akan dilihat "bagian luarnya" saja (sebagai analogi selayaknya orang yang ingin membeli buah-buahan, untuk mengetahui apakah buah yang bersangkutan masih mentah atau sudah busuk cukup dengan melihat permukaan kulitnya, membauinya, dan meraba-raba tekstur atau struktur kulitnya). Dari sini akan dicoba ditemukan hal-hal yang patut untuk dicurigai karena berbeda dengan ciri khas program kebanyakan yang serupa dengannya; dan
- Sang pengkaji tidak mencoba untuk mempelajari "source code" program yang bersangkutan untuk mempelajari algoritma maupun struktur datanya (sebagaimana layaknya melihat sebuah kotak hitam atau "black box".



Gambar 16.1 *CFF Explorer*

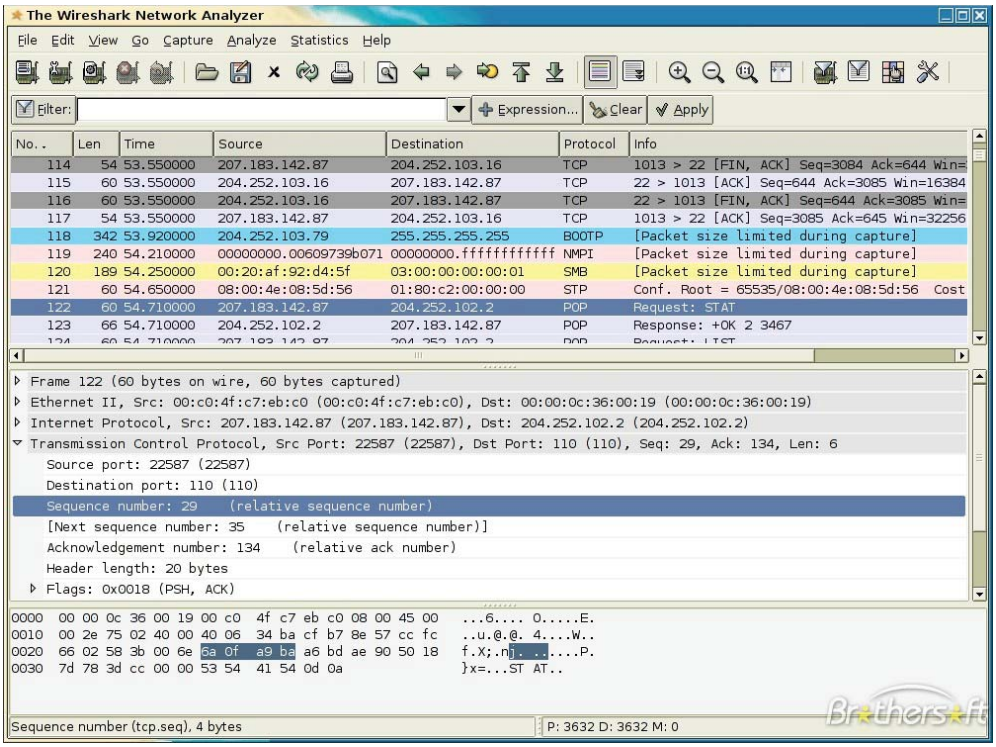
Saat ini cukup banyak aplikasi yang bebas diunduh untuk membantu melakukan kegiatan surface analysis ini, karena cukup banyak prosedur kajian yang perlu

dilakukan, seperti misalnya: HashTab dan digest.exe (Hash Analysis), TrID (File Analysis), BinText dan strings.exe (String Analysis), HxD (Binary Editor), CFF Explorer (Pack Analysis), dan 7zip (Archiver).

16.4 MENJELASKAN MODEL KAJIAN RUNTIME ANALYSIS

Pada dasarnya ada kesamaan antara runtime analysis dengan surface analysis, yaitu keduanya sama-sama berada dalam ranah mempelajari ciri-ciri khas yang selayaknya ada pada sebuah program yang normal. Bedanya adalah bahwa dalam runtime analysis, dipersiapkan sebuah prosedur dan lingkungan untuk mengeksekusi atau menjalankan program yang dicurigai mengandung atau sebagai malware tersebut.

Model analisa ini menghasilkan kajian yang lebih mendalam karena selain dihilangkannya proses "menduga-duga", dengan mengeksekusi malware dimaksud akan dapat dilihat "perilaku" dari program dalam menjalankan "skenario jahatnya" sehingga selanjutnya dapat dilakukan analisa dampak terhadap sistem yang ada.



Gambar 16.2 *Wireshark*

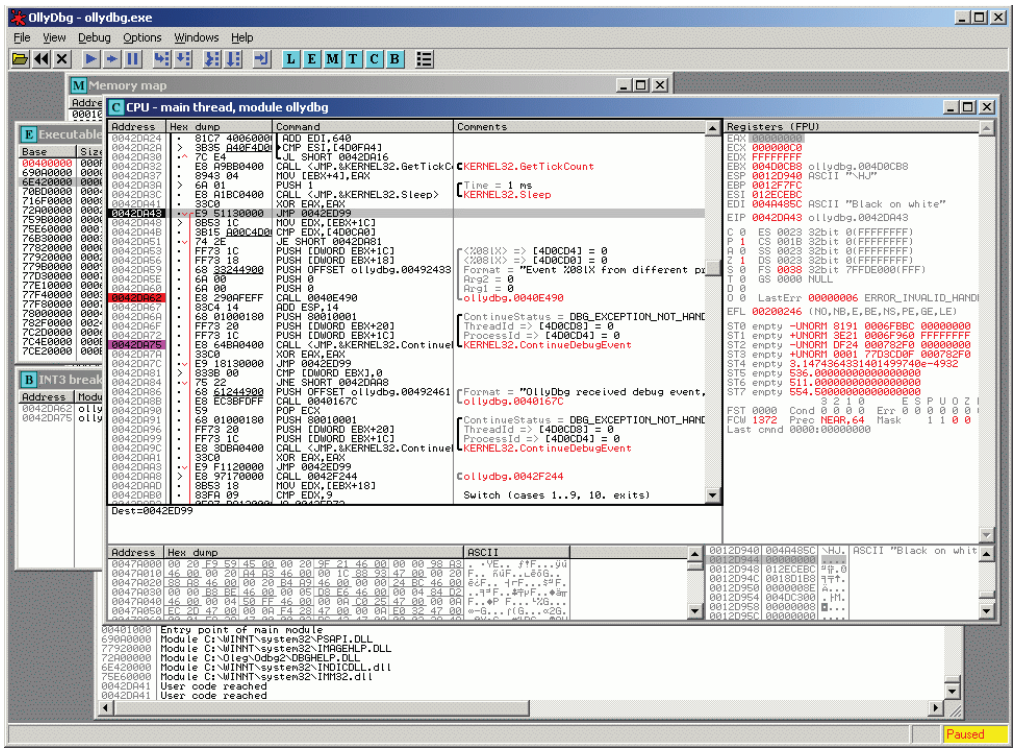
Oleh karena itulah maka aplikasi pendukung yang dipergunakan harus dapat membantu mensimulasikan kondisi yang diinginkan, yaitu melihat ciri khas dan karakteristik sistem, sebelum dan sesudah sebuah malware dieksekusi. Agar aman, maka program utama yang perlu dimiliki adalah software untuk

menjalankan virtual machine, seperti misalnya: VMWare, VirtualBoz, VirtualPC, dan lain sebagainya. Sementara itu aplikasi pendukung lainnya yang kerap dipergunakan dalam melakukan kajian ini adalah: Process Explorer, Regshot, Wireshark, TCPView, Process Monitor, FUNdelete, Autoruns, Streams/ADSSpy, dan lain-lain. Keseluruhan aplikasi tersebut biasanya dijalankan di sisi klien; sementara di sisi server-nya diperlukan FakeDNS, netcat/ncat, tcpdump/tshark, dan lain sebagainya.

16.5 MENJELASKAN MODEL KAJIAN STATIC ANALYSIS

Dari ketiga metode yang ada, static analysis merupakan model kajian yang paling sulit dilakukan karena sifat analisanya yang “white box” alias pengkajian melibatkan proses melihat dan mempelajari isi serta algoritma program malware dimaksud, sambil mengamati sekaligus menjalankan/mengeksekusinya.

Karena sifat dan ruang lingkupnya yang cukup luas dan mendalam, strategi khusus perlu dipersiapkan untuk melakukan kajian ini. Disamping itu, kajian ini juga memerlukan sumber daya yang khusus – misalnya adalah SDM yang memiliki pengetahuan dan pengalaman dalam membuat serta membaca program berbahasa mesin atau rakitan (assembly language) serta ahli arsitektur dan organisasi piranti komputasi seperti komputer, PDA, tablet, mobile phone, dan lain sebagainya.



Gambar 16.3 *OllyDbg*

Cukup banyak aplikasi pendukung yang diperlukan, tergantung dari kompleksitas malware yang ada. Contohnya adalah: IDA Pro (Disassembler); Hex-Rays, .NET Reflector, and VB Decompiler (Decompiler); MSDN Library, Google (Library); OllyDbg, Immunity Debugger, WinDbg/Syser (Debugger); HxD, WinHex, 010editor (Hex Editor); Python, Lunux Shell/Cygwin/MSYS (Others); dan lain-lain.

16.6 MEMBAHAS HASIL ANALISA MALWARE

Terlepas dari berbagai metode yang dipergunakan, apa sebenarnya hasil dari analisa yang dilakukan? Secara umum berdasarkan kajian yang dilakukan terhadap sebuah program yang dicurigai sebagai atau mengandung malware akan diambil kesimpulan:

1. Benar tidaknya program dimaksud merupakan malware atau mengandung unsur malware;
2. Jika benar, maka akan disampaikan jenis atau tipe malware dimaksud dan cara kerjanya;
3. Dampak yang terjadi akibat adanya malware tersebut dalam sebuah sistem;
4. Kiat cara mengurangi dampak negatif seandainya malware tersebut telah terlanjur dieksekusi dalam sebuah sistem atau cara mengeluarkan malware tersebut dalam sebuah sistem untuk mencegah terjadinya efek negatif;
5. Rekomendasi mengenai apa yang harus dilakukan untuk menghindari masuknya malware tersebut di kemudian hari, atau paling tidak cara-cara melakukan deteksi dini terhadap keberadaannya; dan
6. Menyusun panduan atau prosedur dalam menghadapi hal serupa di kemudian hari sebagai referensi (lesson learnt).

-oo0oo-

~ 17 ~

TEKNIK FORENSIK KOMPUTER

Capaian Pembelajaran (Learning Outcomes):

1. Menceritakan Latar Belakang Kebutuhan Forensik Komputer
2. Mendifinisikan Istilah Forensik Komputer
3. Menetapkan Tujuan dan Fokus Forensik Komputer
4. Menjelaskan Manfaat dan Tantangan Forensik Komputer
5. Menguraikan Berbagai Kejahatan Komputer
6. Menetapkan Obyek Forensik
7. Menerapkan Tahapan Aktivitas Forensik
8. Mendefinisikan Kebutuhan Sumber Daya

17.1 MENCERITAKAN LATAR BELAKANG KEBUTUHAN FORENSIK KOMPUTER

Bayangkanlah sejumlah contoh kasus yang dapat saja terjadi seperti dipaparkan berikut ini:

- Seorang Direktur perusahaan multi-nasional dituduh melakukan pelecehan seksual terhadap sekretarisnya melalui kata-kata yang disampaikannya melalui e-mail. Jika memang terbukti demikian, maka terdapat ancaman pidana dan perdata yang membayanginya.
- Sebuah kementrian di pemerintahan menuntut satu Lembaga Swadaya Masyarakat yang ditengarai melakukan penetrasi ke dalam sistem komputernya tanpa ijin. Berdasarkan undang-undang yang berlaku, terhadap LSM yang bersangkutan dapat dikenakan sanksi hukum yang sangat berat jika terbukti melakukan aktivits yang dituduhkan.
- Sekelompok artis pemain band terkemuka merasa berang karena pada suatu masa situsnya diporakporandakan oleh perentas (baca: hacker) sehingga terganggu citranya. Disinyalir pihak yang melakukan kegiatan negatif tersebut adalah pesaing atau kompetitornya.
- Sejumlah situs e-commerce mendadak tidak dapat melakukan transaksi pembayaran karena adanya pihak yang melakukan gangguan dengan cara mengirimkan virus tertentu sehingga pemilik perdagangan di internet tersebut rugi milyaran rupiah karena tidak terjadinya transaksi selama kurang lebih seminggu. Yang bersangkutan siap untuk menyelidiki dan menuntut mereka yang sengaja melakukan kegiatan ini.

Mereka yang merasa dirugikan seperti yang dicontohkan pada keempat kasus di atas, paling tidak harus melakukan 3 (tiga) hal utama:

1. Mencari bukti-bukti yang cukup agar dapat ditangani oleh pihak berwenang untuk memulai proses penyelidikan dan penyidikan, misalnya polisi di unit cyber crime;
2. Memastikan bahwa bukti-bukti tersebut benar-benar berkualitas untuk dapat dijadikan alat bukti di pengadilan yang sah sesuai dengan hukum dan perundang-undangan yang berlaku; dan
3. Mempresentasikan dan/atau memperlihatkan keabsahan alat bukti terkait dengan terjadinya kasus di atas di muka hakim, pengacara, dan tim pembela tersangka.

Oleh karena itulah maka dalam ilmu kriminal dikenal istilah forensik, untuk membantu pengungkapan suatu kejahatan melalui pengungkapan bukti-bukti yang sah menurut undang-undang dan peraturan yang berlaku. Sesuai dengan

kemajuan jaman, berbagai tindakan kejahatan dan kriminal moderen dewasa ini melibatkan secara langsung maupun tidak langsung teknologi informasi dan komunikasi. Pemanfaatan komputer, telepon genggam, email, internet, website, dan lain-lain secara luas dan masif telah mengundang berbagai pihak jahat untuk melakukan kejahatan berbasis teknologi elektronik dan digital. Oleh karena itulah maka belakangan ini dikenal adanya ilmu "computer forensics" atau forensik komputer, yang kerap dibutuhkan dan digunakan para penegak hukum dalam usahanya untuk mengungkapkan peristiwa kejahatan melalui pengungkapan bukti-bukti berbasis entitas atau piranti digital dan elektronik.

17.2 MENDIFINISIKAN ISTILAH FORENSIK KOMPUTER

Menurut Dr. HB Wolfre, definisi dari forensik komputer adalah sebagai berikut:

> *"A methodological series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format."*

Sementara senada dengannya, beberapa definisi dikembangkan pula oleh berbagai lembaga dunia seperti:

- *The preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found; atau*
- *The science of capturing, processing, and investigating data from computers using a methodology whereby any evidence discovered is acceptable in a Court of Law.*

Dimana pada intinya forensik komputer adalah "suatu rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mengumpulkan bukti-bukti berbasis entitas maupun piranti digital agar dapat dipergunakan secara sah sebagai alat bukti di pengadilan."

17.3 MENETAPKAN TUJUAN DAN FOKUS FORENSIK KOMPUTER

Selaras dengan definisinya, secara prinsip ada tujuan utama dari aktivitas forensik komputer, yaitu:

1. Untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat buti yang sah di pengadilan; dan

2. Untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivitasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud.

Adapun aktivitas forensik komputer biasanya dilakukan dalam dua konteks utama. Pertama adalah konteks terkait dengan pengumpulan dan penyimpanan data berisi seluruh rekaman detail mengenai aktivitas rutin yang dilaksanakan oleh organisasi atau perusahaan tertentu yang melibatkan teknologi informasi dan komunikasi. Dan kedua adalah pengumpulan data yang ditujukan khusus dalam konteks adanya suatu tindakan kejahatan berbasis teknologi.

Sementara itu fokus data yang dikumpulkan dapat dikategorikan menjadi 3 (tiga) domain utama, yaitu: (i) Active Data – yaitu informasi terbuka yang dapat dilihat oleh siapa saja, terutama data, program, maupun file yang dikendalikan oleh sistem operasi; (ii) Archival Data – yaitu informasi yang telah menjadi arsip sehingga telah disimpan sebagai backup dalam berbagai bentuk alat penyimpan seperti hardisk eksternal, CD ROM, backup tape, DVD, dan lain-lain; dan (iii) Latent Data – yaitu informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (corrupted file), dan lain sebagainya.

17.4 MENJELASKAN MANFAAT DAN TANTANGAN FORENSIK KOMPUTER

Memiliki kemampuan dalam melakukan forensik komputer akan mendatangkan sejumlah manfaat, antara lain:

- Organisasi atau perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yang dibutuhkan;
- Seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut, dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir;
- Para kriminal atau pelaku kejahatan akan berpikir dua kali sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik komputer; dan
- Membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya.

Terlepas dari manfaat tersebut, teramat banyak tantangan dalam dunia forensik komputer, terutama terkait dengan sejumlah aspek sebagai berikut:

- Forensik komputer merupakan ilmu yang relatif baru, sehingga "Body of Knowledge"-nya masih sedemikian terbatas (dalam proses pencarian dengan metode "learning by doing");
- Walaupun berada dalam rumpun ilmu forensik, namun secara prinsip memiliki sejumlah karakteristik yang sangat berbeda dengan bidang ilmu forensik lainnya – sehingga sumber ilmu dari individu maupun pusat studi sangatlah sedikit;
- Perkembangan teknologi yang sedemikian cepat, yang ditandai dengan diperkenalkannya produk-produk baru dimana secara langsung berdampak pada berkembangnya ilmu forensik komputer tesebut secara pesat, yang membutuhkan kompetensi pengetahuan dan keterampilan sejalan dengannya;
- Semakin pintar dan trampilnya para pelaku kejahatan teknologi informasi dan komunikasi yang ditandai dengan makin beragamnya dan kompleksnya jenis-jenis serangan serta kejahatan teknologi yang berkembang;
- Cukup mahalnya harga peralatan canggih dan termutakhir untuk membantu proses forensik komputer beserta laboratorium dan SDM pendukungnya;
- Secara empiris, masih banyak bersifat studi kasus (happening arts) dibandingkan dengan metodologi pengetahuan yang telah dibakukan dimana masih sedikit pelatihan dan sertifikasi yang tersedia dan ditawarkan di masyarakat;
- Sangat terbatasnya SDM pendukung yang memiliki kompetensi dan keahlian khusus di bidang forensik komputer; dan
- Pada kenyataannya, pekerjaan forensik komputer masih lebih banyak unsur seninya dibandingkan pengetahuannya (more "Art" than "Science").

17.5 MENGURAIKAN BERBAGAI KEJAHATAN KOMPUTER

Berbeda dengan di dunia nyata, kejahatan di dunia komputer dan internet variasinya begitu banyak, dan cenderung dipandang dari segi jenis dan kompleksitasnya, meningkat secara eksponensial. Secara prinsip, kejahatan di dunia komputer dibagi menjadi tiga, yaitu: (i) aktivitas dimana komputer atau piranti digital dipergunakan sebagai alat bantu untuk melakukan tindakan kriminal; (ii) aktivitas dimana komputer atau piranti digital dijadikan target dari kejahatan itu sendiri; dan (iii) aktivitas dimana pada saat yang bersamaan komputer atau piranti digital dijadikan alat untuk melakukan kejahatan terhadap target yang merupakan komputer atau piranti digital juga.

Agar tidak salah pengertian, perlu diperhatikan bahwa istilah "komputer" yang dipergunakan dalam konteks forensik komputer mengandung makna yang luas,

yaitu piranti digital yang dapat dipergunakan untuk mengolah data dan melakukan perhitungan secara elektronik, yang merupakan suatu sistem yang terdiri dari piranti keras (hardware), piranti lunak (software), piranti data/informasi (infoware), dan piranti sumber daya manusia (brainware).

Contoh kejahatan yang dimaksud dan erat kaitannya dengan kegiatan forensi komputer misalnya:

- Pencurian kata kunci atau "password" untuk mendapatkan hak akses;
- Pengambilan data elektronik secara diam-diam tanpa sepengetahuan sang empunya;
- Pemblokiran hak akses ke sumber daya teknologi tertentu sehingga yang berhak tidak dapat menggunakannya;
- Pengubahan data atau informasi penting sehingga menimbulkan dampak terjadinya mis-komunikasi dan/atau dis-komunikasi;
- Penyadapan jalur komunikasi digital yang berisi percakapan antara dua atau beberapa pihak terkait;
- Penipuan dengan berbagai motivasi dan modus agar si korban memberikan aset berharganya ke pihak tertentu;
- Peredaran foto-foto atau konten multimedia berbau pornografi dan pornoaksi ke target individu di bawah umur;
- Penyelenggaraan transaksi pornografi anak maupun hal-hal terlarang lainnya seperti perjudian, pemerasan, penyalahgunaan wewenang, pengancaman, dan lain sebagainya;
- Penyelundupan file-file berisi virus ke dalam sistem korban dengan beraneka macam tujuan;
- Penyebaran fitnah atau berita bohong yang merugikan seseorang, sekelompok individu, atau entitas organisasi; dan lain sebagainya.

17.6 MENETAPKAN OBYEK FORENSIK

Apa saja yang bisa dipergunakan sebgai obyek forensik, terutama dalam kaitannya dengan jenis kejahatan yang telah dikemukakan tersebut? Dalam dunia kriminal dikenal istilah "tidak ada kejahatan yang tidak meninggalkan jejak". Ada banyak sekali hal yang bisa menjadi petunjuk atau jejak dalam setiap tindakan kriminal yang dilakukan dengan menggunakan teknologi seperti komputer. Contohnya adalah sebagai berikut:

- Log file atau catatan aktivitas penggunaan komputer yang tersimpan secara rapi dan detail di dalam sistem;
- File yang sekilas telah terhapus secara sistem, namun secara teknikal masih bisa diambil dengan cara-cara tertentu;

- Catatan digital yang dimiliki oleh piranti pengawas trafik seperti IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System);
- Hard disk yang berisi data/informasi backup dari sistem utama;
- Rekaman email, mailing list, blog, chat, dan mode interaksi dan komunikasi lainnya;
- Beraneka ragam jeis berkas file yang dibuat oleh sistem maupun aplikasi untuk membantu melakukan manajemen file (misalnya: .tmp, .dat, .txt, dan lain-lain);
- Rekam jejak interaksi dan trafik via internet dari satu tempat ke tempat yang lain (dengan berbasis IP address misalnya);
- Absensi akses server atau komputer yang dikelola oleh sistem untuk merekam setiap adanya pengguna yang login ke piranti terkait; dan lain sebagainya.

Beraneka ragam jenis obyek ini selain dapat memberikan petunjuk atau jejak, dapat pula dipergunakan sebagai alat bukti awal atau informasi awal yang dapat dipergunakan oleh penyelidik maupun penyidik dalam melakukan kegiatan penelusuran terjadinya suatu peristiwa kriminal, karena hasil forensik dapat berupa petunjuk semacam:

- Lokasi fisik seorang individu ketika kejahatan sedang berlangsung (alibi);
- Alat atau piranti kejahatan yang dipergunakan;
- Sasaran atau target perilaku jahat yang direncanakan;
- Pihak mana saja yang secara langsung maupun tidak langsung terlibat dalam tindakan kriminal;
- Waktu dan durasi aktivitas kejahatan terjadi;
- Motivasi maupun perkiraan kerugian yang ditimbulkan;
- Hal-hal apa saja yang dilanggar dalam tindakan kejahatan tersebut;
- Modus operandi pelaksanaan aktivitas kejahatan; dan lain sebagainya.

17.7 MENERAPKAN TAHAPAN AKTIVITAS FORENSIK

Secara metodologis, terdapat paling tidak 14 (empat belas) tahapan yang perlu dilakukan dalam aktivitas forensik, sebagai berikut:

1. Pernyataan Terjadinya Kejahatan Komputer – merupakan tahap dimana secara formal pihak yang berkepentingan melaporkan telah terjadinya suatu aktivitas kejahatan berbasis komputer;
2. Pengumpulan Petunjuk atau Bukti Awal – merupakan tahap dimana ahli forensik mengumpulkan semua petunjuk atau bukti awal yang dapat dipergunakan sebagai bahan kajian forensik, baik yang bersifat tangible maupun intangible;
3. Penerbitan Surat Pengadilan – merupakan tahap dimana sesuai dengan peraturan dan perundang-undangan yang berlaku, pihak pengadilan

memberikan ijin resmi kepada penyelidik maupun penyidik untuk melakukan aktiivitas terkait dengan pengolahan tempat kejadian perkara, baik yang bersifat fisik maupun maya;

4. Pelaksanaan Prosedur Tanggapan Dini – merupakan tahap dimana ahli forensik melakukan serangkaian prosedur pengamanan tempat kejadian perkara, baik fisik maupun maya, agar steril dan tidak tercemar/terkontaminasi, sehingga dapat dianggap sah dalam pencarian barang-barang bukti;
5. Pembekuan Barang Bukti pada Lokasi Kejahatan – merupakan tahap dimana seluruh barang bukti yang ada diambil, disita, dan/atau dibekukan melalui teknik formal tertentu;
6. Pemindahan Bukti ke Laboratorium Forensik – merupakan tahap dimana dilakukan transfer barang bukti dari tempat kejadian perkara ke laboratorium tempat dilakukannya analisa forensik;
7. Pembuatan Salinan "2 Bit Stream" terhadap Barang Bukti – merupakan tahap dimana dilakukan proses duplikasi barang bukti ke dalam bentuk salinan yang identik;
8. Pengembangan "MD5 Checksum" Barang Bukti – merupakan tahap untuk memastikan tidak adanya kontaminasi atau perubahan kondisi terhadap barang bukti yang ada;
9. Penyiapan Rantai Posesi Barang Bukti – merupakan tahap menentukan pengalihan tanggung jawab dan kepemilikan barang bukti asli maupun duplikasi dari satu wilayah otoritas ke yang lainnya;
10. Penyimpanan Barang Bukti Asli di Tempat Aman – merupakan tahap penyimpanan barang bukti asli (original) di tempat yang aman dan sesuai dengan persyratan teknis tertentu untuk menjaga keasliannya;
11. Analisa Barang Bukti Salinan – merupakan tahap dimana ahli forensik melakuka analisa secara detail terhadap salinan barang-brang bukti yang dikumpulkan untuk mendapatkan kesimpulan terkait dengan seluk beluk terjadinya kejahatan;
12. Pembuatan Laporan Forensik – merupakan tahap dimana ahli forensik menyimpulkan secara detail hal-hal yang terjadi seputar aktivititas kejahatan yang dianalisa berdasarkan fakta forensik yang ada;
13. Penyerahan Hasil Laporan Analisa – merupakan tahap dimana secara resmi dokumen rahasia hasil forensik komputer diserahkan kepada pihak yang berwajib; dan
14. Penyertaan dalam Proses Pengadilan – merupakan tahap dimana ahli forensik menjadi saksi di pengadilan terkait dengan kejahatan yang terjadi.

17.8 MENDEFINISIKAN KEBUTUHAN SUMBER DAYA

Untuk melakukan aktivitas forensik, dibutuhkan sejumlah piranti bantu, baik yang berbentuk software maupun hardware. Piranti lunak atau software biasanya dipergunakan oleh praktisi untuk membantu mereka dalam melakukan hal-hal sebagai berikut:

- Mencari dan mengembalikan file yang telah terhapus sebelumnya;
- Membantu merekonstruksi pecahan-pecahan file yang ada (corrupted file);
- Mengidentifikasi anomali program melalui analisa serangkaian data beserta struktur algoritma yang terdapat pada sebuah file atau sistem basis data;
- Menemukan jejak-jejak yang tertinggal dalam sebuah peristiwa kriminal tertentu yang telah dilakukan sebelumnya;
- Mendapatkan data berbasis pola-pola tertentu sesuai dengan permintaan penegak hukum dalam proses penyelidikan maupun penyidikan peristiwa kejahatan internet;
- Memfilter dan memilah-milah antara data yang berguna/relevan untuk kebutuhan forensik dengan yang tidak, agar mekanisme analisa dapat dilakukan secara fokus dan detail;
- Menganalisa kejanggalan-kejanggalan yang terdapat pada suatu program atau sub-program tertentu;
- Mempercepat proses pencarian penggalan instruksi atau data tertentu yang dibutuhkan oleh seorang ahli forensik terhadap sebuah media repositori bermemori besar;
- Menguji dan mengambil kesimpulan terhadap sejumlah kondisi tertentu terkait dengan aktivias dan konsep forensik; dan lain sebagainya.

Dewasa ini piranti lunak tersebut cukup banyak tersedia di pasar, mulai dari yang bersifat gratis (open source) hingga yang komersial (berharga milyaran rupiah). Disamping aplikasi pendukung aktivitas forensik, diperlukan pula seperangkat piranti keras atau peralatan elektronik/digital agar proses forensik dapat dilakukan secara efektif dan sesuai dengan prosedur baku standar yang berlaku. Piranti keras ini biasanya dibutuhkan untuk melakukan hal-hal sebagai berikut:

- Membuat replikasi atau copy atau cloning dari sistem basis data (atau media basis data) yang akan diteliti dengan cara yang sangat cepat dan menghasilkan kualitas yang identik dengan aslinya;
- Mengambil atau memindahkan atau mengekstrak data dari tempat-tempat atau media penyimpan yang khusus seperti: telepon genggam, server besar (superkomputer), PDA (Personal Digital Assistance), komputer tablet, dan lain-lain;

- Menggenerasi nilai numerik secara urut maupun random secara ultra cepat untuk membongkar kata kunci (password) atau hal sejenis lainnya, sebagai bagian dari proses deskripsi (tilik sandi);
- Membongkar berbagai proteksi secara piranti keras atau lunak yang menjadi proteksi dari sebagian besar perangkat teknologi informasi dan komunikasi;
- Menghapus dan memformat hard disk secara cepat dan efektif dengan melakukan demagnetisasi agar data benar-benar terhapus sebagai bagian dari penyiapan media replikasi; dan lain sebagainya.

Seperti halnya dalam dunia nyata, diperlukan pula ahli Forensik Komputer dalam melaksanakan pekerjaan terkait. Jika dilihat dari kompetensi dan keahliannya, seorang ahli forensik komputer yang baik dan lengkap harus memiliki tiga domain atau basis pengetahuan maupun keterampilannya, yaitu dari segi akademis, vokasi, dan profesi. Dari sisi akademis, paling tidak yang bersangkutan memiliki latar belakang pengetahuan kognitif mengenai cara kerja komputer dalam lingkungan jejaring teknologi informasi dan komputasi, terutama berkaitan dengan hal-hal yang bersifat fundamental dalam pengembangan sistem berbasis digital. Sementara dari sisi vokasi, dibutuhkan kemampuan “untuk melakukan” atau kerap disebut sebagai psiko-motorik, karena dalam prakteknya seorang ahli forensik akan melakukan kajian, analisa, dan penelitian secara mandiri dengan menggunakan seperangkat peralatan teknis yang spesifik. Dan yang terakhir dari perspektif profesi, seorang ahli yang baik akan berpegang pada kode etik (afektif) seorang ahli forensik. Disamping itu dibutuhkan pula pengalaman yang cukup untuk dapat berkreasi dan berinovasi dalam setiap tantangan kasus forensik. Berdasarkan pengalaman, memang yang paling sulit adalah menyiapkan SDM yang handal di bidang forensik komputer, karena hingga sekarang jumlahnya sangatlah sedikit – tidak sepadan dengan besarnya kebutuhan di masyarakat.

-oo0oo-

~ 18 ~

MENCERMATI FENOMENA KEBOCORAN DATA DAN INFORMASI RAHASIA

Capaian Pembelajaran (*Learning Outcomes*):

1. Menjelaskan Perilaku Senang Berbagi
2. Menjelaskan Kecerobohan Pemilik Data
3. Menjelaskan Fenomena Social Engineering
4. Menjelaskan Fenomena Pelanggaran Etika
5. Menjelaskan Lemahnya Manajemen Informasi
6. Menjelaskan Keberadaan Proses Digitalisasi
7. Menjelaskan Aspek Kerawanan Teknologi
8. Menjelaskan Fenomena Keterbukaan
9. Menjelaskan Menjamurnya Pemulung Data
10. Menjelaskan Rancangan Piranti Lunak
11. Menjelaskan Kegiatan Kriminal

Belakangan ini masyarakat Indonesia cukup resah dengan adanya fenomena "kebocoran data" yang menyebabkan mengemukanya beragam kasus semacam beredarnya dokumen rahasia Wikileaks, SMS penawaran kredit, gambar/ video porno, nomor kartu kredit, data/informasi rahasia perusahaan, dan lain sebagainya. Banyak pihak yang bertanya-tanya, siapa yang perlu disalahkan atau bertanggung jawab terhadap hal ini? Apakah akar penyebab fenomena negatif ini? Mengapa kejadian yang sama berulang kembali dan tidak kunjung berhenti? Dapatkah hal ini ditanggulangi bahkan dihilangkan sama sekali?

Sejalan dengan berkembangnya dunia internet yang memberikan begitu banyak kemudahan, keuntungan, dan manfaat bagi orang banyak, teriring pula bersamanya keberadaan resiko, ancaman, dan aspek negatif dari aktivitas penyalahgunaannya. Kebocoran data yang selama ini disinyalir kerap terjadi, dipicu oleh sejumlah hal, yang kalau dilihat secara sungguh-sungguh disebabkan karena hal-hal yang bersifat non teknis. Ketidaktahuan pengguna teknologi, kecerobohan pemilik data, keterbatasan edukasi masyarakat, kealpaan individu, dan ketidakpedulian seseorang merupakan sejumlah "lubang kerawanan" yang kerap dipergunakan oleh pihak jahat untuk menjalankan misi negatifnya. Berdasarkan pengalaman yang lalu-lalu, dan disertai dari pembelajaran mendalam terhadap kasus-kasus kebocoran informasi, paling tidak terdapat 11 (sebelas) hal yang perlu dicermati secara sungguh-sungguh oleh masyarakat sebagai penyebab utama terjadinya fenomena ini.

18.1 MENJELASKAN PERILAKU SENANG BERBAGI

Pertama, perilaku atau budaya masyarakat Indonesia yang senang membagi-bagi data serta informasi mengenai kerabat dan teman dekatnya. Pernah ada suatu riset yang menarik, dimana jika dua orang Indonesia diambil secara acak (random), dan keduanya dibiarkan ngobrol, maka akan terungkap adanya hubungan langsung maupun tidak langsung di antara keduanya melalui pertalian keluarga atau teman paling banyak enam jarak titik hubungan (six degree of separation). Ramahnya dan senangnya masyarakat Indonesia dalam bersosialisasi menyebabkan setiap individu memiliki banyak teman. Didasari rasa saling percaya, maka kebiasaan atau perilaku saling tukar-menukar data atau informasi pribadi menjadi suatu hal yang biasa. Lihatlah bagaimana mudahnya dua orang yang baru berkenalan dalam sebuah seminar langsung tukar menukar PIN Blackberry-nya, atau kebiasaan mencantumkan nomor telepon genggam dalam kartu nama yang sering dibagikan dan dipertukarkan dalam berbagai kesempatan, atau secara sengaja memberitahukan alamat email maupun telepon pribadinya di seminar-seminar karena merupakan bagian dari pemasaran (marketing), atau bahkan di setiap profil pada akun jejaring sosial (seperti Facebook, Twitter, Friendster,

MySpace, dan lain-lain) individu yang bersangkutan selalu mencantumkan data-data pribadinya secara relatif lengkap dan jujur. Tentu saja secara sengaja maupun tidak sengaja, dipicu dengan karakteristik internet yang terbuka dan bebas, data/ informasi ini mudah sekali mengalir dari satu tempat ke tempat lainnya – tanpa terkendali. Oleh karena itu tidak mengherankan jika ada satu atau sekelompok orang yang rajin mengumpulkan data atau informasi tersebut (database) demi berbagai kepentingan di kemudian hari.

18.2 MENJELASKAN KECEROBOHAN PEMILIK DATA

Kedua, kecerobohan pemilik data dalam mengelola data rahasia miliknya karena ketidaktahuan ataupun keteledoran. Hal yang paling mencolok terkait dengan aspek ini adalah mengenai cara seseorang mengelola kartu kredit yang dimilikinya. Perlu diketahui, bahwa seseorang dapat melakukan transaksi perdagangan via internet dengan mengetahui data atau informasi kartu kredit sebagai berikut: (i) 16 digit nomor kartu kredit yang tercantum di sisi muka; (ii) 3 digit nomor CCV yang ada di sisi belakang kartu kredit; (iii) tanggal akhir berlakunya kartu kredit; dan (iv) nama pemengang kartu kredit yang tercantum. Informasi ini dengan mudahnya dapat dicatat oleh siapa saja yang memperoleh kesempatan memegang kartu kredit orang lain selama beberapa menit, seperti misalnya dalam konteks: membayar makanan di restauran (kartu kredit dibawa pelayan untuk diserahkan ke kasir), membayar belanjaan di supermarket (pembeli tidak memperhatikan secara seksama apa yang dilakukan oleh kasir ketika transaksi berlangsung), membayar kamar di hotel (kartu kredit hilang dari pandangan selama beberapa menit untuk dikonfirmasi dan autentifikasi), membayar transaksi via e-commerce (tanpa melihat status “http” untuk mengetahui profil keamanan situs tempat berinteraksi), dan lain sebagainya. Hal ini bukan berarti ingin menuduh adanya modus kejahatan yang dilakukan para pelayan restauran, kasir, atau karyawan hotel, namun untuk menegaskan adanya resiko atau peluang melakukan tindakan kejahatan dimana-mana. Pengelolaan kartu ATM juga memiliki kerawanan tersendiri. Cukup banyak ditemukan seorang ayah atau ibu yang memperbolehkan anaknya mengambil uang melalui ATM milik orang tuanya tersebut dengan memberitahukan kata kunci atau “password”-nya (ada kemungkinan dalam kenyataan sang anak menyuruh orang lain seperti supir atau pembantu rumah tangganya yang melakukan pengambilan tunai via ATM). Keadaan makin bertambah runyam apabila sang orang tua, yang “password”-nya sudah diketahui orang lain tersebut menggunakan “password” yang sama untuk akun penting lainnya seperti “internet banking” atau “mobile banking” miliknya – termasuk akun email terkemuka di Yahoo atau GMail. Tentu saja dengan mengatahui kata kunci rahasia tersebut, dengan leluasa akun yang bersangkutan dapat dibajak oleh orang lain (sejumlah tokoh politik, pejabat

publik, maupun aktor/artis terkemuka di Indonesia telah menjadi korban dari pembajakan akun ini). Hal lain yang mengemuka adalah seringnya para pimpinan perusahaan menyerahkan atau memberitahu "password" akun miliknya ke sekretaris atau asisten pribadinya. Tujuannya sebenarnya baik, untuk membantu yang bersangkutan mengelola proses korespondensi dan komunikasi yang ada; namun yang bersangkutan lupa bahwa dengan memberitahukan "password" tersebut berarti sang pimpinan secara langsung menyerahkan seluruh "otoritas" yang dimilikinya untuk dapat dieksekusi oleh sekretaris atau asisten pribadinya tersebut (bisa dibayangkan apa yang akan terjadi jika dalam perusahaan tersebut menggunakan sistem "single log-in").

18.3 MENJELASKAN FENOMENA SOCIAL ENGINEERING

Ketiga, maraknya fenomena dengan menggunakan teknik "social engineering" dilakukan oleh pihak tak bertanggung jawab untuk menipu orang lain. "Social Engineering" atau "rekayasa sosial" adalah suatu teknik yang dipergunakan untuk mendapatkan kepercayaan orang lain melalui pendekatan interaksi sosial sehari-hari sehingga tidak menimbulkan kecurigaan. Contoh klasiknya adalah seseorang yang dikabarkan mendapatkan hadiah undian tertentu via SMS dimana hadiah tersebut dapat ditebus apabila yang bersangkutan segera mengirimkan biaya pembayaran pajaknya lewat ATM, atau berita buruk kepada seseorang mengenai adanya kecelakaan lalu lintas yang menimpa keluarga dekatnya sehingga yang bersangkutan diminta untuk segera mengirimkan uang untuk kebutuhan operasi yang harus segera dikirimkan untuk menyelamatkan nyawa sang korban, dan lain sebagainya. Bahkan saat ini modus tersebut sudah berkembang lebih jauh. Misalnya jika ada seorang tokoh politik yang telepon genggamnya rusak, disarankan oleh rekan lainnya (misalnya tokoh politik dari partai yang berbeda) untuk memperbaikinya di sebuah toko yang dikatakan sangat mahir dan handal. Di toko tersebut, selain telepon genggam yang bersangkutan direparasi, data-data yang ada di dalam memori piranti komunikasi tersebut sekaligus direkam untuk tujuan tidak baik di kemudian hari (pemerasan). Tentu saja sang pemilik telepon genggam tidak tahu bahwa banyak berkas-berkas "file" pribadinya hilang (teks, gambar, audio, dan video) mengingat teleponnya telah bekerja kembali dengan normal. Cara menipu lainnya adalah melalui "electronic mail" atau "email" dimana dikatakan bahwa dalam rangka perbaikan dan pengembangan teknologi informasi perusahaan, maka setiap pelanggan diminta untuk memberikan "password"-nya akan yang bersangkutan dapat diprioritaskan dalam proses "upgrading" teknologi yang dimaksud. Tanpa curiga, mereka yang menyerahkan kata kunci dimaksud, akan langsung seketika itu juga menjadi korban penipuan.

18.4 MENJELASKAN FENOMENA PELANGGARAN ETIKA

Keempat, pelanggaran etika atau aturan internal yang dilakukan oleh individu dan/atau kelompok dalam mengelola informasi organisasi. Cukup banyak anak-anak muda, yang berhasil dalam karir dunia teknologi informasi, tidak dibekali pengetahuan yang memadai terkait dengan unsur etika maupun masalah berkaitan dengan peraturan dan perundang-undangan di bidang informasi dan transaksi elektronik. Lihatlah bagaimana secara eksplisit mereka yang pindah bekerja dari satu perusahaan ke perusahaan lainnya dengan leluasanya membawa data dan informasi dari perusahaan lamanya – dan diberikan ke perusahaan barunya (dapat dibayangkan dampaknya jika yang bersangkutan pindah kerja ke perusahaan pesaingnya). Data atau informasi yang dibawa dan disampaikan itu dapat beraneka ragam rupanya, mulai dari profil pelanggan hingga detail transaksi yang terjadi. Hal ini belum termasuk unsur godaan yang selalu menghantui unit divisi teknologi informasi yang secara teknis dapat membaca hampir seluruh data yang berseliweran di sebuah perusahaan karena tidak adanya proses enkripsi atau penyandian yang diberlakukan (otoritas cukup tinggi dimiliki oleh seorang "super user"). Dengan berbekal dan beralasan menjalankan tugas teknis, seorang karyawan dari unit teknologi informasi dapat mengambil data apa saja dan dari mana saja – terutama jika pengguna yang bersangkutan berperilaku "pasrah" karena tidak memiliki pengetahuan teknis di bidang komputer atau teknologi informasi. Merubah konfigurasi, mengecek keberadaan virus, memperbaiki sistem yang "hang", meng-"upgrade" aplikasi lama ke yang baru, atau membantu instalasi program tertentu, merupakan sejumlah alasan yang dapat dipergunakan sebagai topeng untuk dapat masuk ke dalam sistem seseorang (ingat, dalam dunia digital, seseorang tidak akan merasa kehilangan aset elektronik yang dimilikinya, karena semuanya dapat diduplikasi dengan mudah dan bersifat identik).

18.5 MENJELASKAN LEMAHNYA MANAJEMEN INFORMASI

Kelima, lemahnya manajemen informasi yang diberlakukan dan dipraktekan oleh organisasi. Di abad moderen ini, begitu banyak perusahaan dan organisasi yang memutuskan untuk memanfaatkan teknologi informasi dan internet dengan sebanyak-banyaknya dan sebaik-baiknya untuk meningkatkan kinerja dan performannya. Namun sayangnya kebanyakan usaha ini tidak dibarengi dengan sosialisasi dan edukasi mengenai penerapan manajemen informasi yang baik. Lihatlah contoh tidak diberlakukannya aturan untuk menyandikan atau mengenkripsi data atau informasi penting dan tergolong rahasia milik perusahaan; dimana ketika seorang Direktur atau General Manager kehilangan notebook atau laptopnya, dengan mudahnya sang pencuri akan memperoleh aset berharga

tersebut (untuk kemudian diperdagangkan atau disebarkan ke pihak-pihak lain untuk mendapatkan keuntungan). Contoh lain dalam kasus promosi seorang pegawai atau karyawan. Biasanya, di posisinya yang baru, yang bersangkutan akan mendapatkan fasilitas komputer meja atau pun notebook/laptop yang baru pula – sehingga yang lama dapat ditinggalkan. Masalahnya adalah tidak ada prosedur yang mengharuskan komputer atau notebook/laptom yang lama tersebut dibersihkan dan diformat ulang sehingga orang baru yang menggantikan posisi yang ditinggalkan tersebut tidak dapat mengetahui isi dari file-file lama yang dimiliki oleh individu yang dipromosi. Jika hal tersebut tidak dilakukan, bisa dibayangkan berapa banyak data individu maupun rahasia perusahaan yang akan diketahui yang bersaangkutan. Yang dapat dijadikan sebagai contoh klasik lainnya adalah masalah kebiasaan merekam isi pembicaraan sebuah rapat strategis dengan menggunakan perekam digital, agar nanti mempermudah proses pembuatan notulen rapat. Banyak hal yang terjadi dalam sebuah rapat, mulai dari yang bersifat rahasia hingga yang kritikal. Bayangkan dampak yang dapat terjadi, apabila sekretaris yang memiliki rekaman tersebut memiliki niat jahat dengan membeberkan rekaman dimaksud ke beberapa orang, maka hancurlah reputasi organisasi perusahaan yang dimaksud.

18.6 MENJELASKAN KEBERADAAN PROSES DIGITALISASI

Keenam, adanya proses digitalisasi dari koleksi data/informasi sekunder yang dimiliki komunitas tertentu yang diunggah ke dunia siber (internet). Masyarakat Indonesia tumbuh dalam kelompok-kelompok, dimana setiap komunitas berusaha untuk memperlihatkan eksistensinya. Contohnya adalah sekelompok alumni dari SMA atau perguruan tinggi tertentu yang mengadakan pesta reuni. Sebagaimana layaknya komunitas alumni yang lain, mereka bersepakat membuat buku alumni dimana di dalamnya lengkap didaftarkan seluruh mantan pelajar atau mahasiswa, lengkap dengan alamat rumah, email, dan nomor telepon pribadi. Mereka yang punya hobi atau kesukaan seperti fitness, golf, fotografi, kuliner, atau filateli misalnya terdaftar sebagai anggota aktif klub-klub terkait, yang untuk menjadi anggotanya dibutuhkan sejumlah persyaratan administrasi ketika mendaftar – termasuk di dalamnya pengisian formulir menengai data pribadi. Klub ini kemudian menyimpan seluruh data anggotanya dalam sebuah buku induk keanggotaan. Hal yang sama berlaku pula untuk konteks seperti: kartu diskon anggota toko waralaba/ retail, kartu anggota organisasi atau kelompok sosial, daftar pelanggan loyal jasa komersial, daftar pasien rumah sakit atau puskesmas, daftar penerima bantuan pemerintah, dan lain sebagainya. Berbeda dengan jaman dulu, saat ini hampir seluruh catatan tersebut telah diubah bentuknya menjadi file digital – dengan menggunakan program pengolah kata atau sejenisnya. Dan setelah menjadi berkas

digital, maka untuk meningkatkan pelayanan pelanggan, data tersebut diunduh ke internet agar para pemangku kepentingan dapat mengaksesnya secara bebas.

18.7 MENJELASKAN ASPEK KERAWANAN TEKNOLOGI

Ketujuh, adanya kerawanan (vulnerabilities) dari kebanyakan sistem teknologi informasi yang dimiliki institusi. Sudah menjadi rahasia umum, bahwa kebanyakan situs atau "website" internet di Indonesia ini didesain dan dikembangkan secara sederhana (dan mungkin sedikit "asal-asalan"). Hasil pemantauan Komunitas Keamanan Informasi memperlihatkan betapa banyak dan umumnya lubang-lubang kerawanan serta kelemahan dari situs-situs internet di tanah air yang dapat dengan mudah dimanfaatkan dan dieksploitasi oleh pihak-pihak jahat yang tidak bertanggung jawab. Penyebabnya macam-macam, antara lain: ingin cepat-cepat instalasi sistem (sehingga melupakan setting tingkat keamanan), menggunakan piranti lunak bajakan (yang didalamnya banyak malware), kurang pemahaman mengenai teknologi yang dipergunakan, kekurangmampuan SDM yang menangani, dan lain sebagainya. Oleh karena itu tidaklah heran jika banyak sekali terjadi peristiwa seperti: website yang diubah isi dan kontennya (web defacement), data/informasi yang diambil tanpa sepengetahuan empunya via internet, kata kunci atau password yang dicuri, virus atau program mata-mata (malware) yang ditanamkan secara diam-diam di server tertentu, dan lain-lain. Untuk mengetahui tingkat kerawanan yang ada, perusahaan atau organisasi perlu melakukan audit atau "penetration test". Oleh karena itu tidaklah perlu heran jika banyak data atau informasi yang berhasil dicuri karena banyaknya lubang-lubang kerawanan yang tidak diamankan sama sekali. Dengan sistem keamanan yang baik, maka hanya mereka yang berhak dapat mengaksesnya; namun ketidakadaan sistem keamanan informasi berakibat sebaliknya, siapa saja dapat dengan bebas dan leluasa mengetahui data pribadi orang lain. Apalagi saat ini dimana penyebaran dapat dengan mudah dilakukan melalui berbagai cara seperti: email, mailing list, SMS, twitter, dan lain sebagainya.

18.8 MENJELASKAN FENOMENA KETERBUKAAN

Kedelapan, terkait dengan karakteristik dari internet yang "memaksa" seseorang untuk senantiasa bersikap terbuka. Lihatlah bagaimana aplikasi terkemuka dan populer semacam Yahoo, Gmail, Twitter, Facebook, Blogspot, dan lain sebagainya yang mewajibkan pengguna untuk mendaftarkan dirinya secara benar agar dapat menggunakan berbagai fitur aplikasi dimaksud. Dan memang pada kenyataannya kebanyakan dari para pengguna memberitahukan data diri dan lingkungannya secara benar karena selain berusaha untuk menerapkan etika

yang baik dalam berinternet, tidak pernah terpikirkan oleh sang pengguna bahwa pemilik aplikasi tersebut akan menyalahgunakan data pelanggan yang dimilikinya. Situs-situs e-business atau e-commerce pun selalu didesain sedemikian rupa sehingga senantiasa "memaksa" pegguna untuk membeberkan data dirinya seperti nama, tanggal lahir, alamat rumah/kantor, dan nomor telepon terkait agar barang yang dipesan dan dibelunya dapat dikirimkan atau diposkan ke rumah. Masalahnya adalah tidak semua penyedia jasa di internet memiliki etika dan profesionalisme yang baik. Banyak sekali terdapat situs-situs game, berita, perdagangan, dan lain-lain yang dibuat secara khusus sebagai "honeypot" atau umpan untuk mengumpulkan data pribadi individu-individu demi kepentingan jual-beli informasi di kemudian hari. Mereka tahu persis betapa mahal dan strategisnya memiliki data pribadi individu karena dapat dipergunakan untuk berbagai kepentingan – sehingga tidak segan-segan investasi untuk membuat aplikasi internet yang menarik. Oleh karena itu perlu berhati-hati setiap kali terdapat situs atau website yang meminta pengguna untuk mengisi sebanyak mungkin informasi detail karena berpotensi dapat disalahgunakan.

18.9 MENJELASKAN MENJAMURNYA PEMULUNG DATA

Kesembilan, menjamurnya para "pemulung data" di dunia siber (internet). Berbekal mesin pencari seperti Google.com, Yahoo.com, Altavista.com, atau MSNSearch.com, seseorang dapat dengan mudah melakukan berbagai jenis pencarian terhadap data atau informasi pribadi seseorang. Dengan ketekunan sedemikian rupa, seorang individu dapat dengan mudah mengumpulkan satu demi satu data pribadi seseorang dengan cara terencana (menggunakan teknik pencarian terfokus, artinya secara khusus mencari data individu tertentu) maupun dengan cara acak (memanfaatkan pola generik tertentu, mencari siapa saja yang dapat dikumpulkan datanya). Jika satu hari saja yang bersangkutan dapat mengumpulkan 100 data, berarti dalam satu bulan paling tidak 3,000 data individu dapat dikoleksi (apalagi jika yang melakukan pengumpulan adalah sekelompok orang). Pola ini jika dilakukan dengan benar dapat secara efektif digunakan untuk mengoleksi data pribadi berkualitas yang kelak dapat diperjualbelikan di pasar dunia siber.

18.10 MENJELASKAN RANCANGAN PIRANTI LUNAK

Kesepuluh, perilaku piranti lunak (software) rancangan khusus yang diperuntukkan untuk mengoleksi beragam data dan informasi pribadi. Berbeda dengan teknik "pemulungan" sebelumnya, secara teknis dapat dikembangkan sebuah aplikasi, yang dapat secara otomatis melakukan pencarian terhadap data

pribadi seseorang dengan memanfaatkan pendekatan algoritma tertentu (misalnya: crawling, filtering, profiling, dan lain sebagainya). Dengan berawal pada data email terkemuka seperti Yahoo atau Gmail misalnya, dapat ditelusuri kemudian profil seseorang melalui berbagai situs terkemuka jejaring sosial semacam Facebook, Twitter, Flickr, MySpace, Skype, dan lain-lain – bahkan terbuka kemungkinan untuk lebih jauh masuk ke dalam website "proprietary" organisasi tertentu seperti perguruan tinggi, pemerintahan, komunitas, perusahaan, dan lain sebagainya. Aplikasi semacam ini dapat tampil dalam dua rupa, yaitu yang bersifat legal formal maupun tergolong sebagai virus. Dikatakan legal formal karena memang dibuat, dirancang khusus, dan diperjual belikan untuk mereka yang bergerak di bidang pemasaran dan penjualan. Namun banyak pula piranti lunak "malware" yang dibuat untuk menyebarkan virus tertentu berbasis alamat email. Pada intinya adalah, sangat mudah dikembangkan sebuah program yang bertujuan untuk membantu seseorang dalam melakukan pengumpulan terhadap data tertentu untuk berbagai keperluan. Bahkan tidak jarang ditemukan sejumlah individu yang sengaja membuat program untuk mengoleksi berbagai dokumen dengan kategori "rahasia" atau informasi sensitif lainnya.

18.11 MENJELASKAN KEGIATAN KRIMINAL

Kesebelas, memang ada kesengajaan dari pihak-pihak tertentu untuk melakukan kegiatan kriminal, baik melalui domain eksternal maupun internal. Yang terakhir dapat dikategorikan sebagai penyebab bocornya data atau informasi tertentu karena memang adanya pihak-pihak internal maupun eksternal organisasi yang memiliki niat dan agenda melakukan tindakan kejahatan tertentu, seperti: pencurian data, penjebolan rekening, pengelabuan pelanggan, pengubahan informasi, pengambilalihan akses, pembohongan publik, dan lain sebagainya. Individu maupun komplotan yang mahir dalam melakukan kejahatan berbasis komputer maupun internet ini dapat berasal dari pihak luar maupun pihak dalam organisasi. Biasanya pihak luar melakukannya dengan berbekal pada teknik "hacking" yang dimilikinya, sementara pihak dalam melakukannya dengan berbekal pada teknik "social engineering" sebagai kuncinya. Secara karakteristik, kejahatan yang dilakukan oleh pihak internal organisasi lebih mudah dilakukan, mengingat yang bersangkutan tahu persis bagaimana cara kerja sebuah sistem dalam institusi terkait. Oleh karena itulah perlu adanya sistem keamanan informasi dalam rupa kebijakan, kendali teknis (kontrol), dan SOP (Standard Operating Procedure) yang ketat untuk mencegah terjadinya peristiwa yang tidak diinginkan tersebut.

Pada akhirnya, aspek edukasi merupakan kunci paling efektif dalam usaha untuk mencegah terjadinya peristiwa kebocoran data secara masal dan masif yang kerap

terjadi belakangan ini. Setiap individu harus memiliki kesadaran, keperdulian, dan kemampuan – sesuai dengan kapasitas dan pekerjaannya sehari-hari – untuk mengelola keamanan informasi dalam lingkungannya sendiri. Prinsip "your security is my security" perlu ditanamkan secara mendalam ke seluruh insan pengguna komputer dan internet. Kebiasaan bersifat hati-hati atau "prudent" harus merupakan budaya yang perlahan-lahan perlu ditanamkan melalui pendekatan pendidikan kepasa semuar orang tanpa kecuali. Beragam organisasi dengan segala variasi dan karakteristiknya pun memiliki kewajiban dalam melakukan edukasi tiada henti kepada seluruh pemangku kepentingannya – mulai dari manajemen, karyawan, pelanggan, mitra, dan seluruh stakeholder terkait lainnya. Pepatah mengatakan "there is no patching for human stupidity" secara eksplisit mengatakan bahwa kerawanan teknis pada sistem dapat dengan mudah diperbaiki, namun lubang-lubang kerawanan pada manusia tidak ada obatnya kecuali pengetahuan, kemampuan, dan kemauan.

-oo0oo-

LATIHAN, TUGAS, DAN UJIAN

Latihan

1. Huruf E pada CERT berasal dari kata:
   a. emergency
   b. electronic
   c. enteprise
   d. escalation
2. Dalam konsep Cyber Six, fenomena antara Cyber Attack dan Cyber Crime adalah:
   a. Cyber Security
   b. Cyber Law
   c. Cyber Threat
   d. Cyber Space
3. Standar kemanan informasi yang dikeluarkan oleh standar internasional adalah:
   a. ISO 27001
   b. ISO 38500
   c. ISO 20000
   d. ISO 31000
4. Yang dianggap sebagai tipe serangan pertama kali adalah:
   a. password guessing,
   b. password cracking
   c. hijacking sessions
   d. sniffers

5. Contoh serangan yang termasuk kategori fabrication adalah:
   a. phishing
   b. web defacement
   c. DDOS
   d. Sniffing
6. Undang-Undang mengenai Informasi dan Transaksi Elektronik di Indonesia adalah:
   a. UU no.11 tahun 2008
   b. UU no.11 tahun 2011
   c. UU no.11 tahun 2005
   d. UU no.11 tahun 2014
7. Asosiasi penyelenggara jasa internet yang ada di Indonesia bernama:
   a. APJII
   b. APWARI
   c. ASPILUKI,
   d. APKOMINDO
8. Filosofi 3D dalam CERT/CSIRT adalah:
   a. Discover-Determine-Defend
   b. Determine-Defend-Discover
   c. Discover-Defend-Determine
   d. Determine-Discover-Defend
9. Aplikasi atau software jahat disebut sebagai:
   a. malware
   b. virusware
   c. zipware
   d. badware
10. Yang termasuk dalam domain aspek teknis pengamanan internet adalah:
    a. antispyware
    b. IT audit
    c. ISO compliance
    d. reward-punishment
11. Yang bukan termasuk dalam domain aspek bisnis pengamanan internet adalah:
    a. software patches
    b. backup management
    c. business contingency plan
    d. security management

12. Organisasi komunitas CERT yang beroperasi di wilayah Asia Pasifik adalah:
    a. APCERT
    b. ACERT
    c. AsiaCERT
    d. PacificCERT
13. Menurut EC-Council, hacker dalam melakukan aktivitas penyerangan melalui:
    a. lima tahap
    b. empat tahap
    c. enam tahap
    d. tujuh tahap
14. Strategi mencari informasi sebelum melakukan penyerangan disebut sebagai:
    a. reconnaissance
    b. resonance
    c. scanning
    d. spidering
15. Individu yang kerap melakukan aktivitas ofensif maupun defensif di dunia maya disebut sebagai:
    a. gray hats
    b. black hats
    c. white hats
    d. suicide hacks
16. Jenis virus yang merupakan penggalan program untuk menggantikan program utama atau host disebut sebagai:
    a. overwriting virus
    b. prepending virus
    c. appending virus
    d. infector virus
17. FTP Trojan bekerja dengan memanfaatkan:
    a. port 21
    b. port 80
    c. port 20
    d. port 81
18. Fungsi yang berperan sebagai single point of contact dalam sebuah CERT disebut sebagai:
    a. triage
    b. handling
    c. feedback
    d. reporter

19. Lembaga nasional di Indonesia yang bertanggung jawab untuk mengembangkan teknik kriptologi adalah:
    a. Lemsaneg
    b. Lemhannas
    c. ID-SIRTII
    d. Kemkominfo
20. Yang bukan merupakan aplikasi untuk kebutuhan surface analysis adalah:
    a. SourceFire
    b. HashTab
    c. TrID
    d. 7zip
21. Yang bukan merupakan aplikasi virtualisasi adalah:
    a. CFF Explorer
    b. VirtualBoz
    c. VMWare
    d. VirtualPC
22. ISO 27001 merupakan pengembangan dari:
    a. ISO 17799
    b. ISO 20000
    c. ISO 30000
    d. ISO 38500
23. Menurut EC-Council elemen kunci yang harus diperhatikan dalam menyusun kebijakan keamanan ada:
    a. tujuh
    b. enam
    c. delapan
    d. lima
24. Uji ketangguhan terhadap sebuah sistem dinamakan sebagai:
    a. penetration test
    b. vulnerability analysis
    c. social engineering
    d. security spidering
25. Dalam 14 tahapan forensik, hal keempat yang harus dilakukan adalah:
    a. pelaksanaan prosedur tanggapan dini
    b. pembekuan barang bukti
    c. pengumpulan bukti awal
    d. pemindahan bukti ke laboratorium forensik

Tugas 1

Carilah tiga contoh serangan dunia siber (internet) yang secara masif menimpa tiga buah negara yang pernah terjadi, dan jawablah pertanyaan berikut:

A. Apakah nama serangan atau kasus dimaksud?
B. Mengapa serangan tersebut dapat terjadi?
C. Bagaimana serangan tersebut dilakukan?
D. Kerugian apa yang dialami oleh negara terkait?
E. Siapakah yang disinyalir melakukan serangan tersebut?

Tugas 2

Jelaskan bagaimana situs-situs di bawah ini mengembangkan dan menerapkan sistem keamanannya:

A. Bhinneka.com
B. Lazada.co.id
C. Facebook.com
D. OLX.co.id
E. Foodpanda.co.id

Ujian Tengah Semester

1. Mengapa negara-negara mendirikan CERT-nya masing-masing? Apakah alasan utama di balik strategi ini?
2. Apakah perbedaan antara cyber threat dan cyber attack? Mengapa perlu memahami secara sungguh-sungguh perbedaan dari kedua aspek ini?
3. Apakah yang dimaksud dengan hactivism? Mengapa gerakan ini begitu masif mengemuka di dunia internet?
4. Siapakah yang bertanggung jawab dalam merencanakan dan mengelola aspek keamanan informasi dalam sebuah organisasi? Apa alasannya?
5. Komponen keamanan apa saja yang harus diperhatikan agar dibangun sistem yang kuat dan efektif? Mengapa komponen tersebut dianggap penting? Apa alasannya?

Ujian Akhir Semester

1. Apakah yang dimaksud dengan social engineering? Bagaimana cara efektif mencegah terjadinya serangan jenis ini?
2. Jelaskan secara ringkas apa yang dimaksud dengan jenis serangan sebagai berikut: (i) phishing; (ii) botnet; (iii) web defacement; dan (iv) denial of services.

3. Apakah yang dimaksud dengan permissive policy, primiscuous policy, dan prudent policy?
4. Aspek apakah yang sebenarnya dilindungi dengan diterapkannya konsep kriptografi? Bagaimana cara kerjanya?
5. Apakah yang dimaksud dengan forensik komputer? Bagaimana langkah-langkah metodologis aktivitas ini dilakukan?

-oo0oo-

DAFTAR PUSTAKA

Calder, Alan, and Steve Watkins. (2006). *International IT Governance: An Executive Guide to ISO-17799/ISO-27001.* Kogan Page: United Kingdom.

Cappelli, Dawn M., Andrew P. Moore, and Randall F. Trzeciak. (2012). *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes.*

EC-Council. (2009). *Ethical Hacking and Countermeasures: Attack Phases – EC-Council Certified Ethical Hacker (CEH).* Cengage Learning: United States.

Engebretson, Patrick. (2013). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier: Massachusetts, United States.

Gartner. (2001). *Gartner's Information Security Strategies Research Note TU-14-5662.*

Hadnagy, Christopher, and Paul Wilson. (2010). *Social Engineering: The Art of Human Hacking.* Wiley: United States.

ISACA. (2007). *Control Objectives for Information and Related Technology – version 4.1.* ISACA Publisher: United States.

Kennedy, David, Jim O'Gorman, Devon Kearns, and Mati Aharoni. (2011). *Metasploit: The Penetration Tester's Guid*e. No Starch Press: United States.

McClure, Stuart, *Joel Scambray and George Kurtz.* (2005). Hacking Exposed Fifth Edition. New York: McGraw-Hill.

Mitnick, Kevin D. (2003). *The Art of Deception: Controlling the Human Element of Security.* Wiley: United States.

Mulligan, Deirdre K. and Fred B. Schneider. (2011). *Doctrine for Cyber Security. Dædalus, the Journal of the American Academy of Arts & Sciences 140 (4) Fall Edition.* UC Berkeley School of Information, California, United States.

Pfleeger, Charles. (2003). *Security in Computing*. New York: Pearson Education.

Sikorski, Michael, and Andrew Honig. (2012). *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software.* No Stratch Press: United States.

Simpson, M. T. (2013). *Hands-on ethical hacking and network defense*. Boston, MA, Course Technology.

Speed, T. J. (2012). *Asset protection through security awareness*. Boca Raton, FL, CRC Press.

Weingarten, F.W. (1989). *Federal Information Policy Development: The Congressional Perspective.* In C. McClure, P. Hernon and H. Relyea (eds), United States Government Information Policies: views and Perspectives - Ablex, Norwood, NJ.

-oo0oo-

TENTANG PENULIS

Richardus Eko Indrajit, guru besar ilmu komputer ABFI Institute Perbanas, dilahirkan di Jakarta pada tanggal 24 Januari 1969. Menyelesaikan studi program Sarjana Teknik Komputer dari Institut Teknologi Sepuluh Nopember (ITS) Surabaya dengan predikat Cum Laude, sebelum akhirnya menerima bea siswa dari Konsorsium Production Sharing Pertamina untuk melanjutkan studi di Amerika Serikat, dimana yang bersangkutan berhasil mendapatkan gelar Master of Science di bidang Applied Computer Science dari Harvard University (Massachusetts, USA) dengan fokus studi di bidang artificial intelligence. Adapun gelar Doctor of Business Administration diperolehnya dari University of the City of Manyla (Intramuros, Phillipines) dengan disertasi di bidang Manajemen Sistem Informasi Rumah Sakit. Gelar akademis lain yang berhasil diraihnya adalah Master of Business Administration dari Leicester University (Leicester City, UK), Master of Arts dari the London School of Public Relations (Jakarta, Indonesia) dan Master of Philosophy dari Maastricht School of Management (Maastricht, the Netherlands). Selain itu, aktif pula berpartisipasi dalam berbagai program akademis maupun sertifikasi di sejumlah perguruan tinggi terkemuka dunia, seperti: Massachusetts Institute of Technology (MIT), Stanford University, Boston University, George Washington University, Carnegie-Mellon University, Curtin University of Technology, Monash University, Edith-Cowan University, dan Cambridge University. Saat ini menjabat sebagai Ketua Umum Asosiasi Perguruan Tinggi Informatika dan Komputer (APTIKOM) se-Indonesia dan Chairman dari International Association of Software Architect (IASA) untuk Indonesian Chapter. Selain di bidang akademik, karir profesionalnya sebagai konsultan sistem dan teknologi informasi diawali dari Price Waterhouse Indonesia, yang diikuti dengan berperan aktif sebagai konsultan senior maupun manajemen pada sejumlah perusahaan terkemuka di tanah air, antara lain: Renaissance Indonesia, Prosys Bangun Nusantara, Plasmedia, the

Prime Consulting, the Jakarta Consulting Group, Soedarpo Informatika Group, dan IndoConsult Utama. Selama kurang lebih 15 tahun berkiprah di sektor swasta, terlibat langsung dalam berbagai proyek di beragam industri, seperti: bank dan keuangan, kesehatan, manufaktur, retail dan distribusi, transportasi, media, infrastruktur, pendidikan, telekomunikasi, pariwisata, dan jasa-jasa lainnya. Sementara itu, aktif pula membantu pemerintah dalam sejumlah penugasan. Dimulai dari penunjukan sebagai Widya Iswara Lembaga Ketahanan Nasional (Lemhannas), yang diikuti dengan beeperan sebagai Staf Khusus Bidang Teknologi Informasi Sekretaris Jendral Badan Pemeriksa Keuangan (BPK), Staf Khusus Balitbang Departemen Komunikasi dan Informatika, Staf Khusus Bidang Teknologi Informasi Badan Narkotika Nasional, dan Konsultan Ahli Direktorat Teknologi Informasi dan Unit Khusus Manajemen Informasi Bank Indonesia. Saat ini ditunjuk oleh pemerintah Republik Indonesia untuk menakhodai institusi pengawas internet Indonesia ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure). Seluruh pengalaman yang diperolehnya selama aktif mengajar sebagai akademisi, terlibat di dunia swasta, dan menjalani tugas pemerintahan dituliskan dalam sejumlah publikasi. Hingga menjelang akhir tahun 2008, telah lebih dari 25 buku hasil karyanya yang telah diterbitkan secara nasional dan menjadi referensi berbagai institusi pendidikan, sektor swasta, dan badan pemerintahan di Indonesia – diluar beragam artikel dan jurnal ilmiah yang telah ditulis untuk komunitas nasional, regional, dan internasional. Seluruh karyanya ini dapat dengan mudah diperoleh melalui situs pribadi http://www.eko-indrajit.com. Sehari-hari dapat dihubungi melalui nomor telepon 0818-925-926 atau email indrajit@post.harvard.edu.

-oo0oo-