



Mata Ajar

MANAJEMEN KEAMANAN INFORMASI DAN INTERNET

Topik Bahasan

PERMASALAHAN MENDASAR KEAMANAN INTERNET

Versi

2013/1.0

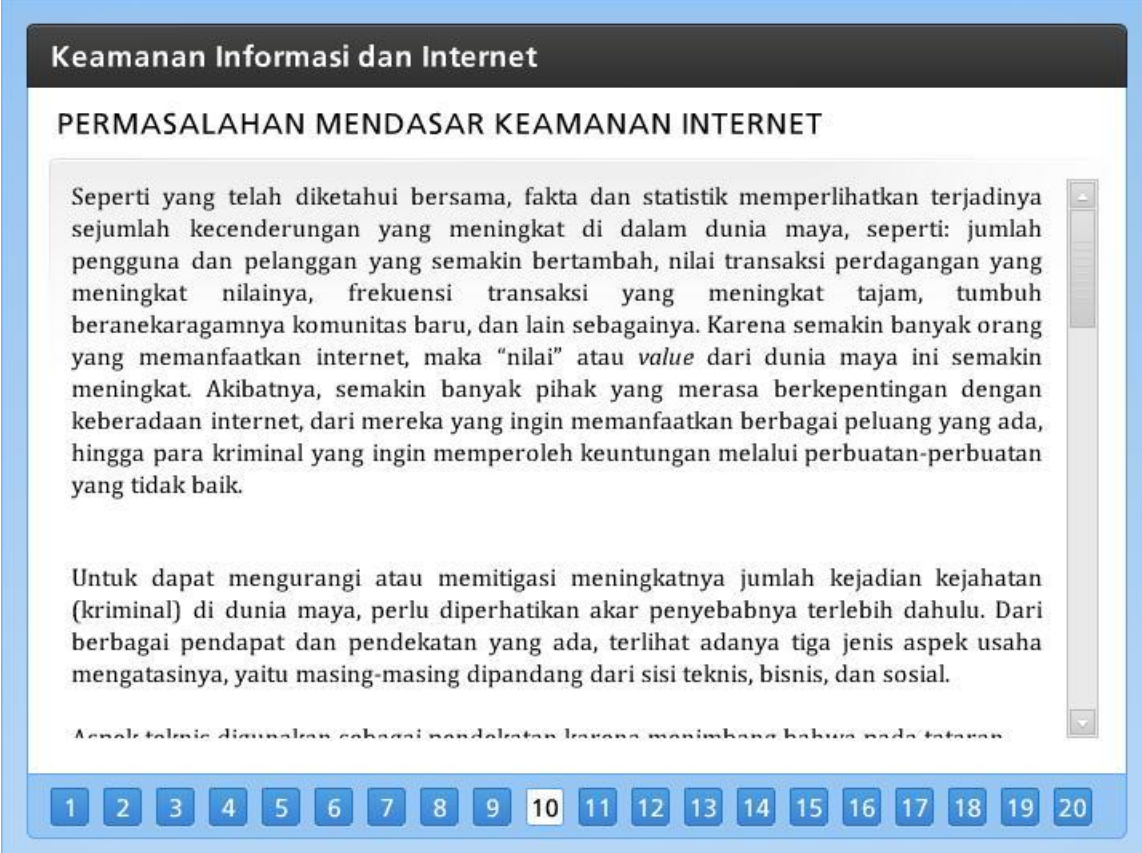
Nama File

MKIDI-2A-PermasalahanMendasar.pdf

Referensi Pembelajaran

2-A

PERMASALAHAN MENDASAR KEAMANAN INTERNET



Keamanan Informasi dan Internet

PERMASALAHAN MENDASAR KEAMANAN INTERNET

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.

Untuk dapat mengurangi atau memitigasi meningkatnya jumlah kejadian kejahatan (kriminal) di dunia maya, perlu diperhatikan akar penyebabnya terlebih dahulu. 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

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

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.

Untuk dapat mengurangi atau memitigasi meningkatnya jumlah kejadian kejahatan (kriminal) di dunia maya, perlu diperhatikan akar penyebabnya terlebih dahulu. 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 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.

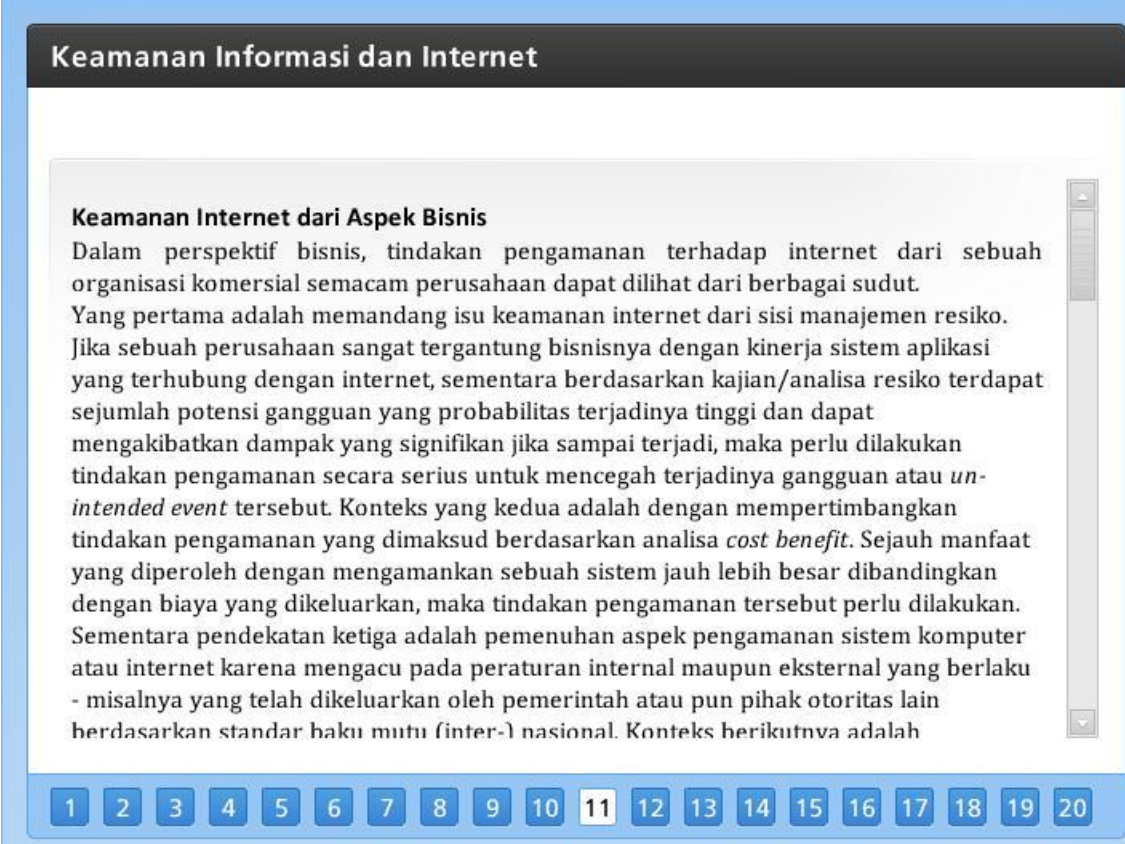
Di satu sisi ada perusahaan yang jika internetnya tidak jalan akan menimbulkan kerugian yang luar biasa, sementara di pihak lain ada organisasi yang tanpa internet masih dapat berjalan dengan baik. Sehingga kebutuhan untuk mengamankan internet harus dipandang dari sisi ini. Sementara itu aspek sosial 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.

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.

Misalnya adalah instalasi *firewalls* untuk melindungi 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.



Keamanan Informasi dan Internet

Keamanan Internet dari Aspek Bisnis

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

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Keamanan Internet dari Aspek Bisnis

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

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 keamanannya, maka dibuatlah SOP yang harus ditaati dalam kegiatan operasional sehari-hari.

Keamanan Internet dari Aspek Sosial

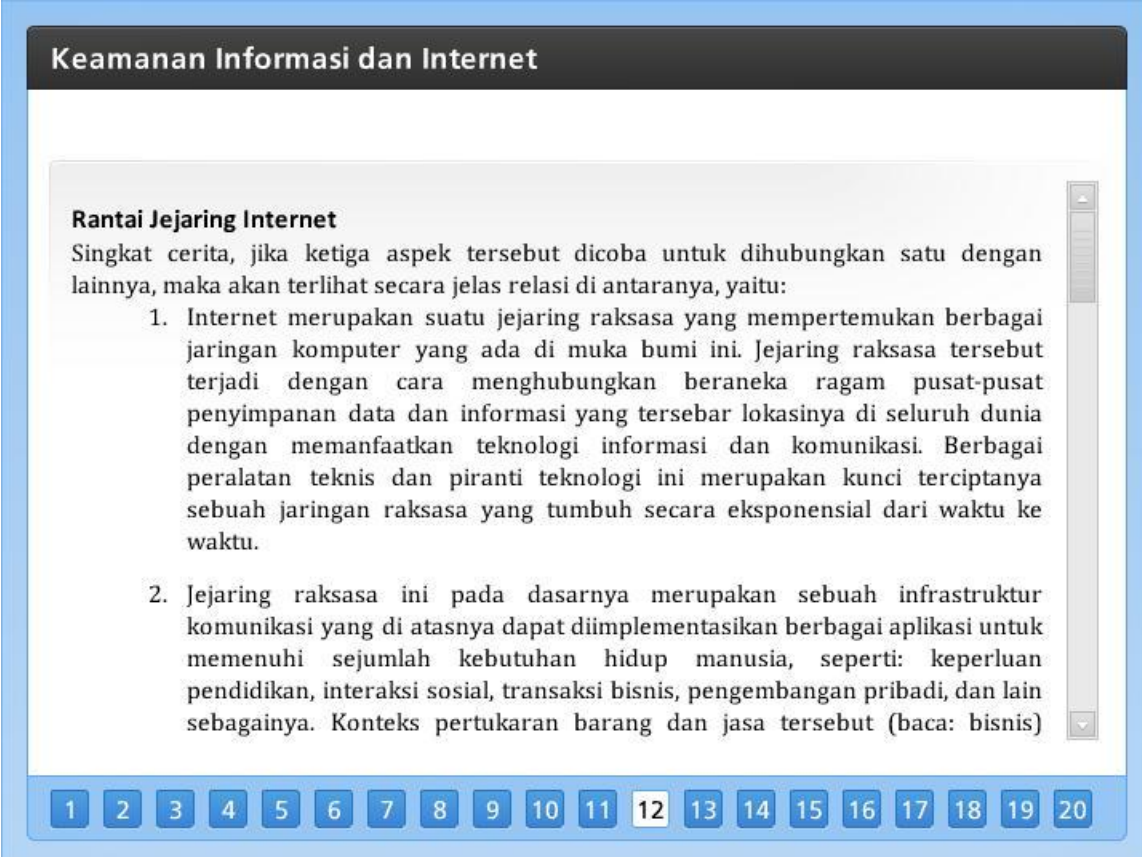
Sifat dan karakteristik manusia sangat dipengaruhi oleh keadaan lingkungan di sekitarnya. Dalam jaman moderen ini, dimana teknologi informasi dan komunikasi telah merasuki seluruh aspek kegiatan dan kehidupan manusia, para generasi muda semakin akrab dengan keberadaan

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 arusny 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.



Keamanan Informasi dan Internet

Rantai Jejaring Internet

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

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)

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Rantai Jejaring Internet

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

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.

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 *firewall* dalam sebuah organisasi tanpa diiringi dengan perilaku/budaya pengamanan oleh seluruh pengguna sistem maupun kualitas keamanan seluruh aplikasi yang dipergunakan.

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:

- 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.
- 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*).

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.