Modul

01

MSIM4405
Edisi 1

Pengantar Keamanan Sistem Informasi

Indri Sulistyowati, S.Kom., M.MT.

Daftar Isi Modul

Pendahuluan

Setelah mempelajari modul ini Anda diharapkan akan dapat memahami tentang pengertian dan masalah keamanan sistem informasi. Anda dapat menjelaskan tujuan keamanan sistem informasi dan permasalahan yang sering terjadi serta bagaimana menyikapinya.

Secara lebih rinci Anda diharapkan dapat melakukan hal-hal berikut:

1. menjelaskan berbagai contoh permasalahan dalam sistem keamanan informasi;
2. menguraikan penanggung jawab Keamanan Sistem Informasi beserta perannya;
3. menjelaskan tentang *Zero-day-attack* sebagai masalah utama dalam keamanan SI;
4. menguraikan tentang tindakan umum untuk penyelesaian masalah *Zero-day-attack*;
5. menguraikan jenis-jenis kerawanan sistem keamanan yang sering di jumpai;
6. menjelaskan Pengertian Keamanan Sistem Informasi;
7. menjelaskan Tujuan Keamanan Sistem Informasi;
8. menjelaskan Aset Keamanan Informasi;
9. menjelaskan Risiko Keamanan Informasi;
10. menjelaskan Evaluasi Keamanan Informasi.

Kegiatan Belajar 1

Pengenalan Masalah Keamanan Sistem Informasi

Organisasi terkadang memiliki pemahaman yang keliru tentang keamanan informasi yang telah diterapkan di dalam organisasinya. Mereka merasa aman apabila komputer dalam organisasi tersebut telah terinstal anti virus. Padahal kenyataannya tidak demikian karena hampir semua komputer terkoneksi ke jaringan internet setiap harinya. Berbagai macam gangguan dapat terjadi di jaringan seperti Windows yang memiliki *bugs* yang selalu ditemukan dari waktu ke waktu (Linux juga memiliki sejumlah *bug* sendiri). *Bugs*/kelemahan tersebut kemudian dieksploitasi dengan cepat oleh *malware* dan langsung menyebar ke seluruh jaringan yang saling terkait. Kadang kala ditemukan satu-dua jenis kerentanan yang tidak memerlukan tindakan apapun dari pengguna.

Beberapa jenis serangan dapat dihentikan cara menggunakan *firewall* dengan konfigurasi yang benar atau menerapkan *patch*. Pernyataan "*firewall* yang dikonfigurasi dengan benar" merupakan kata kunci sebab *firewall* yang dikonfigurasi dengan buruk kurang dapat memberikan perlindungan atau bahkan sama sekali tidak memberikan perlindungan pada sistem komputer yang ada di jaringan kita. Namun, *firewall* itu sendiri juga memiliki *bug* tersendiri, mereka dapat menjadi *vulnerable*; solusi terbaik untuk melindungi *firewall* adalah dengan melakukan *update* pada *software firewall* yang kita gunakan sesegera mungkin setelah mendapatkan informasi tentang *vunerability* baru dari *firewall* yang kita pakai.

Beberapa orang berasumsi bahwa dengan melakukan *update operating system* (OS), antivirus, *firewall* dan *software* lain, maka berarti bahwa mereka 100% aman. Pada subyek bahasan kita "tidak ada keamanan 100% selamanya". Hanya mesin yang tidak terkoneksi dengan *network* yang 100% aman dan *lock down* secara fisik dan tentu saja tidak digunakan. Katakanlah Anda telah melakukan *update* anti virus secara otomatis setiap 24 jam. Kemudian, misalkan pada saat setelah melakukan *update*, suatu virus baru yang tidak dikenal oleh anti virus yang telah Anda instal mulai menyebar ke *network*, ini berarti fasilitas komputer Anda berisiko kena virus selama 24 jam ke depan.

Terkadang terdapat persepsi bahwa ancaman terbesar organisasi berasal dari luar organisasi, mungkin dari organisasi pesaing atau personal tidak menyukai organisasi kita. Namun kita terkadang juga lupa bahwa dalam organisasi tersebut terdapat karyawan yang bekerja untuk organisasi. Apabila terdapat karyawan yang sakit hati karena perlakuan yang dirasa tidak adil dari manajemen seperti rotasi pegawai, pegawai yang mengundurkan diri, pemecatan pegawai, atau bahkan mungkin karena sakit hati

oleh tindakan sesama karyawan; segala hal tersebut dapat menyebabkan munculnya ancaman pada keamanan sistem informasi. Ancaman tersebut bisa berbentuk penyebaran informasi rahasia kepada pihak yang tidak berwenang baik itu di dalam organisasi maupun diluar organisasi. Oleh karenanya diperlukan tindakan pendataan asset yang dipegang oleh masing-masing pegawai; dan hak akses apa saja yang dimiliki oleh masing-masing pegawai. Semua hal tersebut harus diatur dalam suatu mekanisme pengembalian ke perusahaan pada saat seorang pegawai mengalami rotasi, mengundurkan diri, pensiun, dan lain-lain terkait dengan peraturan kepegawaian.

Kesalahan dalam proses rekrutmen pegawai yang dilakukan tanpa adanya *screening* dan pengecekan latar belakang pegawai juga dapat menyebabkan insiden timbulnya ancaman terhadap keamanan informasi seperti terjadinya tindakan kriminal, pencurian data/aset, dan lain sebagainya. Tindakan pengambilan "Tanda tangan *Non disclosure agreement* (NDA)" sangat diperlukan pada masing-masing pegawai baru, selain mereka juga harus menandatangani kontrak kerja.

Catatan:

***Non-Disclosure Agreement* (NDA)** adalah perjanjian kerahasiaan antara dua pihak untuk menjaga kerahasiaan informasi dan atau material tertentu yang mereka bagi bersama akses/informasinya, namun tidak diizinkan diketahui pihak diluar mereka (pihak ketiga).

NDA (*Non Disclosure Agreement*) merupakan suatu kontrak dalam hubungan kerja profesional yang mengikat secara hukum dan bersifat konfidensial. Beberapa perusahaan mengenal arti NDA dengan istilah perjanjian rahasia.

Perjanjian antara kedua pihak ini tidak boleh disebarluaskan isinya. Bahkan, ketika kedua pihak tersebut sudah tidak bekerja sama lagi, tetap dilarang untuk menyebarkan informasi pada perjanjian tersebut.

Cara ini kerap digunakan oleh perusahaan untuk melindungi informasi yang perlu dijaga kerahasiaannya. Umumnya, hal ini menyangkut dengan prosedur kerja, tata cara kerja, dan kebijakan privasi perusahaan lainnya.

Apabila terdapat kebocoran informasi yang disebabkan oleh suatu pihak, maka perusahaan dapat menuntut dan membawanya ke jalur hukum.

Silahkan Anda pertimbangkan skenario berikut ini:

Seorang mantan administrator jaringan di suatu pabrik berpikir bahwa dia telah menghancurkan tidak hanya kemampuan manufaktur mantan atasannya, tetapi juga bukti yang akan menghubungkannya dengan kejahatan tersebut.

Karyawan tersebut sudah 11 tahun terpercaya membangun dan memelihara jaringan di perusahaan. Ketika dia jatuh dari kejayaan perusahaan dan tahu dia akan dipecat karena masalah kinerja dan perilaku, dia membuat bom waktu perangkat lunak untuk menghancurkan sistem.

Tiga minggu setelah administrator jaringan dipecat, seorang pekerja pabrik memulai hari dengan masuk ke *server file* pusat. Alih-alih melakukan *booting*, sebuah pesan muncul di layar yang mengatakan bahwa area sistem operasi sedang diperbaiki. Kemudian *server* macet, dan dalam sekejap, semua dari 1.000 program *tools* dan manufaktur pabrik hilang. *Server* tidak dapat diaktifkan kembali. Manajer pabrik memerintahkan agar mesin manufaktur tetap berjalan dengan rangkaian program sebelumnya. Tidak ada masalah jika pesanan sudah dipenuhi. Namun karena harus menjaga agar mesin tetap berjalan, kemudian manajer pabrik pergi untuk mendapatkan solusi dari masalah yang dia hadapi, melihat *backup* cadangan yang disimpan di lemari arsip di departemen sumber daya manusia. Tapi *tape backup* sudah hilang. Dia kemudian beralih ke *workstation* yang terhubung ke *file server*. Program, setidaknya sebagian besar, harus disimpan secara lokal di masing-masing *workstation*. Namun program yang diperlukan juga tidak dapat ditemukan.

Administrator jaringan yang dipecat, adalah merupakan satu-satunya karyawan yang bertanggung jawab untuk memelihara, mengamankan, dan mem*backup server file*, sebelum dia diganti.

Pada hari-hari setelah kecelakaan itu, perusahaan memanggil tiga orang yang berbeda untuk mencoba pemulihan data. Lima hari setelah kecelakaan, manajer pabrik mulai memindahkan pekerja di sekitar departemen dan mematikan mesin yang kehabisan bahan mentah atau membuat persediaan berlebih. Dia mengambil langkah-langkah untuk menyewa tim *programmer* untuk mulai membangun kembali sekitar 1.000 program yang hilang.

Kepala keuangan perusahaan bersaksi bahwa bom perangkat lunak menghancurkan semua program dan *generator code* yang memungkinkan perusahaan untuk membuat 25.000 produk berbeda dan menyesuaikan produk dasar tersebut menjadi sebanyak 500.000 desain berbeda. Perusahaan kehilangan keuntungan keduanya karena dapat memodifikasi produk dengan mudah dan memproduksinya dengan murah. Perusahaan tersebut mengalami kerugian lebih dari $10 juta, kehilangan posisinya di kancah industri, dan akhirnya harus memberhentikan 80 karyawan.

Dari skenario tersebut kita bisa melihat bahwa, hanya karena satu perbuatan karyawan yang tidak suka dengan perusahaan, perusahaan dapat merugi dengan cukup besar, dan banyak karyawan lain yang tidak bersalah harus diberhentikan karena perusahaan harus menghemat biaya operasional, dan mempertahankan kembali bisnisnya agar tetap berjalan.

Keamanan informasi itu bukan hanya tanggung jawab dari tim teknologi informasi (TI), namun merupakan tanggung jawab semua pihak dalam organisasi. Keamanan informasi tidak hanya merupakan keamanan pada aspek teknologi informasi; salah satu

contohnya adalah keamanan fisik atas sarana TI. Keamanan fisik bukan hanya tanggung jawab tim TI, namun keamanan fisik juga merupakan salah satu bagian dari sistem manajemen keamanan informasi. Apabila ada salah satu asset penting organisasi hilang akibat pencurian atau kerusakan, dan ternyata di dalam asset tersebut terdapat informasi rahasia atau merupakan penunjang utama untuk bisnis organisasi maka keadaan tersebut juga dapat merugikan bisnis organisasi. Pihak manajemen juga bertanggungjawab terhadap sistem manajemen keamanan informasi yang harus diterapkan di dalam suatu organisasi.

Kesadaran terhadap keamanan informasi harus dibangun menjadi budaya organisasi, karena keamanan informasi merupakan tanggung jawab bersama semua pihak yang ada dalam organisasi tersebut. Kesadaran/*awareness* merupakan titik awal bagi seluruh pegawai dalam organisasi untuk dapat memahami pengetahuan mengenai tentang keamanan teknologi informasi.

Sebagai contoh lainnya, situs web dari organisasi yang tidak pernah di bobol oleh *hacker*; apabila organisasi menganggap bahwa hal tersebut merupakan parameter untuk menilai keamanan sistem informasi; dan anggota organisasi menjadi lengah sehingga tidak melakukan *update* terhadap sistem tersebut, maka kejadian ini merupakan tindakan yang tidak dapat dibenarkan.

Kerentanan yang ada terus berkembang dan terjadi seiring dengan perkembangan teknologi; dan juga seiring dengan kemampuan *hacker* dalam meningkatkan kemampuan diri untuk melakukan tindakan *hacking*, selain juga dengan makin majunya sarana dan prasarana yang mungkin dapat digunakan untuk melakukan tindakan yang bersifat destruktif. Mungkin hari ini website kita aman, tetapi belum tentu besok masih tetap aman.

A. SIAPAKAH YANG BERTANGGUNG JAWAB TERHADAP SISTEM MANAJEMEN KEAMANAN INFORMASI

Pada bagian ini akan kita bahas siapa saja yang bertanggung jawab terhadap keamanan sistem informasi suatu organisasi atau perusahaan. Berikut ini adalah suatu ilustrasi untuk memahami cara organisasi membagi peran dan tanggung jawab terhadap keamanan informasi.

1. Pada bagian *back-end* pada suatu organisasi harus memiliki strategi sistem pertahanan dalam membangun sistem manajemen keamanan informasi sehingga tidak mudah di bobol oleh *attacker* atau *hacker*. Bagian *back end* ini terdiri dari sysadmin, *network*, *database administrator* (DBA), *firewall,* dan lain-lain.
2. Pada bagian operasional yang bertanggungjawab untuk menjalankan operasional bisnis perusahaan sehari-hari, menilai risiko organisasi, mitigasi risiko. Mereka harus menyadari dan memahami strategi dan penerapan sistem manajemen keamanan informasi yang telah menjadi komitmen organisasi, bagian operasional ini terdiri dari *compliancy*, *informations security officer, risk management officer*, dan lain-lain.

3. Sebagai garda terdepan adalah *helpdesk* yang juga memiliki peran penting dalam implementasi sistem manajemen keamanan informasi, terutama dalam menyampaikan informasi kepada *user* pada saat *user* menyampaikan keluhan (*complaint*). *Helpdesk* harus mematuhi *Standart Operasional Prosedure* (SOP) dalam menangani keluhan dan juga harus mengetahui tentang klasifikasi informasi yang dapat disampaikan kepada *user* : (a) apakah informasi tersebut untuk umum, (b) untuk internal organisasi, atau (c) untuk kalangan tertentu organisasi.
4. Selain *helpdesk* di bagian depan terdapat penguji sistem (*system tester*) yang bertugas untuk melakukan *scanning vulnerability* yang ada pada *network* dan aplikasi yang dimiliki organisasi, sehingga bisa dilakukan rencana mitigasi risiko terkait dengan *vulnerability* yang ditemukan.
5. Sedangkan TOP manajemen adalah merupakan bagian yang mengarahkan semua tim dalam organisasi untuk mencapai tujuan dalam penerapan sistem manajemen keamanan informasi, membuat kebijakan tentang sistem manajemen keamanan informasi, memasukkan aspek keamanan informasi dalam rencana strategi organisasi, dan lain sebagainya.
6. *Stakeholder* juga memiliki peran penting dalam mengimplementasikan sistem manajemen keamanan informasi. *Stakeholder* biasanya merupakan pihak yang paling jeli dalam melihat celah dari sistem manajemen keamanan informasi yang sudah dibangun oleh organisasi. Kemudian *stakeholder* dapat memberikan informasi tentang hal tersebut pada bagian yang bertanggungjawab atas keamanan informasi organisasi. Celah yang dimaksud bukan hanya sekedar yang ada pada sistem aplikasi atau sistem *network*; bisa jadi celah yang terjadi terdapat pada manajemen organisasi atau bahkan tata kelola yang dimiliki organisasi. Untuk mengimplementasikan sistem manajemen keamanan informasi, organisasi dapat mengadopsi salah satu internasional standar yang ada seperti ISO 27001:2013, COBIT, PCI DSS (*Payment Card Industry Data Security Standard*) dan lain sebagainya.

Di lansir dari laman web https://cyberthreat.id tentang kasus peretasan data terbesar dalam sejarah. Pada situs tersebut tertera setidaknya terdapat 10 kasus peretasan data yang melibatkan milyaran data pribadi penduduk yang ada di muka bumi ini.

Berikut ini adalah contoh kasus peretasan data terbesar dalam sejarah, berapa banyak pengguna yang terdampak, siapa yang bertanggung jawab, dan bagaimana perusahaan merespons.

1. Yahoo

Tanggal: 2013-2014

Dampak: 3 miliar akun pengguna

Yahoo mengumumkan pada September 2016 bahwa pada tahun 2014 telah menjadi korban peretasan data terbesar yang pernah ada. Para penyerang, yang oleh perusahaan diyakini sebagai "*hacker* yang disponsori negara", meretas data pengguna

Yahoo berupa nama asli, alamat *email*, tanggal lahir dan nomor telepon dari 500 juta pengguna. Yahoo mengklaim bahwa sebagian besar kata sandi yang dicuri dilindungi oleh teknologi hash.

Pada Desember 2016, Yahoo mengungkapkan pelanggaran lain telah terjadi dari tahun 2013 oleh penyerang berbeda yang membahayakan nama, tanggal lahir, alamat *email* dan kata sandi (*password* pengguna), serta pertanyaan dan jawaban keamanan 1 miliar akun pengguna. Yahoo merevisi perkiraan itu pada Oktober 2017 untuk memasukkan semua 3 miliar akun penggunanya.

Saat pengumuman peretasan data itu, Yahoo sedang dalam proses akuisisi oleh Verizon, yang akhirnya membayar US$4,48 miliar untuk bisnis internet inti Yahoo. Pelanggaran itu menghancurkan nilai perusahaan.

Akibat peretasan data itu, Yahoo digugat *class action* karena dianggap lalai melindungi data konsumen. Pada Oktober 2019, Yahoo mengumumkan mengalokasikan dana Rp1,65 triliun untuk ganti rugi kepada pengguna yang terdampak. Yahoo menawarkan uang pengganti hingga US$358 per akun atau setara Rp 5 juta (asumsi US$1 = Rp 14.000) kepada pengguna Yahoo yang *email*nya diretas oleh *hacker*.

Sedangkan kasus yang baru-baru ini terjadi adalah upaya peretasan situs *e-commerce* ternama di Indonesia. Situs *e-commerce* merupakan situs favorit yang paling banyak diretas oleh *hacker* untuk mendapatkan keuntungan finansial dari situs tersebut, salah satunya mencuri data bank pengguna, atau user dan password pengguna, dll. Berdasarkan berita yang dilansir oleh situs web https://www.kompas.com, sebagaimana diuraikan di bawah ini:

2. Tokopedia

Sebelumnya, kabar ini beredar di media sosial, salah satunya diunggah oleh akun Twitter @underthebreach, yang mengatakan bahwa ada sekitar 15 juta pengguna Tokopedia yang datanya telah diambil. Menurut akun tersebut, data yang telah diambil dari akun di antaranya berisi *e-mail, hash password,* dan nama pengguna. Hingga Minggu (3/5/2020) pukul 14.30 WIB, *tweet* tersebut telah memperoleh 10,6 ribu *likes* dan 12,2 ribu *retweet*. Menanggapi hal tersebut, Tokopedia membenarkan adanya upaya peretasan data milik pengguna. Akan tetapi, pihak Tokopedia mengklaim bahwa informasi miliki pengguna tetap aman dan terlindungi.

Dari berbagai contoh insiden keamanan informasi diatas, dimana situs *website* perusahaan dibobol oleh *hacker* dan data yang dapat dicuri, kita bisa melihat bahwa setiap perusahaan perlu memiliki strategi untuk membangun sistem manajemen keamanan informasi dan harus selalu direviu dan di*update* sesuai dengan perkembangan teknologi saat itu.

Respons perusahaan yang cepat dan akurat juga berpengaruh penting terhadap keberlangsungan bisnis perusahaan, sehingga *customer* tidak meninggalkan perusahaan dan beralih ke perusahaan pesaing; karena pihak manajemen mampu mempertahankan kepercayaan *customer* meskipun telah terjadi insiden keamanan informasi. Pihak manajemen juga harus menjaga agar insiden yang terjadi tidak akan terjadi lagi

sehingga menumpuk dan akhirnya berubah menjadi problem besar yang membebani perusahaan. Tidak hanya respons terhadap *customer* yang perlu diperhatikan, tetapi rencana untuk menangani insiden secara jangka pendek dan jangka panjang perlu dibuat dan diimplementasikan sesuai jadwal dan prosedur yang telah ditetapkan.

B. *ZERO DAY ATTACK*

Salah satu dari berbagai pelanggaran keamanan informasi yang sering terjadi, selain peretasan pada situs *website* perusahaan, adalah eksploitasi kelemahan/kekurangan yang terjadi pada *software* atau *operating system* (OS), keadaan ini sering dikenal/disebut sebagai *Zero Day Attack*. Eksploitasi *zero-day* merupakan serangan di dunia maya yang terjadi pada hari yang sama pada saat pertama kali ditemukannya kelemahan pada suatu *software* atau sistem operasi (OS). Pada titik itu, mulai terjadi eksploitasi atas kekurangan tersebut sebab belum dilakukan perbaikan *software/OS* oleh pembuatnya. Pada awalnya, ketika seorang pengguna menemukan bahwa adanya risiko keamanan atas suatu program; mereka kemudian melaporkannya ke perusahaan *software* terkait; perusahaan tersebut kemudian akan mengembangkan suatu *patch* keamanan untuk memperbaiki kekurangan tersebut. Pengguna yang menemukan kekurangan tersebut juga akan menggunakan fasilitas internet untuk memperingatkan orang lain atas kekurangan yang ditemukannya. Pada umumnya pembuat program dapat melakukan perbaikan secara cepat guna meningkatkan perlindungan program miliknya. Namun ada kalanya peretas yang memiliki informasi atas kekurangan tersebut terlebih dahulu secara cepat melakukan eksploitasi. Apabila hal demikian yang terjadi maka perlindungan atas penggunaan *software* tersebut menjadi amat lemah, sebab serangan akan mudah terjadi karena adanya cacat (*bugs*) yang masih sangat baru diketahui.

Organisasi yang berisiko dari eksploitasi semacam itu dapat menggunakan beberapa cara deteksi, termasuk salah satunya adalah dengan cara menggunakan *virtual local area network* (VLAN) untuk melindungi data yang dikirimkan, dengan menggunakan *firewall*, dan menggunakan sistem Wi-Fi yang aman untuk melindungi dari serangan *malware wireless*. Selain itu, individu dapat meminimalkan risiko dengan selalu melakukan *updated OS* (OS dengan *update* terkini) dan *updated software* mereka; atau dengan menggunakan SSL (*security socket layer*) pada situs *web*, guna mengamankan informasi yang dikirim antara pengguna dan situs.

Dari hasil penelitian dapat disimpulkan terdapat tujuh titik waktu kritis yang menentukan rentang serangan *zero day*.

1. Kerentanan diperkenalkan; kode rentan dirilis sebagai bagian dari aplikasi *software*, atau *software* yang digunakan oleh pengguna.
2. Eksploitasi dirilis di alam liar/dunia bebas; penyerang telah menemukan kerentanan dan menemukan teknik yang dapat mereka gunakan untuk menyerang sistem yang rentan.
3. Kerentanan ditemukan oleh *vendor*; *vendor* menjadi sadar akan kerentanan tersebut, tetapi *patch* masih belum tersedia.

4. Kerentanan diungkapkan secara publik; *vendor* atau peneliti keamanan, mengumumkan kerentanan, membuat pengguna dan penyerang menyadarinya secara luas.
5. *Signature* anti virus dirilis; jika penyerang telah membuat *malware zero-day*, *vendor* anti virus dapat mengidentifikasi *signature*-nya dengan relatif cepat dan melindunginya. Sistem masih dapat terekspos karena mungkin ada cara lain untuk mengeksploitasi kerentanan.
6. *Patch* dirilis; *vendor* akhirnya merilis perbaikan untuk kerentanan yang ditemukan; keadaan ini bisa memakan waktu antara beberapa jam hingga berbulan-bulan, bergantung pada kerumitan perbaikan dan prioritas *vendor* dalam melakukan perbaikan dan proses pengembangan mereka.
7. Penerapan *patch* selesai; bahkan walaupun *patch* telah dirilis, kadang kala pengguna masih memerlukan sejumlah waktu, yang mungkin cukup lama untuk dapat menerapkannya. Hal ini ditimbulkan akibat dari organisasi mungkin tidak memiliki manajemen *patch* dan proses penerapan yang tidak terorganisir; atau pengguna rumahan mungkin mengabaikan pemberitahuan tentang harus dilakukannya pembaruan terhadap suatu perangkat lunak (*software*).

Kesempatan terjadinya keterpaparan pada saat sistem mungkin rentan terhadap serangan adalah seluruh periode waktu antara # 1 dan # 7. Serangan *zero-day* dapat terjadi antara # 2 dan # 4 ; dan waktu/tahap ini merupakan periode yang paling berbahaya dimana penyerang mengetahui tentang kerentanan *software* sementara sedangkan pengguna yang lain tidak mengetahuinya.

Bahkan beberapa hari/minggu setelah hari ke nol (*Zero-day*), serangan lanjutan bisa tetap akan terjadi. Setelah kerentanan terungkap, ada kompetisi antara penyerang, *vendor*, dan pengguna. Jika penyerang berhasil mencapai sistem yang rentan/cacat (*bugs*) sebelum antivirus atau program diperbarui atau *patch* diterapkan, kemungkinan besar mereka dapat berhasil, dan mempunyai pengaruh atau kendali ada fungsi kerja sistem.

Serangan *zero-day* dapat mengeksploitasi kerentanan di berbagai sistem berikut ini.

1. Sistem operasi (OS); merupakan salah satu target paling menarik untuk serangan *zero day*; karena keberadaannya yang di mana-mana dan dapat memberikan peluang bagi penyerang untuk bisa menguasai kendali atas sistem pengguna.
2. *Browser web*; kerentanan yang belum di *patch* dapat memungkinkan penyerang untuk melakukan *drive-by download*, menjalankan *script*, atau bahkan mengeksekusi *file program* pada mesin pengguna.
3. Aplikasi perkantoran (*Office automation*); *malware* yang disematkan ke dalam dokumen atau *file* lain sering kali dapat mengeksploitasi kerentanan pada *zero day,* khususnya pada fungsi aplikasi dasar yang digunakan untuk mengedit *file* tersebut.

4. Komponen *open source*; beberapa proyek *open source* tidak dipelihara secara aktif atau tidak memiliki praktik keamanan yang baik. *Vendor software* dapat menggunakan komponen ini tanpa menyadari kerentanan yang dikandungnya.
5. *Watering holes*; program *software* yang banyak digunakan oleh organisasi atau pengguna rumahan berada di bawah pengawasan ketat oleh penyerang yang sedang mencari kerentanan yang tidak diketahui.
6. *Hardware*; kerentanan di *router, switch,* peralatan jaringan, atau perangkat rumah seperti konsol *game*, dapat memungkinkan penyerang untuk menyusupi perangkat ini, mengganggu aktivitas mereka atau menggunakannya untuk membangun *botnet* besar-besaran. Botnet adalah jaringan yang terdiri dari komputer yang dikendalikan dari jarak jauh, atau "bot". Komputer ini telah terinfeksi perangkat lunak perusak yang memungkinkannya dikontrol dari jarak jauh. Beberapa botnet terdiri dari ratusan ribu - atau bahkan jutaan - komputer. "Bot" hanyalah singkatan dari "robot". Seperti robot, bot perangkat lunak bisa baik atau jahat. Kata "bot" tidak selalu berarti perangkat lunak yang buruk, tetapi kebanyakan orang merujuk pada jenis perangkat lunak perusak saat mereka menggunakan kata ini. Kata botnet berasal dari dua kata, robot dan *network*. Istilah ini biasanya digunakan dengan konotasi negatif.
7. *Internet of Things* (IoT); perangkat yang terhubung, dari peralatan rumah tangga dan televisi hingga sensor kendali, mobil yang terhubung jaringan, dan mesin pabrik semuanya rentan terhadap serangan *zero-day*. Banyak perangkat IoT tidak memiliki mekanisme untuk melakukan *patch* atau memperbarui *software* mereka.

Kemampuan untuk dapat mencegah serangan *zero-day* secara efektif adalah merupakan tantangan yang *signifikan* bagi tim keamanan mana pun. Serangan ini datang tanpa peringatan dan dapat menembus berbagai sistem keamanan. Serangan ini umumnya mengandalkan metode berbasis *signature*.

Agar dapat meningkatkan pemahaman dan kesadaran Anda atas keamanan sehingga diharapkan mampu mengurangi risiko atas keamanan sistem; Anda dapat mulai dengan mempelajari berbagai jenis serangan yang baru-baru ini terjadi.

1. *Microsoft*

Pada Maret 2020, Microsoft memperingatkan pengguna tentang serangan *zero-day* yang mengeksploitasi dua kerentanan terpisah. Kerentanan ini mempengaruhi semua versi yang didukung oleh Windows dan tidak tersedia *patch* yang diharapkan hingga berminggu-minggu kemudian. Saat ini tidak ada pengenal di *Common Vulnerabilities and Exposures* (CVE) untuk kerentanan ini.

Serangan tersebut menargetkan kerentanan eksekusi *remote code execution* (RCE) di *library Adobe Type Manager* (ATM). *Library* ini dibangun di dalam Windows untuk *PostScript Type 1 fonts*. Apabila cacat (*bugs*) ini terjadi di ATM, maka keadaan ini memungkinkan penyerang untuk menggunakan dokumen berbahaya yang dapat menjalankan *script* dari jarak jauh. Dokumen berbahaya tersebut dapat datang/sampai/

tiba ke komputer kita atau peralatan lainnya melalui *spam* atau diunduh oleh pengguna yang tidak menaruh curiga. Pada saat dokumen tersebut dibuka, atau di pratinjau dengan *Windows File Explorer*, *script* akan berjalan, dan menginfeksi perangkat pengguna.

2. *Internet Explorer*

Internet Explorer (IE), *browser* lama Microsoft, adalah titik sumber yang banyak mengalami serangan *zero-day* baru-baru ini. Kerentanan ini (CVE-2020-0674) terjadi karena kesalahan dalam cara mesin *script* IE mengelola objek dalam memori. Keadaan ini terjadi dan berpengaruh pada IE versi 9 hingga 11.

Penyerang dapat memanfaatkan kerentanan ini dengan cara mengelabuhi pengguna agar mengunjungi situs *web* yang dibuat untuk mengeksploitasi kekurangan tersebut. Ini dapat dilakukan melalui *email phishing* atau melalui pengalihan *link* (*redirect link)* dan *request server*.

Lalu bagaimana cara mengantisipasi serangan *zero-day*?

Secara alami, serangan *zero day* sulit untuk dilawan; namun terdapat beberapa cara untuk mempersiapkan dan dapat mengurangi ancaman secara efektif bagi organisasi Anda. Berikut empat praktik terbaik (*four best practice*) yang sering dilakukan dan banyak yang terbantu dalam mengurangi/menekan atau menghilangkan ancaman yang ditimbulkan oleh serangan *zero day*.

a. Gunakan Windows Defender Exploit Guard

Pada Windows 2010, Microsoft memperkenalkan *Windows Defender Exploit Guard*, yang memiliki beberapa kemampuan untuk melindungi dari serangan *zero day*:

Attack Surface Reduction (ASR); melindungi dari infeksi *malware* dengan cara memblokir ancaman berdasarkan *file Office*, *script*, dan *email*. ASR dapat memblokir perilaku yang mendasari dokumen berbahaya sambil mengaktifkan skenario produktif. Fitur ini dapat mendeteksi dan memblokir *malicious software*, mengaburkan *macro code*, JavaScript, VBScript dan PowerShell, serta dapat mencegah *script* mengeksekusi muatan yang diunduh dari internet atau konten yang dapat dijalankan dalam *email*.

Perlindungan jaringan; *Exploit Guard* memblokir semua koneksi keluar sebelum digunakan, mencegah *malware* untuk dapat terhubung dengan *command and control server* (C&C) secara otomatis. Lalu lintas jaringan keluar dievaluasi berdasarkan nama *host* dan reputasi IP, dan koneksi jaringan apapun ke tujuan yang tidak terpercaya dihentikan.

Melakukan kontrol pada akses *folder*; memantau perubahan yang dibuat oleh aplikasi ke *file* di *folder* yang dilindungi. Fitur tersebut dapat mengunci *folder* penting dan hanya mengizinkan untuk diubah/ diakses oleh aplikasi yang resmi dibuat oleh produsen. Fasilitas ini dapat mencegah terjadinya enkripsi *file* akibat terinfeksi oleh suatu *ransomware*.

b. Manfaatkan Next-Generation Antivirus (NGAV)

Solusi antivirus tradisional, yang mendeteksi *malware* menggunakan *signature file*, tidak efektif untuk melawan ancaman *zero d*ay. Antivirus tersebut masih bisa berguna, karena pada saat kerentanan diumumkan ke publik, *vendor* antivirus akan dengan cepat memperbarui basis data *malware* mereka, dan kemudian antivirus akan dengan efektif melawan ancaman tersebut; namun jeda antara saat penyimpangan (*bugs*) ditemukan hingga saat pembaharuan *library* antivirus/*malware*, merupakan periode yang rawan atas terjadinya serangan *zero day*. Oleh karena itu dibutuhkan kemampuan dari organisasi untuk memblokir *malware zero-day* yang belum diketahui penyebab dan cacat yang terjadi serta solusi untuk mengatasi cacat tersebut.

Solusi dari *Next Generation Antivirus* (NGAV) memanfaatkan fitur kecerdasan dalam menganalisis terjadinya ancaman, analisis perilaku yang berdasar pada anomali perilaku pada sistem serta mengidentifikasi perilaku anomali yang mencurigakan. Analisis berbasis kode pembelajaran mesin dilakukan untuk mengidentifikasi dan mendeteksi terjadinya infeksi dari untaian *malware* yang belum dikenali, tetapi telah menyebabkan perubahan perilaku secara tidak normal dari sistem yang ada. Setelah mendeteksi kehadiran *malware* semacam itu, NGAV secara otomatis mampu memblokir proses berbahaya dan memblokir serangan agar tidak menyebar ke titik akhir (*end point*) lainnya.

Teknologi NGAV yang tersedia pada saat ini belum mampu untuk mendeteksi semua jenis *malware zero-day*, akan tetapi secara signifikan dapat mengurangi (mencegah) kemungkinan penyerang dapat menembus titik akhir (*end point*) dengan cara menggunakan *malware* yang tidak dikenal.

c. Menerapkan manajemen patch

Setiap organisasi harus memiliki kebijakan dan proses manajemen *patch*, dan dikomunikasikan dengan jelas kepada semua karyawan dalam bentuk SOP serta dikoordinasikan kepada tim pengembangan, tim operasi TI, dan tim keamanan.

Dalam organisasi yang lebih besar, penting untuk menggunakan otomatisasi untuk pengelolaan *patch*. Secara otomatis mendapatkan *patch* dari vendor *software*; mengidentifikasi sistem yang memerlukan pembaruan, menguji perubahan yang diperkenalkan oleh *patch*, dan secara otomatis menerapkan *patch* ke produksi. Hal ini diperlukan untuk menghindari terjadinya penundaan dalam produksi karena menerapkan *patch*, serta mencegah terjadinya kealpaan yang diwariskan oleh pihak manajemen sebelumnya; atau terlupa/tertinggal pada saat terjadi pembaharuan sistem.

Manajemen *patch* tidak dapat mencegah terjadinya serangan *zero-day*, namun secara signifikan dapat mengurangi jendela eksposur. Apabila terjadi kerentanan yang parah, *vendor software* mungkin baru akan mampu mengeluarkan *patch* dalam waktu beberapa jam atau hari ke depan. Manajemen *patch* otomatis dapat membantu dalam penerapan *patch* secara cepat; sebelum penyerang dapat mengidentifikasi kerentanan dalam sistem dan mengeksploitasinya.

d. Siapkan rencana insiden respons

Organisasi dari semua ukuran akan mendapatkan keuntungan atas ketersediaan rencana insiden respons (rencana tanggap darurat). Tatanan ini menunjukkan proses yang terorganisir dalam mengidentifikasi dan menangani serangan di dunia maya. Ketersediaan suatu rencana khusus yang berfokus pada serangan *zero-day* akan memberi keuntungan besar apabila terjadi serangan, mengurangi kebingungan, serta meningkatkan peluang untuk menghindari atau mengurangi/menekan kerusakan.

Pada saat menyusun rencana; sebaiknya mengikuti enam tahap tanggap bencana/ insiden dari SANS Institute.

Rencana tersebut harus mengikuti ketentuan berikut ini.

1) **Persiapan;** lakukan penilaian risiko dan identifikasi aset paling sensitif yang harus menjadi fokus tim keamanan. Siapkan dokumentasi yang menyatakan peran, tanggung jawab, dan proses.
2) **Identifikasi;** tentukan cara mendeteksi potensi serangan *zero-day* (menggunakan alat dan/atau proses operasional), lakukan validasi bahwa kejadian tersebut adalah benar merupakan suatu serangan; serta informasi tambahan apa yang perlu dikumpulkan untuk menghadapi ancaman.
3) **Penahanan;** setelah insiden keamanan teridentifikasi; langkah apa saja yang dapat diambil untuk mengatasi insiden tersebut dan mencegah terjadinya kerusakan lebih lanjut, serta langkah jangka panjang apa yang dapat diambil untuk membersihkan dan memulihkan sistem yang terkena dampak.
4) **Pemberantasan;** tentukan cara mengidentifikasi akar penyebab serangan dan memastikan langkah-langkah diambil untuk mencegah serangan serupa.
5) **Pemulihan;** tentukan cara menghidupkan kembali sistem produksi, mengujinya, dan tetapkan jangka waktu untuk memantau sistem guna memastikan bahwa situasi telah kembali normal.
6) **Pelajaran yang dipetik;** lakukan retrospektif selambat-lambatnya dua minggu dari akhir insiden, untuk meninjau *tools* yang telah tersedia dan proses organisasi, dan lakukan analisa agar menjadi lebih siap apabila terjadi serangan berikutnya.

C. *VULNERABILITY*

Kerentanan sering kali dapat menimbulkan suatu konsekuensi hukum. Kerentanan apa pun yang memungkinkan terjadinya ancaman dapat mengakibatkan tindakan hukum. Suatu komputer harus menjalankan *software* agar dapat berguna, dan sebab pembuat *software* adalah manusia yang tidak luput dari kesalahan, maka program/*software* pasti mengandung kesalahan. Dengan demikian, *vendor software* harus melindungi diri mereka sendiri dari kewajiban kerentanan mereka sendiri dengan *End-User License Agreement* (EULA). EULA mulai berlaku saat pengguna membuka paket dan menginstal *software*. Semua *vendor software* menggunakan EULA. Itu berarti beban untuk melindungi sistem dan data TI terletak pada para profesional keamanan sistem informasi internal.

Kerentanan (*vulnerability*) terus berkembang dari hari ke hari dengan jumlah dan *variant* yang semakin banyak. Kerentanan yang ditemukan telah didokumentasikan dan diberi nomor yang unik pada masing-masing kerentanan yang berbeda. Pada saat ini telah tersedia sistem yang mencatat kerentanan dan paparan keamanan informasi yang diketahui publik berdasarkan metode referensi. Salah satu dari sistem yang telah tersedia tersebut adalah CVE.

Daftar *Common Vulnerabilities and Exposures* (CVE) diluncurkan oleh MITRE sebagai upaya komunitas pada tahun 1999. Pada tahun 2005 *National Vulnerability Database* (NVD) AS meluncurkan *National Institute of Standards and Technology* (NIST).

Daftar catatan CVE masing-masing berisi nomor identifikasi, deskripsi, dan setidaknya satu referensi publik yang menyatakan kerentanan keamanan *cyber* yang telah diketahui oleh publik. *CVE Records* digunakan di berbagai produk dan layanan keamanan *cyber* dari seluruh dunia, termasuk NVD. NVD yang merupakan basis data yang mencatat kerentanan sistem informasi, kemudian disinkronkan sepenuhnya dengan daftar CVE; sehingga setiap kali terjadi pembaharuan di CVE maka otomatis akan segera muncul juga di NVD. Hubungan daftar CVE dengan NVD bisa dikatakan bahwa CVE memberi makan NVD.

NVD memperkaya catatan data yang dibuat berdasarkan informasi yang diperoleh dari CVE dengan beberapa informasi/data lain seperti (a) informasi perbaikan yang dilakukan, (b) skor/tingkat keparahan, dan (c) peringkat dampak atas serangan. Sebagai bagian dari informasi yang disempurnakan, NVD juga menyediakan fitur pencarian lanjutan misalnya berdasarkan (a) Sistem Operasi, (b) nama vendor, (c) nama produk dan/atau nomor versi, (d) jenis kerentanan, (e) tingkat keparahan, (f) jangkauan eksploitasi terkait, dan (g) dampak.

Software yang tidak aman telah mengancam hampir di semua bidang dari mulai infrastruktur keuangan, kesehatan, pertahanan, energi, hingga infrastruktur kritikal lainnya. Dengan semakin kompleks dan terhubungnya infrastruktur digital kita, maka kesulitan untuk dapat mencapai keamanan aplikasi meningkat secara eksponensial. Kita tidak lagi boleh mentoleransi masalah keamanan sederhana seperti yang ditampilkan dalam OWASP Top 10.

Open Web Application Security Project (OWASP) merupakan proyek keamanan aplikasi *web* terbuka. Proyek ini adalah suatu komunitas *online* yang menghasilkan artikel, metodologi, dokumentasi, alat, dan teknologi yang tersedia secara bebas di bidang keamanan aplikasi *web*. OWASP telah membantu berbagai organisasi dalam meningkatkan kesadaran tentang keamanan aplikasi dengan cara mengidentifikasi beberapa risiko kritikal yang dihadapi organisasi. Dengan adanya daftar kerentanan dan daftar risiko kritikal pada aplikasi diharapkan dapat membantu organisasi untuk memulai membangun sistem keamanan aplikasi pada internal organisasi. Pengembang dapat belajar dari kesalahan organisasi lain. Manajemen harus mulai memikirkan tentang tata-cara mengelola risiko yang ditimbulkan oleh aplikasi pada perusahaan mereka.

Dirilis di halaman resmi OWASP (https://owasp.org) kita dapat melihat peringkat 10 teratas *vulnerability* yang memiliki risiko kritikal pada aplikasi, dan diantaranya dijelaskan di bawah ini:

1) **Injeksi. *Injection flaws*** (seperti injeksi SQL, NoSQL, OS, dan LDAP) terjadi saat 'data tidak terpercaya' dikirim ke *interpreter* sebagai bagian dari perintah atau queri. Data yang dimiliki oleh penyerang dapat mengelabui *interpreter* agar menjalankan perintah yang tidak diinginkan atau mengakses data tanpa otorisasi yang tepat.
2) **Otentikasi rusak**. Fungsi aplikasi yang terkait dengan autentikasi dan pengelolaan *session* sering kali tidak diterapkan dengan benar, sehingga memungkinkan penyerang untuk menyusupi sandi, kunci, atau *token session*, atau mengeksploitasi kelemahan implementasi lainnya untuk membangkitkan asumsi atas/sebagai identitas pengguna lain secara sementara atau permanen.
3) **Keterpaparan data sensitif.** Banyak aplikasi *web* dan *API* yang tidak melindungi data sensitif dengan benar, seperti keuangan, perawatan kesehatan, dan sebagainya. Penyerang dapat mencuri atau mengubah 'data yang dilindungi secara lemah' tersebut dan kemudian melakukan penipuan kartu kredit, pencurian identitas, atau kejahatan lainnya. Data sensitif dapat disusupi jika tanpa perlindungan ekstra, seperti enkripsi saat diam atau saat transit, dan memerlukan tindakan pencegahan khusus saat dipertukarkan dengan *browser*.

Latihan

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

1) Apakah kesadaran/*awareness* keamanan informasi itu?
2) Siapakah yang bertanggungjawab atas keamanan sistem informasi dalam organisasi? Jelaskan!
3) Jelaskan yang dimaksud dengan serangan *zero-day*!
4) Apakah hubungan antara CVE dan NVD?
5) Sebutkan salah satu standar internasional yang dapat diadopsi oleh perusahaan untuk mengimplementasikan sistem manajemen keamanan informasi!

Petunjuk Jawaban Latihan

1) Kesadaran/*awareness* keamanan informasi adalah merupakan titik awal untuk seluruh pegawai suatu organisasi dalam menyadari atau memahami pengetahuan mengenai keamanan teknologi informasi.
2) Yang bertanggungjawab terhadap keamanan informasi adalah seluruh elemen yang ada dalam organisasi mulai dari manajemen tertinggi, *senior manager, low manager, technical support, engineer, administrator,* dan pihak yang berkepentingan terhadap bisnis organisasi. Semua pihak yang telah disebutkan memiliki peran dan tanggung jawab masing-masing.

3) Eksploitasi *zero day* adalah serangan dunia maya yang terjadi pada hari yang sama ketika ditemukan kelemahan dalam *software*. Mulai saat ditemukan kelemahan, dapat terjadi eksploitasi atas kelemahan tersebut sebelum tersedia perbaikan dari pembuat *software*. Diawali dengan kejadian ketika ada pengguna yang menemukan bahwa ada risiko keamanan dalam suatu program, mereka kemudian melaporkannya ke perusahaan *software*, yang kemudian akan mengembangkan *patch* keamanan untuk memperbaiki kekurangan/kelemahan tersebut.
4) NVD merupakan basis data kerentanan yang dibangun dan disinkronkan sepenuhnya dengan daftar CVE sehingga pembaruan apa pun yang terjadi pada CVE, maka akan segera muncul di NVD. NVD juga memberikan informasi tambahan tentang perbaikan yang telah/sedang dilakukan, skor keparahan, dan peringkat dampak, juga menyediakan fitur pencarian lanjutan seperti berdasarkan sistem operasi, nama vendor, nama produk dan/atau nomor versi, juga berdasarkan jenis kerentanan, tingkat keparahan, jangkauan eksploitasi terkait, dan dampak.
5) Standar Internasional yang dapat diadopsi oleh suatu perusahaan untuk mengimplementasikan sistem manajemen keamanan informasi adalah ISO 27001:2013.

Rangkuman

1. Kesadaran/*awareness* keamanan informasi merupakan awal bagi seluruh pegawai pada organisasi untuk menyadari dan memahami pengetahuan mengenai keamanan teknologi informasi.
2. Dari berbagai contoh insiden keamanan informasi seperti diretasnya *website* perusahaan besar dunia dan juga *e-commerce* besar yang ada di Indonesia, dimana situs *website* perusahaan dibobol oleh *hacker* serta data yang dapat dicuri; kita dapat melihat bahwa setiap perusahaan perlu memiliki strategi dalam membangun sistem manajemen keamanan informasi dan harus selalu dikaji/telaah dan di*update* sesuai dengan perkembangan teknologi yang terjadi.
3. Eksploitasi *zero day* adalah suatu serangan yang terjadi di dunia maya. Serangan tersebut terjadi pada hari yang sama ketika ditemukan kelemahan pada suatu *software*. Eksploitasi atas kelemahan terjadi sebelum tersedianya perbaikan dari pembuat *software*. Keadaan ini diawali pada saat seorang pengguna menemukan bahwa terdapat risiko keamanan dalam suatu program, kemudian mereka melaporkannya ke perusahaan *software*, yang akan mengembangkan *patch* keamanan untuk memperbaiki kekurangan tersebut.
4. CVE merupakan daftar kerentanan yang berisi nomor identifikasi, deskripsi, dan setidaknya satu referensi publik atas kerentanan keamanan *cyber* yang diketahui publik.
5. NVD merupakan basis data kerentanan yang dibangun dan disinkronkan sepenuhnya dengan daftar CVE sehingga pembaharuan apa pun yang terjadi pada CVE akan segera muncul di NVD. NVD juga memberikan informasi tentang perbaikan, skor keparahan, dan peringkat dampak. Selain itu juga menyediakan

fitur pencarian lanjutan seperti berdasarkan sistem operasi, nama vendor, nama produk, dan/atau nomor versi, serta berdasarkan jenis kerentanan, tingkat keparahan, jangkauan eksploitasi terkait dan dampak.

6. *Open Web Application Security Project* (OWASP) merupakan proyek keamanan aplikasi *web* terbuka adalah komunitas *online* yang menghasilkan artikel, metodologi, dokumentasi, alat, dan teknologi yang tersedia secara bebas di bidang keamanan aplikasi *web*.

Tes Formatif 1

Pilihlah satu jawaban yang paling tepat!

1) Berikut ini merupakan upaya yang dapat dilakukan organisasi untuk meningkatkan keamanan sistem informasi pada area kepegawaian, *kecuali* ....
   A. melakukan pengecekan latar belakang calon pegawai, melakukan *screening* calon pegawai
   B. melakukan penandatanganan *non-disclosure agreement* (NDA) untuk setiap pegawai
   C. pegawai yang sudah tanda tangan kontrak tidak perlu tanda tangan *non-disclosure agreement* (NDA)
   D. organisasi harus memiliki mekanisme pengembalian aset ketika pegawai mengalami rotasi, pegawai mengundurkan diri, pensiun, dan lain-lain terkait dengan peraturan kepegawaian

2) Berikut ini merupakan upaya perusahaan ketika situs *website* mereka dibobol oleh *hacker*, *kecuali* ....
   A. dibiarkan saja, asal *webite* masih dapat diakses
   B. menginformasikan kepada *user* untuk melakukan penggantian *password*
   C. melakukan *patching*
   D. melakukan perbaikan *script* pada kerentanan yang telah ditemukan

3) ISO 27001:2013 adalah standar internasional yang memiliki fokus pada ....
   A. kesehatan dan keselamatan kerja
   B. sistem manajemen keamanan rantai pasok
   C. sistem manajemen keamanan informasi
   D. sistem manajemen risiko

4) Serangan dunia maya yang terjadi pada hari yang sama ketika ditemukan kelemahan dalam *software* adalah pengertian dari ....
   A. CVE
   B. *zero-day attack*
   C. *vulnerability*
   D. *awareness*

5) Titik awal bagi seluruh pegawai dalam suatu organisasi untuk mengejar atau memahami pengetahuan mengenai keamanan teknologi informasi adalah ....
   A. CVE
   B. *zero-day attack*
   C. *vulnerability*
   D. *awareness*

6) Kerentanan atau *code* cacat merupakan kelemahan pada asset yang dapat dimanfaatkan oleh pelaku ancaman, seperti penyerang, untuk melintasi batas-batas privilege dalam suatu sistem komputer, adalah pengertian dari ....
   A. CVE
   B. *zero-day attack*
   C. *vulnerability*
   D. *awareness*

7) Daftar kerentanan yang berisi nomor identifikasi, deskripsi, dan setidaknya satu referensi publik untuk kerentanan keamanan *cyber* yang diketahui publik, adalah pengertian dari ....
   A. CVE
   B. *zero-day attack*
   C. *vulnerability*
   D. *awareness*

8) Berikut ini adalah cara untuk menanggulangi serangan *zero-day* ....
   A. melakukan konfigurasi pada *firewall* dengan benar
   B. memberlakukan jam lembur pada satpam perusahaan untuk berjaga-jaga
   C. menginstruksikan pada pegawai untuk menonaktifkan anti virus
   D. memberlakukan sistem penjagaan pada data *center* selama 7 x 24 jam

9) OWASP Top 10 dapat membantu perusahaan untuk ....

A. membantu organisasi meningkatkan kesadaran tentang keamanan aplikasi dengan mengidentifikasi siapa yang melakukan *hacking*

B. membantu organisasi meningkatkan kesadaran tentang keamanan aplikasi dengan mengidentifikasi beberapa risiko kritikal yang dihadapi organisasi

C. membantu organisasi meningkatkan kesadaran tentang keamanan aplikasi dengan melakukan forensik ketika terjadi *hacking*

D. membantu organisasi meningkatkan kesadaran tentang keamanan aplikasi pada pegawai perusahaan

10) Apakah yang harus dilakukan ketika kita sebagai pegawai mengetahui di dalam perusahaan terjadi insiden keamanan informasi seperti terjadinya pencurian data?

A. Diam saja, takut dipecat.

B. Melaporkan kepada pihak yang berwenang di dalam perusahaan.

C. Lapor pak RT.

D. Menggosipkan dengan teman-teman kantor.

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.

$$\text{Tingkat Penguasaan} = \frac{\text{Jumlah Jawaban yang Benar}}{\text{Jumlah Soal}} \times 100$$

Arti tingkat penguasaan

<70%	70% - 79%	80% - 89%	90% - 100%
kurang	cukup	baik	baik sekali

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. Bagus! Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

Kegiatan Belajar 2

Pengertian, Tujuan, dan Pengelolaan Keamanan SI

Pada pelajaran sebelumnya kita sudah tahu tentang persoalan-persoalan yang dihadapi oleh organisasi maupun individu tentang bahaya yang mengancam dunia *cyber* dan cara mengatasi bahaya tersebut. Penjelasan berikut ini adalah tentang tata cara mengidentifikasi dan memerangi bahaya yang umum terjadi di dalam sistem informasi dan infrastruktur TI. Agar memahami tentang cara membuat komputer lebih aman, maka Anda harus terlebih dahulu memahami konsep risiko, ancaman, dan kerentanan. Namun sebelum itu kita bahas terlebih dulu definisi tentang keamanan *cyber* dan keamanan informasi sekaligus relasi diantara keduanya.

A. PENGERTIAN DAN TUJUAN KEAMANAN SISTEM INFORMASI

Istilah keamanan *cyber* sering digunakan secara bergantian dengan istilah keamanan informasi, meskipun ada tumpang tindih yang substansial antara keamanan dunia *cyber* dan keamanan informasi, namun kedua konsep ini tidak sepenuhnya sejalan. Keamanan dunia maya (*cyber*) melampaui batas-batas keamanan informasi tradisional karena memasukkan tidak hanya perlindungan sumber daya informasi, tetapi juga aset lain, termasuk individu yang terlibat di dalamnya.

> Dalam **keamanan informasi,** acuan pada faktor manusia biasanya berkaitan dengan peran manusia dalam proses keamanan.
> Dalam **keamanan *cyber*** terdapat dimensi tambahan yakni manusia sebagai target potensial pada suatu serangan *cyber* atau bahkan tanpa disadari ikut serta dalam serangan *cyber*.

Dimensi tambahan ini memiliki implikasi etika bagi masyarakat secara keseluruhan, karena di dalamnya terdapat komponen perlindungan terhadap kelompok rentan tertentu, misalnya anak; hal ini dapat dilihat sebagai suatu tanggung jawab sosial. Pada sebagian besar literatur, keamanan *cyber* digunakan sebagai istilah yang mencakup semua subyek/topik. Definisi atas istilah ini dapat berbeda-beda; misalnya andas Merriam Webster mendefinisikannya sebagai “tindakan yang diambil untuk melindungi komputer atau sistem komputer (seperti di Internet) dari akses atau serangan yang tidak sah”.

International Telecommunications Union (ITU) mendefinisikan keamanan dunia maya/*cyber* sebagai berikut:

> **Keamanan *cyber*** adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi serta aset pengguna.
> Organisasi dan aset pengguna mencakup perangkat komputasi yang saling terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan totalitas informasi yang dikirimkan dan/atau disimpan di lingkungan *cyber*.
> Keamanan *cyber* berusaha keras untuk memastikan pencapaian dan pemeliharaan properti keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan di lingkungan *cyber* yang berdasarkan *CIA (confidentiality, Integrity, dan Availability)*

Tujuan keamanan informasi adalah untuk memastikan kelangsungan bisnis dan meminimalkan terjadinya kerusakan bisnis dengan cara menekan/membatasi risiko atas dampak dari terjadinya suatu insiden keamanan (Von Solms, 1998). Keamanan informasi dapat didefinisikan dengan beberapa cara.

Standar internasional, ISO / IEC 27002 (2013), mendefinisikan bahwa "Keamanan informasi sebagai pengembangan dari kerahasiaan, integritas dan ketersediaan informasi. Dalam konteks ISO / IEC 27002 (2013), informasi dapat muncul/tersedia dalam berbagai bentuk, dapat dicetak atau ditulis di atas kertas; disimpan secara elektronik melalui pos atau sarana elektronik; dan ditampilkan dalam bentuk film, disampaikan dalam bentuk percakapan, dan sebagainya".

Whitman dan Mattord (2009:8) mendefinisikan keamanan informasi sebagai "Perlindungan atas informasi dan elemen kritisnya, termasuk sistem dan perangkat keras yang menggunakan, menyimpan, dan mengirimkan informasi itu". Whitman dan Mattord (2009) juga mengidentifikasi beberapa karakteristik penting dari informasi yang memberinya nilai dalam organisasi. Karakteristik tersebut meliputi (a) kerahasiaan, (b) integritas dan (c) ketersediaan informasi, sebagaimana yang disebutkan dalam definisi ISO / IEC 27002 (2013); namun tidak terbatas pada ketiga karakteristik tersebut saja. Menurut Whitman dan Mattord (2009:8), memastikan kerahasiaan, integritas dan ketersediaan informasi, juga dikenal dalam keamanan informasi sebagai segitiga CIA (*Confidentiality, Integrity dan Availability*) yang secara tradisional telah menjadi standar industri. "Keamanan dari ketiga karakteristik informasi ini adalah hari ini sama pentingnya seperti sebelumnya, namun model segitiga CIA tidak lagi memadai untuk membahas lingkungan yang terus berubah di industri komputer" (Whitman dan Mattord, 2009:8). Dengan demikian, Whitman dan Mattord (2009) menambahkan keakuratan, keaslian, kegunaan, dan kepemilikan ke daftar karakteristik informasi yang perlu dilindungi.

Beberapa konsep dalam definisi di atas perlu dikaji secara lebih mendalam.

1. Pertama, harus jelas bahwa keamanan informasi bukanlah produk atau teknologi, tetapi suatu proses. Pada masa yang lalu keamanan informasi adalah hanya merupakan masalah teknis yang ketat. Namun, seiring berkembangnya penggunaan komputer dan jaringan, proses pengamanan komputer dan jaringan ini juga harus berkembang melampaui batasan teknisnya. Proses keamanan informasi mungkin memerlukan penggunaan produk tertentu, tetapi bukanlah sesuatu yang dapat dibeli begitu saja.
2. Faktor penting kedua yang perlu diperhatikan tentang definisi di atas adalah bahwa keamanan informasi secara umum didefinisikan dalam sifat atau karakteristik yang seharusnya dimiliki oleh informasi yang aman. Ini biasanya mencakup kerahasiaan, integritas, dan ketersediaan informasi, tetapi dapat mencakup karakteristik tambahan.

Keamanan teknologi informasi dan komunikasi (TIK) berkaitan dengan perlindungan berbasis teknologi yang sebenarnya, dan sistem tempat informasi umumnya disimpan dan/atau disebarluaskan.

Definisi keamanan TIK meliputi segala aspek yang berkaitan dengan:

1. mendefinisikan,
2. mencapai dan menjaga kerahasiaan,
3. integritas, ketersediaan,
4. non-penyangkalan (*non-repudiation*),
5. akuntabilitas,
6. keaslian (*originality*), dan
7. kehandalan sumber daya informasi (*reliability*).

Keamanan informasi mencakup perlindungan sumber daya informasi yang mendasarinya, sehingga dapat dikatakan bahwa "keamanan TIK" merupakan sub-komponen dari "keamanan informasi". Definisi keamanan TIK sangat mirip dengan definisi keamanan informasi. Namun, karakteristik tambahan, dapat lebih baik dijelaskan sebagai layanan yang harus disediakan oleh sumber daya informasi yang aman, termasuk *non-repudiation*, akuntabilitas, keaslian dan reliabilitas, juga mengacu pada konsep keamanan data dan menunjukkan adanya perlindungan data aktual pada sistem informasi.

Dari definisi diatas, tampak ada perbedaan antara mengamankan sumber daya informasi dan mengamankan sumber daya TIK. Sumber daya informasi yang aman dapat mencakup entitas mana pun, dari mana informasi diterima atau ke mana informasi dikirim. Sumber daya teknologi informasi yang aman adalah sumber daya informasi yang berada pada sistem teknologi informasi yang aman pula. Penting untuk dicatat bahwa, dalam hal sistem berbasis TIK, suatu informasi "tidak dapat dianggap aman" kecuali semua sumber daya dan proses yang berhubungan dengan informasi tersebut

juga aman.

Tiga karakteristik pertama, kerahasiaan, integritas, dan ketersediaan, umumnya yag dikenal sebagai model segitiga CIA, yang telah dianggap sebagai standar industri untuk keamanan komputer sejak pengembangan komputer *mainframe* (Whitman dan Mattord, 2009:8). Beberapa karakteristik tambahan telah disematkan ke dalam definisi tersebut guna memenuhi kebutuhan standar keamanan tambahan pada suatu organisasi/ bisnis yang berada di dalam lingkungan koneksi antar-jaringan saat ini.

Pemahaman yang jelas tentang makna dari semua karakteristik (dan/atau layanan) yang disebutkan di atas sangat penting untuk dipahami sebagai informasi dan keamanan TIK; karena tanpa kerahasiaan, integritas, ketersediaan, non-penyangkalan, akuntabilitas, keaslian dan kehandalan sumber informasi, informasi tidak dapat dianggap aman. Semua hal di atas (termasuk akurasi, kegunaan dan kepemilikan informasi) memainkan peran secara integral dalam keamanan informasi dan semua komponen harus dianggap sama pentingnya. Namun, mungkin satu atau beberapa karakteristik tersebut dapat lebih mudah diterapkan ke dalam skenario tertentu daripada komponen yang lainnya, bergantung pada sifat informasi itu sendiri.

Misalnya, integritas "data statistik inflasi" jelas penting bagi para ekonom, sementara kerahasiaan data yang sama tampaknya tidak terlalu penting sebab setiap orang mungkin akan diizinkan untuk boleh memiliki akses kepada informasi tersebut. Namun, menurut definisi, pelanggaran kerahasiaan hanya terjadi jika entitas yang tidak berwenang memperoleh informasi tersebut. Namun karena setiap orang akan menjadi pengguna resmi dari statistik inflasi, dalam hal ini kerahasiaan informasi akan benar-benar dijaga. Dalam konteks organisasi, wajib untuk memastikan bahwa keamanan informasi organisasi bukanlah merupakan kasus memutuskan karakteristik atau layanan mana yang dapat diterapkan, melainkan mendefinisikan entitas yang berwenang, serta parameter lain untuk setiap bagian informasi secara benar.

Saat melakukan analisis keamanan TIK, tampak bahwa terdapat berbagai macam ancaman yang menargetkan kerentanan terkandung di dalam suatu system; dan kemudian akhirnya memberi dampak negatif pada infrastruktur TIK. Dalam situasi ini terlihat jelas bahwa infrastruktur teknologi dapat dianggap sebagai suatu aset yang perlu dilindungi. Dengan demikian, dalam keamanan TIK, TIK adalah aset yang diamankan. Dalam kasus keamanan informasi, TIK adalah merupakan infrastruktur yang memproses, menyimpan, dan mengkomunikasikan informasi. Dalam hal ini informasi dianggap sebagai aset yang memerlukan perlindungan. Teknologi informasi dan komunikasi dalam hal ini dapat digolongkan sebagai sasaran dari berbagai ancaman dalam akibat adanya kerentanan yang ada di dalamnya. Tujuan utama dari penyerangan adalah untuk mendapatkan informasi atau memanipulasi informasi yang disimpan. Oleh karena itu, penting untuk diperhatikan bahwa, dalam kasus keamanan informasi, informasi adalah aset yang harus diamankan.

Seperti disebutkan sebelumnya, banyak publikasi saat ini yang berhubungan dengan keamanan *cyber* menggunakan istilah keamanan *cyber* secara bergantian dengan istilah keamanan informasi. Jika keamanan *cyber* identik dengan keamanan informasi,

maka akan masuk akal untuk mengasumsikan bahwa insiden keamanan *cyber* juga dapat dijelaskan dalam istilah karakteristik yang digunakan untuk mendefinisikan keamanan informasi. Jadi, insiden keamanan *cyber*, misalnya, juga akan berujung melanggar kerahasiaan, integritas, atau ketersediaan informasi. Hal ini berlaku pada sebagian besar ancaman terkait keamanan dunia maya yang mungkin dihadapi oleh pengguna dan/atau organisasi.

Namun, von Solms (2013) dalam jurnalnya mengatakan bahwa tidak semua ancaman keamanan *cyber* merupakan bagian dari cakupan keamanan informasi yang ditentukan secara formal.

Berikut ini akan disajikan secara singkat beberapa skenario yang dapat dijadikan sebagai contoh.

1. Skenario 1: *Cyber Bullying*

   Cyber bullying telah menjadi perhatian utama masyarakat modern, beberapa penelitian terbaru menemukan bahwa teknologi semakin banyak digunakan untuk menindas, "menimbulkan rasa malu, memicu pelecehan dan kekerasan, dan menimbulkan kerugian psikologis". Hal ini dapat menyebabkan "dampak yang parah dan negatif bagi mereka yang menjadi korban". Kebutuhan untuk mengatasi penindasan *cyber* telah diakui secara luas sebagai masalah keamanan *cyber* dan bahkan pemerintah Indonesia telah mengatur dan menyebutkan secara khusus di UU ITE (UU no 19 tahun 2016) bahwa setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3) UU ITE dapat dituntut dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp 750 juta.

   Namun, "ditindas di dunia maya" bukan berarti hilangnya kerahasiaan, integritas, atau ketersediaan informasi. Sebaliknya, target dari aktivitas tersebut adalah penggunanya sendiri. Oleh karena itu, penindasan dunia maya mengakibatkan kerugian langsung bagi orang yang ditindas.

2. Skenario 2: Otomatisasi Rumah/*Internet of Things* (IoT)

   Kemajuan dalam TIK, serta kemajuan di bidang elektronik, telah memunculkan banyak aplikasi otomasi rumah. Banyak dari fasilitas tersebut memungkinkan pemilik rumah untuk mengintegrasikan sistem keamanan rumah, air panas, lemari es, kompor, televisi dan peralatan lainnya dengan sistem manajemen berbasis *web*. Sayangnya, meningkatnya kenyamanan dalam mengelola rumah seseorang melalui *web* disertai dengan peningkatan risiko bahwa seseorang yang tidak berhak mungkin bisa mendapatkan akses secara tidak sah ke dalam sistem tersebut dan menyebabkan kerusakan. Kerusakan ini dapat berkisar dari "lelucon" seperti mematikan air panas, hingga kejahatan serius seperti mematikan sistem keamanan untuk merampok rumah. Sekali lagi, dalam kasus ini orang dapat membantah bahwa informasi korban tidak selalu terpengaruh secara negatif. Sebagai gantinya, aset korban lainnya menjadi sasaran kejahatan dunia *cyber*.

3. Skenario 3: Media Digital

   Salah satu industri yang terkena dampak langsung dari peningkatan berbagi informasi adalah industri hiburan. Setiap tahun, potensi pendapatan yang sangat besar hilang karena terjadinya berbagi film, musik, dan beberapa bentuk media digital ilegal lainnya. Pembagian ilegal ini tidak serta merta memengaruhi kerahasiaan, integritas, atau ketersediaan media yang dibagikan; namun, hal itu secara langsung memengaruhi kesejahteraan finansial pemilik sah hak atas media tertentu. Justifikasi diri atas aktivitas ilegal, seperti menyalin media secara ilegal, bahkan dapat menjadi katalisator yang memudahkan untuk melakukan tindakan ilegal lainnya di kemudian hari.

   Dalam kasus ini, dapat dikatakan bahwa korban kejahatan dunia maya lebih dari sekadar pihak yang kekayaan intelektual yang diretas. Bahkan meluas hingga menyerang sistem nilai (baik hak kepemilikan maupun etika pelakunya) yang dirugikan secara negatif.

4. Skenario 4: Terorisme *Cyber*

   Di Amerika Serikat, infrastruktur yang dianggap kritis didefinisikan sebagai "aset, sistem, dan jaringan, baik fisik maupun virtual, yang sangat penting bagi Amerika Serikat sehingga ketidakmampuan atau kehancurannya akan berdampak melemahkan keamanan, keamanan ekonomi nasional, kesehatan atau keselamatan publik, atau kombinasinya". Infrastruktur yang menyalurkan listrik dan air, mengontrol lalu lintas udara, atau mendukung transaksi keuangan dipandang sebagai "infrastruktur penopang kehidupan yang kritis" dan semuanya secara langsung bergantung pada komunikasi yang mendasari dan infrastruktur jaringan. Perlindungan infrastruktur kritis semacam itu merupakan bagian penting dari keamanan *cyber* dan dimasukkan sebagai keharusan nasional yang penting dalam strategi keamanan *cyber* nasional.

   Teroris *cyber* atau "spesialis musuh" dapat menargetkan infrastruktur penting suatu negara melalui dunia maya. Keadaan ini dapat terjadi secara langsung atau tidak langsung, misalnya dengan mempengaruhi ketersediaan layanan informasi menggunakan serangan penolakan layanan (DoS) ; atau secara langsung, melalui serangan terhadap jaringan listrik nasional. Dalam kasus serangan terhadap infrastruktur kritis semacam itu, kerugian tidak hanya mencakup integritas atau ketersediaan sumber daya informasi, tetapi juga akses ke layanan kritis tersebut. Dalam situasi ini, bukan informasi itu sendiri maupun pengguna informasi individu yang menjadi komponen berisiko, melainkan kesejahteraan masyarakat secara keseluruhan. Contohnya adalah serangan di Estonia pada bulan April / Mei 2007.

   Skenario ini terkait dengan aspek tertentu dari keamanan *cyber* di mana kepentingan seseorang, masyarakat atau negara, termasuk aset berbasis non-informasi mereka, perlu dilindungi dari risiko yang berasal dari interaksi dengan ruang *cyber*. Subyek ini bertujuan untuk menyoroti perbedaan antara keamanan

informasi dan keamanan *cyber*. Semua keamanan adalah tentang perlindungan aset dari berbagai ancaman yang ditimbulkan oleh kerentanan bawaan tertentu. Proses keamanan biasanya berurusan dengan pemilihan dan implementasi kontrol keamanan (juga disebut tindakan balasan) yang membantu mengurangi risiko yang ditimbulkan oleh kerentanan ini (ISO / IEC 27002, 2013; Von Solms, 2013).

B. ASET KEAMANAN INFORMASI DAN RISIKO KEAMANAN INFORMASI

Dalam kasus keamanan TIK, aset yang perlu dilindungi adalah infrastruktur teknologi informasi yang merupakan komponen dasar/utamanya. Keamanan informasi, di sisi lain, memperluas definisi aset yang akan dilindungi untuk mencakup semua aspek informasi itu sendiri. Dengan demikian, hal ini mencakup perlindungan atas aset TIK yang mendasarinya, dan mencakup bukan hanya teknologi yang digunakan untuk mengelola informasi yang dikomunikasikan secara langsung menggunakan TIK.

Seperti yang ditunjukkan dalam skenario di atas, dalam keamanan *cyber*, aset yang perlu dilindungi dapat berkisar dari individu itu sendiri hingga peralatan rumah tangga biasa, hingga kepentingan masyarakat luas, termasuk infrastruktur nasional yang kritis. Aset tersebut mutlak mencakup siapa saja atau apa pun yang bisa dijangkau melalui dunia maya.

Istilah terkait keamanan *cyber* tidak dapat dianalogikan dengan istilah keamanan informasi. Dalam keamanan dunia maya, informasi dan TIK adalah penyebab utama kerentanan. Aset yang ditangani dalam keamanan masih mungkin mencakup informasi itu sendiri, atau bahkan infrastruktur informasi dan komunikasi. Namun, satu-satunya karakteristik keamanan *cyber* yang paling menentukan adalah kenyataan bahwa semua aset yang terkait perlu dan harus dilindungi karena kerentanan yang ada dapat berakibat negatif dalam penggunaan TIK di dunia maya.

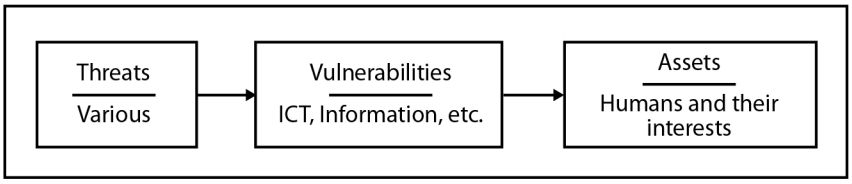
Kerentanan ini bahkan dapat memengaruhi aset tidak berwujud. Misalnya, keamanan *cyber* menambahkan dimensi etika, karena masalah seperti *cyber bullying* melampaui batas hukum dan menghadirkan masalah etika yang perlu ditangani oleh masyarakat secara umum. Dimensi etika ini kemudian meluas ke masalah seperti botnet. Menjadi bagian dari botnet tidak selalu berarti bahwa kerahasiaan, integritas, ketersediaan, atau karakteristik lain dari sumber daya informasi seseorang telah terpengaruh secara langsung; sangat mungkin bahwa botnet hanya dapat "mencuri" siklus jam di komputer sementara itu akan menjadi tidak aktif. Namun, jika botnet semacam itu digunakan untuk melakukan kejahatan, maka pemilik komputer yang bersangkutan mungkin merupakan kaki tangan yang tidak diketahui/disadarinya. Meskipun demikian, dimensi etika dari keamanan *cyber* ini bukanlah satu-satunya aset tidak berwujud yang perlu dilindungi; perlindungan atas kepercayaan yang dimiliki warga negara dalam menggunakan ruang *cyber* untuk tujuan komersial dipandang penting oleh semua negara yang kebijakannya tercakup dalam tinjauan ini.

Dengan mempertimbangkan diskusi dan skenario yang disebutkan di atas, jelaslah bahwa dalam keamanan dunia maya, aset yang perlu dilindungi melampaui batas-batas

informasi itu sendiri sebagaimana didefinisikan untuk keamanan informasi.

1. Pertama, dari skenario pertama dan kedua sangat jelas bahwa, dalam keamanan *cyber*, aset mencakup aspek pribadi atau fisik, baik yang berwujud maupun tidak berwujud, dari seorang manusia.
2. Selain itu, seperti yang dapat dilihat pada skenario ketiga dan keempat, keamanan *cyber* juga mencakup perlindungan nilai-nilai sosial (tidak berwujud) dan infrastruktur nasional (berwujud).
3. Dalam keamanan *cyber*, aset mencakup aset berwujud dan tidak berwujud yang berkaitan dengan kesejahteraan individu atau masyarakat pada umumnya.
4. Dalam kasus keamanan *cyber*, informasi itu sendiri dapat diklasifikasikan sebagai kerentanan.

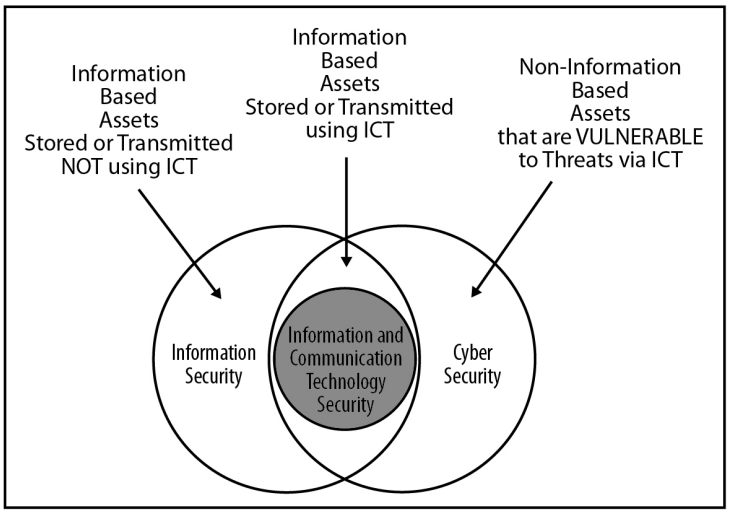
Dalam semua skenario di atas, kompromi informasi mengarah langsung pada dampak ke asset. Dalam hal ini mungkin manusia dalam kapasitas pribadinya, atau mas



Gambar 1.1
Keamanan *Cyber*

Sama seperti keamanan informasi yang diperluas pada konsep keamanan TIK untuk melindungi informasi itu sendiri, terlepas dari bentuk dan/atau lokasinya saat ini, keamanan *cyber* perlu dilihat sebagai perluasan dari keamanan informasi.

Keamanan dunia maya memiliki ruang lingkup tentang melindungi lebih dari sekadar informasi, atau sumber daya sistem informasi dari seseorang / organisasi. Keamanan *cyber* juga tentang perlindungan orang-orang yang menggunakan sumber daya di lingkungan *cyber* dan tentang perlindungan aset lainnya, termasuk aset milik masyarakat pada umumnya, yang telah terpapar risiko sebagai akibat dari kerentanan yang berasal dari penggunaan TIK. Hubungan antara ketiga konsep yang tumpang tindih ini diilustrasikan pada Gambar 1.2.



Gambar 1.2
Hubungan antara Keamanan Teknologi Informasi dan Komunikasi (TIK), Keamanan Informasi, dan Keamanan *Cyber*

Dari pembahasan di atas tampak bahwa dalam keamanan informasi dan komunikasi, aset yang akan diamankan adalah teknologi yang mendasarinya. Dalam kasus keamanan informasi, aset yang akan diamankan adalah informasi bersama dengan teknologi yang mendasarinya. Namun, dalam kasus keamanan dunia maya, tujuannya jelas bukan untuk mengamankan dunia maya melainkan untuk mengamankan mereka yang berfungsi di dunia maya, baik perorangan, organisasi, atau negara.

Karena peran TIK menjadi semakin tersebar di mana-mana dalam masyarakat maka peran yang dimainkan manusia dalam informasi yang mendasari dan proses keamanan terkait TIK akan terus berkembang. Dalam keamanan TIK, peran manusia sebagian besar dibatasi hanya sebagai ancaman. Dalam keamanan informasi peran ini telah berkembang menjadi bagian yang semakin tidak terpisahkan dari sistem pendukung dan dengan demikian manusia menjadi kerentanan. Saat ini, dalam keamanan dunia maya, manusia dan masyarakat manusia telah tumbuh menjadi bagian dari aset yang perlu dilindungi. Meski manusia masih dianggap sebagai ancaman sekaligus kerentanan, namun saat ini manusia juga dianggap sebagai aset yang perlu dilindungi di dunia maya.

Sehubungan dengan hal tersebut di atas, keamanan *cyber* dapat diartikan sebagai perlindungan terhadap:

1. dunia maya itu sendiri,
2. informasi elektronik,
3. TIK yang mendukung dunia maya, dan
4. pengguna dunia maya dalam kapasitas pribadi,
5. kemasyarakatan dan nasional, termasuk segala kepentingan, baik yang berwujud atau tidak berwujud, yang rentan terhadap serangan yang berasal dari dunia maya.

Dari definisi di atas jelaslah bahwa keamanan dunia maya jauh lebih luas daripada informasi dan/atau keamanan TIK yang dicakupnya. Unsur manusia, termasuk kepentingan nasional, memainkan peran yang terus meningkat dalam keamanan dunia maya dan tentu saja standar internasional dan praktik terbaik saat ini tidak cukup komprehensif untuk mengamankan dunia maya.

Dalam bukunya Solomon (2018) menjelaskan bahwa risiko adalah kemungkinan bahwa sesuatu yang buruk akan terjadi pada suatu aset. Risiko adalah tingkat keterpaparan dari beberapa peristiwa yang berdampak pada aset. Dalam konteks keamanan TI, aset dapat berupa komputer, *database*, atau sepotong informasi. Contoh risikonya adalah sebagai berikut.

1. Kehilangan data.
2. Kehilangan bisnis karena bencana telah menghancurkan gedung Anda.
3. Gagal mematuhi hukum dan peraturan.

Ancaman adalah tindakan apa pun yang dapat merusak aset. Sistem informasi menghadapi ancaman alami dan ancaman yang disebabkan oleh manusia. Ancaman banjir, gempa bumi, atau badai hebat mengharuskan organisasi membuat rencana untuk memastikan bahwa operasi bisnis dapat segera berlanjut dan organisasi dapat pulih. Rencana kesinambungan bisnis/*business continuity planning* (BCP) memberikan prioritas pada fungsi yang dibutuhkan organisasi untuk terus berjalan.

Rencana pemulihan bencana/*Disaster recovery planning* (DRP) menjelaskan bagaimana bisnis bangkit kembali setelah bencana besar seperti kebakaran atau badai. Ancaman yang disebabkan manusia terhadap sistem komputer termasuk virus, kode berbahaya, dan akses tidak sah. Virus adalah program komputer yang dibuat untuk menyebabkan kerusakan pada sistem, aplikasi, atau data. Kode berbahaya atau *malware*, adalah program komputer yang dibuat untuk menyebabkan terjadinya suatu tindakan tertentu, seperti menghapus *hard drive*. Ancaman ini dapat merugikan individu, bisnis, atau organisasi.

Kebanyakan orang setuju bahwa informasi pribadi harus aman. Tapi apa sebenarnya makna dari kata "mengamankan informasi"?

Informasi yang aman memenuhi tiga prinsip utama atau properti, informasi. Jika Anda dapat memastikan ketiga prinsip ini, Anda memenuhi persyaratan keamanan informasi. Ketiga prinsip tersebut yang juga sudah dijelaskan di atas adalah sebagai berikut.

1. **Kerahasiaan/*Confidentiality* (C)**, hanya pengguna resmi yang dapat melihat informasi.
2. **Integritas/*Integrity* (I)**, hanya pengguna resmi yang dapat mengubah informasi.
3. **Ketersediaan/*Availability* (A)**, informasi dapat diakses oleh pengguna yang berwenang setiap kali mereka meminta informasi.

1. Kerahasiaan/*Confidentiality*

Kerahasiaan adalah istilah umum, yang berarti menjaga informasi dari semua orang kecuali mereka yang memiliki hak atasnya. Informasi rahasia meliputi:

a. data pribadi individu,
b. kekayaan intelektual bisnis,
c. keamanan nasional untuk negara dan pemerintah.

Dengan pertumbuhan *e-commerce*, lebih banyak orang melakukan pembelian *online* dengan kartu kredit. Ini mengharuskan orang memasukkan data pribadi ke situs *web* e-niaga. Konsumen harus berhati-hati dalam melindungi identitas pribadi dan data pribadinya. Hukum mewajibkan organisasi untuk menggunakan kontrol keamanan untuk melindungi data pribadi pelanggan.

Di Indonesia, UU ITE memang belum memuat aturan perlindungan data pribadi secara khusus. Namun dalam ketentuannya, terdapat Pasal 26 ayat (1) dan penjelasannya UU 19/2016, yang berbunyi:

Pasal 26 ayat (1) UU 19/2016:

> Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan.

Penjelasan Pasal 26 ayat (1) UU 19/2016:

Dalam pemanfaatan teknologi informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut.

a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai.
c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Jika terjadi penggunaan data pribadi seseorang tanpa izin dari orang yang bersangkutan, maka orang yang dilanggar haknya itu dapat mengajukan gugatan atas kerugian yang ditimbulkan. Selain UU ITE terdapat peraturan tingkat menteri, Menteri Komunikasi dan Informatika telah mengeluarkan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Perlindungan Data Pribadi Dalam Sistem Elektronik. Di dalamnya antara lain memuat ketentuan tentang hak pemilik data pribadi, kewajiban pengguna data pribadi, kewajiban penyelenggara sistem elektronik, dan penyelesaian sengketa.

Kontrol keamanan adalah sesuatu yang dilakukan organisasi untuk membantu mengurangi risiko. Contoh dari pengendalian tersebut meliputi berikut ini.

a. Mengadakan pelatihan kesadaran keamanan tahunan untuk karyawan. Kegiatan ini membantu mengingatkan staf tentang penanganan data pribadi yang benar. Ini juga mendorong kesadaran tentang kerangka kerja organisasi tentang kebijakan, standar, prosedur, dan pedoman keamanan.
b. Menerapkan kerangka kebijakan keamanan TI. Kerangka kebijakan seperti garis besar yang mengidentifikasi di mana kontrol keamanan harus digunakan.
c. Merancang solusi keamanan berlapis untuk infrastruktur TI. Semakin banyak lapisan atau kompartemen yang memblokir atau melindungi data pribadi dan kekayaan intelektual, semakin sulit data dan properti tersebut untuk ditemukan dan dicuri.
d. Melakukan penilaian risiko keamanan, audit, dan *penetration testing* secara berkala pada situs *web* dan infrastruktur TI. Beginilah cara profesional keamanan memverifikasi bahwa mereka telah menginstal kontrol dengan benar.
e. Mengaktifkan insiden keamanan dan pemantauan peristiwa di titik masuk dan keluar internet Anda. Tindakan ini seperti menggunakan mikroskop untuk melihat apa yang masuk dan keluar.
f. Menggunakan antivirus pada *workstation* dan *server* yang bersifat otomatis serta memberi perlindungan dari *software* yang berbahaya. Hal ini merupakan cara untuk mencegah virus dan *software* berbahaya masuk ke komputer Anda.
g. Menggunakan kontrol akses yang lebih ketat di luar ID masuk dan *password* untuk sistem, aplikasi, dan data yang sensitif. ID *logon* dengan *password* hanya merupakan salah satu pemeriksaan pengguna. Akses ke sistem yang lebih sensitif harus menjalani pengujian kedua untuk mengkonfirmasi identitas pengguna.
h. Meminimalkan kelemahan perangkat lunak di komputer dan *server* Anda dengan memperbarui *patch* dan perbaikan keamanan. Tindakan ini merupakan cara untuk selalu memperbarui sistem operasi dan *software* aplikasi Anda.

Melindungi data pribadi adalah merupakan proses untuk memastikan kerahasiaan data. Organisasi harus menggunakan kontrol keamanan yang tepat khusus untuk masalah ini.

Beberapa contohnya adalah sebagai berikut.

a. Mendefinisikan kebijakan, standar, prosedur, dan pedoman di seluruh organisasi untuk melindungi data rahasia. Subyek tersebut berisi petunjuk tentang tata cara menangani data pribadi.
b. Mengadopsi standar klasifikasi data yang menentukan cara menangani data di seluruh infrastruktur TI Anda. Subyek tersebut merupakan peta jalan untuk dapat mengidentifikasi tentang jenis kendali/kontrol yang diperlukan untuk menjaga keamanan data.
c. Membatasi akses ke dalam sistem dan aplikasi yang menyimpan data rahasia hanya bagi mereka yang berwenang untuk menggunakan data itu.

d. Menggunakan teknik kriptografi untuk menyembunyikan data rahasia dan menjaga agar data tersebut tidak terlihat oleh pengguna yang tidak berwenang.
e. Mengenkripsi data yang melintasi jalur internet publik.
f. Mengenkripsi data yang disimpan dalam *database* dan perangkat penyimpanan.

Mengirim data ke komputer lain menggunakan jaringan terutama untuk jaringan publik berarti Anda harus mengambil langkah-langkah khusus untuk menjaga kerahasiaan data pengguna dari intipan/endusan (*sniffing*) pihak yang tidak berwenang. Kriptografi merupakan cara/praktik untuk menyembunyikan data dan menjauhkannya dari pengguna yang tidak sah. Enkripsi merupakan proses untuk mengubah data dari *cleartext* menjadi *ciphertext*. Data *cleartext* adalah data yang sifatnya terbuka dan dapat dibaca siapa saja secara mudah. *Ciphertext* adalah data yang diacak yang merupakan hasil enkripsi *cleartext*.

2. Integritas/*Integrity*

Integritas berkaitan dengan validitas dan akurasi data. Data yang kurang integritasnya adalah data yang tidak akurat atau tidak *valid*; data yang berintegritas rendah tidak akan digunakan oleh pihak yang berkepentingan. Bagi beberapa organisasi, data dan informasi merupakan aset yang bersifat intelektual properti. Sebagai contoh adalah subyek-subyek yang termasuk dalam kelompok hak cipta, paten, formula rahasia, dan *database* pelanggan.

Informasi ini dapat memiliki nilai yang besar. Perubahan yang terjadi secara tidak sah dapat merusak nilai dan makna data tersebut. Inilah penyebab bahwa integritas data merupakan salah satu prinsip utama dalam keamanan sistem. Sabotase dan korupsi atas integritas data merupakan ancaman serius bagi organisasi, terutama jika data tersebut penting untuk operasi bisnis.

3. Ketersediaan/*Availability*

Ketersediaan adalah istilah umum dalam kehidupan sehari-hari. Misalnya, Anda mungkin memperhatikan ketersediaan layanan internet Anda, layanan TV, atau layanan ponsel. Dalam konteks keamanan informasi, ketersediaan umumnya dinyatakan sebagai jumlah waktu pengguna dapat menggunakan sistem, aplikasi, dan data. Pengukuran waktu ketersediaan secara umum meliputi berikut ini.

a. *Uptime*; *Uptime* adalah jumlah total waktu sistem, aplikasi, dan data dapat diakses. *Uptime* biasanya diukur dalam satuan detik, menit, dan jam dalam satu bulan kalender tertentu. Sering kali *uptime* dinyatakan sebagai persentase waktu yang tersedia, misal: 99,5 persen waktu aktif.
b. Waktu Henti (*Down-time*); Waktu Henti adalah jumlah total waktu sistem, aplikasi, dan data tidak dapat diakses. Waktu henti juga diukur dalam satuan detik, menit, dan jam untuk satu bulan kalender.

c. Ketersediaan (*Availability*); Ketersediaan adalah fungsi perhitungan matematis di mana A = (Total Waktu Aktif) / (Total Waktu Aktif + Total Waktu Henti).
d. *Mean time to failure* (MTTF); MTTF adalah jumlah waktu rata-rata antara kegagalan untuk sistem tertentu. Semikonduktor dan elektronik tidak rusak dan memiliki MTTF bertahun-tahun (25 tahun atau lebih, dan lain-lain). Komponen fisik seperti konektor, kabel, kipas, dan catu daya memiliki MTTF yang jauh lebih rendah (lima tahun atau kurang), mengingat keausan dapat merusaknya.
e. *Mean time to repair* (MTTR); MTTR adalah jumlah rata-rata waktu yang diperlukan untuk memperbaiki sistem, aplikasi, atau komponen. Tujuannya adalah untuk mengembalikan sistem dengan cepat.
f. *Mean time between failures* (MTBF); MTBF adalah perkiraan jumlah waktu antara suatu kegagalan sistem TI dengan kegagalan berikutnya selama beroperasi.
g. *Recovery time objective* (RTO); RTO adalah jumlah waktu yang diperlukan untuk memulihkan dan membuat sistem atau aplikasi agar dapat kembali beroperasi, dan data dapat kembali tersedia untuk digunakan setelah pemadaman. Rencana kesinambungan bisnis biasanya menetapkan RTO untuk suatu sistem, aplikasi, dan akses data karena merupakan komponen yang sangat penting.

Penyedia layanan telekomunikasi dan internet menawarkan perjanjian tingkat layanan/*Service level agreement* (SLA) kepada pelanggan mereka. SLA adalah merupakan suatu kontrak yang menjamin ketersediaan layanan bulanan minimum untuk *wide area network* (WAN) dan tautan akses Internet. SLA biasanya menyertai layanan WAN dan tautan akses internet yang disediakan untuk kepentingan khusus. Faktor ketersediaan ini biasanya digunakan untuk mengukur komitmen tingkat layanan waktu operasional bulanan. Seperti dalam contoh waktu henti layanan selama 30 menit dalam 30 hari kalender berarti sama dengan ketersediaan 99,993 persen. Penyedia jasa layanan Internet biasanya menawarkan SLA mulai dari 99,5 persen hingga 99,999 persen ketersediaan.

C. EVALUASI KEAMANAN INFORMASI

Pendekatan OCTAVE digunakan untuk melakukan evaluasi keamanan secara mandiri. Metodologi ini dikembangkan di *CERT(R) Coordination Center.*

Pendekatan ini dirancang untuk membantu Anda dalam melakukan hal berikut.

1. Identifikasi dan rangking aset informasi utama.
2. Pertimbangkan ancaman terhadap aset tersebut.
3. Analisis kerentanan yang melibatkan teknologi dan praktik.

OCTAVE (SM) memungkinkan organisasi untuk mengembangkan prioritas keamanan berdasarkan masalah bisnis khusus organisasi. Pendekatan tersebut memberikan kerangka kerja yang koheren untuk menyelaraskan tindakan keamanan dengan tujuan keseluruhan. Mengelola Risiko Keamanan Informasi, yang ditulis

oleh pengembang OCTAVE, adalah merupakan suatu panduan lengkap dan pedoman implementasinya.

Pada saat ini sering membuat kita bingung dalam memilih metode yang paling tepat untuk mengevaluasi risiko keamanan informasi bagi kondisi kita. Sebagian besar metode saat ini bersifat *"bottom-up"*: yang di mulai dengan infrastruktur komputasi dan berfokus pada kerentanan teknologi tanpa mempertimbangkan risiko terhadap misi dan tujuan bisnis organisasi. Alternatif yang lebih baik adalah dengan melihat organisasi itu sendiri dan mengidentifikasi apa yang perlu dilindungi, menentukan mengapa berisiko, dan mengembangkan solusi yang membutuhkan solusi berbasis teknologi dan praktik.

Karakteristik pendekatan evaluasi risiko keamanan informasi yang komprehensif adalah sebagai berikut.

1. Menggabungkan aset, ancaman, dan kerentanan.
2. Memungkinkan pembuat keputusan untuk mengembangkan prioritas relatif berdasarkan apa yang penting bagi organisasi.
3. Menggabungkan masalah organisasi yang berkaitan dengan bagaimana orang menggunakan infrastruktur komputasi untuk memenuhi tujuan bisnis organisasi.
4. Menggabungkan masalah teknologi yang terkait dengan konfigurasi infrastruktur komputasi.
5. Harus menjadi metode fleksibel yang dapat disesuaikan secara unik untuk setiap organisasi.

Salah satu cara untuk membuat pendekatan evaluasi yang peka konteks adalah dengan menetapkan seperangkat persyaratan dasar untuk evaluasi dan kemudian mengembangkan serangkaian, atau kelompok, metode yang memenuhi persyaratan tersebut. Setiap metode dalam pendekatan dapat ditargetkan ke lingkungan atau situasi operasional yang unik.

OCTAVE menyusun proyek *Operationally Critical Threat, Asset, and Vulnerability Evaluation* [SM] (OCTAVE [SM]) untuk mendefinisikan pendekatan sistematis dan berskala organisasi untuk mengevaluasi risiko keamanan informasi dengan menerapkan beberapa metode yang konsisten. Proyek tersebut juga merancang pendekatan untuk dapat diarahkan secara mandiri, dan memungkinkan individu untuk mempelajari tentang masalah keamanan dan meningkatkan postur keamanan organisasi mereka tanpa ketergantungan kepada pihak luar. Evaluasi mandiri yang dilakukan hanya memberikan petunjuk/arahan untuk kegiatan keamanan informasi organisasi. Hasil atau peningkatan keamanan tidak akan terjadi kecuali jika organisasi tersebut melakukan tindak lanjut dengan cara menerapkan hasil evaluasi dan mengelola risiko keamanan informasinya.

Sangat mudah untuk mengabaikan fakta bahwa keamanan informasi dapat mempengaruhi organisasi secara keseluruhan. Namun pada akhirnya, hal ini adalah masalah bisnis yang solusinya harus melibatkan lebih dari sekadar penerapan teknologi informasi seperti penggunaan *firewall* dan *patch virus*. Beberapa survei tentang insiden dan pelanggaran keamanan menunjukkan bahwa sebagian besar pelanggaran keamanan

terjadi dari dalam, bukan dari serangan pihak luar yang melakukan uji coba dalam rangka belajar. Namun survei terbaru menunjukkan bahwa mayoritas serangan memang datang dari luar. Terdapat beberapa indikator lain yang menyatakan bahwa serangan paling mahal datang dari dalam, padahal frekuensi serangan tertinggi datang dari pihak luar.

Dengan menafikan data statistik yang ada, Anda tetap perlu mempertimbangkan akan kehadiran ancaman dari pihak internal maupun eksternal. Organisasi Anda hanya seaman *link* terlemahnya, dan mungkin *link* tersebut adalah diri Anda sendiri. Berapa banyak orang yang dapat menyatakan dengan pasti bahwa mereka sengaja atau tidak sengaja mengungkapkan *password* mereka dalam satu tahun terakhir? Berapa banyak yang memiliki *file* di handphone / laptop mereka yang mencantumkan *password* atau berisi informasi rahasia? Berapa banyak yang memiliki " *yellow stickies*" (kertas catatan kecil) di bawah keyboard? Berapa banyak karyawan yang memuat *game* di *workstation* mereka atau membuka lampiran *email* yang tidak dikenal? Berapa banyak perusahaan yang menghabiskan waktu dan uangnya untuk mengikuti *patch* terbaru dan alat keamanan teknologi? Tanpa praktik organisasi yang baik dan tetap ditegakkan, selain pengamanan teknologi, organisasi dan asset perusahaan akan selalu berada dalam risiko.

Keamanan informasi lebih dari sekadar menyiapkan *firewall*, menerapkan *patch* untuk memperbaiki kerentanan yang baru ditemukan di perangkat lunak sistem Anda, atau mengunci kabinet yang berisi *tape backup* Anda. Keamanan informasi menentukan apa yang perlu dilindungi dan mengapa, serta bagaimana cara melindunginya. Pertanyaan yang utama tentu saja adalah bagaimana memastikan organisasi Anda memiliki tingkat keamanan yang memadai dari waktu ke waktu. Ada banyak jawaban untuk pertanyaan yang menantang ini, sama seperti ada banyak pendekatan untuk mengelola keamanan organisasi. Sayangnya, tidak ada satu solusi yang tepat, tidak ada solusi tunggal yang akan menyelesaikan semua masalah Anda.

Ada empat pendekatan umum untuk menganalisa masalah ini.

1. Penilaian kerentanan/*vulnerability assessment.*
2. Audit sistem informasi.
3. Evaluasi risiko keamanan informasi.
4. Mengelola *service provider/*penyedia layanan.

Berikut adalah uraian singkat dari masing-masing pendekatan di atas:

1. Penilaian Kerentanan/*Vulnerability Assessment*

Penilaian kerentanan adalah pemeriksaan secara sistematis dan tepat waktu atas dasar teknologi, kebijakan, dan prosedur organisasi. Hal ini mencakup analisis lengkap tentang keamanan lingkungan komputasi internal dan kerentanannya terhadap serangan internal dan eksternal.

Penilaian berbasis teknologi ini umumnya:

a. menggunakan standar untuk aktivitas keamanan TI tertentu (seperti memperkuat

jenis *platform* tertentu);

b. menilai seluruh infrastruktur komputer;

c. menggunakan perangkat lunak (terkadang berlisensi) untuk menganalisis infrastruktur dan semua komponennya;

d. memberikan analisis terperinci dengan menunjukkan kerentanan teknologi yang terdeteksi dan mungkin merekomendasikan langkah-langkah khusus untuk mengatasi kerentanan tersebut.

2. Audit Keamanan Informasi

Audit sistem informasi adalah penilaian secara independen atas pengendalian internal perusahaan untuk memastikan bahwa manajemen, otoritas pengatur, dan pemegang saham perusahaan memperoleh informasi tersebut secara akurat dan valid. Audit biasanya akan memanfaatkan model proses khusus industri dengan, tolok ukur dan standar kehati-hatian, atau praktik terbaik yang telah pernah ditetapkan. Mereka melihat kinerja kelompok keuangan dan operasional. Suatu audit juga dapat didasarkan pada pengendalian risiko atas proses bisnis, metode dan alat analisis. Audit umumnya dilakukan oleh auditor berlisensi atau bersertifikat dan memiliki implikasi hukum dan kewajiban. Selama audit, catatan bisnis perusahaan ditinjau keakuratan dan integritasnya.

3. Evaluasi Risiko Keamanan Informasi

Evaluasi risiko keamanan memperluas penilaian kerentanan untuk melihat risiko terkait keamanan dalam perusahaan, termasuk sumber risiko internal dan eksternal serta risiko berbasis elektronik, berbasis manusia, dan bencana alam. Evaluasi multifaset ini berupaya menyelaraskan evaluasi risiko dengan pendorong atau sasaran bisnis dan biasanya berfokus pada empat aspek keamanan berikut.

a. Memeriksa praktik perusahaan yang berkaitan dengan keamanan untuk mengidentifikasi kekuatan dan kelemahan yang dapat membuat atau mengurangi risiko keamanan. Prosedur ini dapat mencakup analisis komparatif yang memberi peringkat informasi terhadap standar industri dan praktik terbaik.

b. Memeriksa teknologi sistem, tinjauan kebijakan, dan keamanan fisik.

c. Memeriksa infrastruktur TI untuk menentukan kerentanan teknologi. Kerentanan tersebut mencakup kerentanan terhadap salah satu situasi berikut.
   1) Sebuah pengenalan kode berbahaya.
   2) Kerusakan atau penghancuran data.
   3) Eksfiltrasi informasi.
   4) Kegagalan layanan.
   5) Perubahan hak akses dan hak istimewa yang tidak sah.

d. Membantu pembuat keputusan memeriksa *trade-off* untuk memilih tindakan pencegahan yang hemat biaya.

4. Mengelola *Security Service Provider*/Penyedia Layanan Keamanan

Mengelola keamanan penyedia layanan umumnya mengandalkan keahlian

manusia dalam/untuk mengelola sistem dan jaringan perusahaan. *Vendor* menggunakan perangkat lunak dan perangkat keamanan milik sendiri atau dari *vendor* lain untuk melindungi infrastruktur Anda. Biasanya, pengelola keamanan layanan akan secara proaktif memantau dan melindungi infrastruktur komputasi organisasi dari serangan dan penyalahgunaan. Solusi yang diberikan umumnya cenderung disesuaikan dengan kebutuhan bisnis dari setiap klien. *Vendor* dapat secara aktif menanggapi gangguan atau memberi tahu bahwa telah terjadi suatu abnormalitas pada sistem yang dipantau. Beberapa *vendor* menggunakan *computer-based learning and analysis*, yang diharapkan dapat memberikan penurunan waktu respons dan peningkatan akurasi.

Penilaian kerentanan, audit sistem informasi, dan evaluasi risiko keamanan informasi diharapkan dapat membantu Anda dalam mengkarakterisasi masalah keamanan pada sistem Anda, tetapi tidak mengelolanya. Pengelola penyedia layanan yang melakukan pengelolaan keamanan sistem untuk Anda.

Meskipun masing-masing pendekatan ini dapat berguna untuk organisasi yang mencoba melindungi dirinya sendiri, semuanya tetap memiliki beberapa batasan, berdasarkan konteks penggunaannya. Perusahaan kecil mungkin tidak punya pilihan selain menggunakan penyedia layanan. Perusahaan dengan sumber daya TI yang terbatas mungkin tidak dapat melakukan lebih dari sekadar mengelola kerentanan, dan bergantung pada apa yang harus dilindungi, mungkin tidak perlu melakukan lebih banyak lagi. Bagian selanjutnya adalah untuk melihat pendekatan yang lebih komprehensif yang dibangun di atas pendekatan sebelumnya, mengkaji kemungkinan organisasi untuk memikul tanggung jawab dan mengelola masalah keamanannya.

Pikirkan tentang seberapa besar Anda mengandalkan akses ke informasi dan sistem agar dapat melakukan pekerjaan Anda. Pada saat ini, sistem informasi sangat penting bagi sebagian besar organisasi, karena hampir semua informasi ditangkap, disimpan, dan diakses dalam bentuk digital. Para pengguna dan pebisnis mengandalkan data digital yang dapat diakses, handal dan terlindungi dari penyalahgunaan. Setiap sistem saling berhubungan dengan cara yang tidak dapat dibayangkan belasan tahun yang silam. Sistem jaringan telah memungkinkan akses yang belum pernah terjadi sebelumnya. Sayangnya, teknologi ini juga mampu untuk membeberkan segala informasi yang ada sehingga menimbulkan berbagai ancaman baru.

Pada saat ini, banyak organisasi telah menerapkan berbagai macam infrastruktur komputasi yang kompleks. Mereka membutuhkan pendekatan yang fleksibel yang memungkinkan mereka untuk dapat memahami risiko keamanan informasi secara spesifik dan kemudian membuat strategi untuk mengatasi risiko tersebut.

Organisasi yang ingin meningkatkan keamanan harus siap mengambil langkah-langkah berikut.

a. Ubah dari pendekatan reaktif berbasis masalah ke pencegahan masalah secara proaktif.
b. Pertimbangkan keamanan dari berbagai perspektif.
c. Membangun infrastruktur yang fleksibel di semua tingkat organisasi yang mampu merespons dengan cepat untuk mengubah kebutuhan teknologi dan keamanan.

d. Memulai upaya berkelanjutan untuk memelihara dan meningkatkan keamanan.

Latihan

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

1) Jelaskan pengertian keamanan informasi!
2) Jelaskan tujuan dari menerapkan keamanan informasi bagi organisasi/perusahaan!
3) Jelaskan perbedaan keamanan *cyber*, keamanan informasi, dan keamanan TIK!
4) Apakah risiko keamanan informasi itu?
5) Jelaskan bagaimana organisasi/perusahaan menerapkan evaluasi risiko keamanan informasi!

Petunjuk Jawaban Latihan

1) Keamanan informasi menurut standar internasional, ISO / IEC 27002 (2013), mendefinisikan bahwa keamanan informasi sebagai pengembangan dari kerahasiaan, integritas dan ketersediaan informasi.
2) Tujuan keamanan informasi adalah untuk memastikan kelangsungan bisnis dan meminimalkan kerusakan bisnis dengan membatasi dampak insiden keamanan, dengan tepat mengacu pada tujuan keamanan secara umum yaitu *integrity, availability, confidentiality.*
3) Keamanan *cyber* adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi serta aset pengguna. Keamanan informasi menurut standar internasional, ISO / IEC 27002 (2013), didefinisikan sebagai pengembangan dari kerahasiaan, integritas dan ketersediaan informasi. Keamanan teknologi informasi dan komunikasi (TIK) berkaitan dengan perlindungan berbasis teknologi yang meliputi, sistem tempat informasi umumnya disimpan dan/atau disebarluaskan, yang mencakup semua aspek yang berkaitan dengan mendefinisikan, mencapai dan menjaga kerahasiaan, integritas, ketersediaan, non-penyangkalan, akuntabilitas, keaslian, dan keandalan sumber daya informasi.
4) Risiko keamanan informasi adalah penilaian kerentanan untuk melihat risiko terkait keamanan dalam perusahaan, termasuk sumber risiko internal dan eksternal serta risiko berbasis elektronik, berbasis manusia dan bencana alam.
5) Cara organisasi menerapkan evaluasi risiko keamanan informasi adalah sebagai berikut.
   a) Penilaian kerentanan/*vulnerability assessment.*
   b) Audit sistem informasi.

c) Evaluasi risiko keamanan informasi.
d) Mengelola *service provider/*penyedia layanan.

Rangkuman

1. Keamanan *cyber* adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi serta aset pengguna.
2. Keamanan informasi menurut standar internasional, ISO / IEC 27002 (2013), didefinisikan sebagai pengembangan dari kerahasiaan, integritas dan ketersediaan informasi. Informasi dapat mengambil berbagai bentuk, dapat dicetak atau ditulis di atas kertas, disimpan secara elektronik melalui pos atau sarana elektronik, ditampilkan di film, disampaikan dalam percakapan, dan sebagainya.
3. Keamanan teknologi informasi dan komunikasi (TIK) berkaitan dengan perlindungan berbasis teknologi yang meliputi, sistem tempat informasi umumnya disimpan dan / atau disebarluaskan, yang mencakup semua aspek yang berkaitan dengan mendefinisikan, mencapai dan menjaga kerahasiaan, integritas, ketersediaan, non-penyangkalan, akuntabilitas, keaslian, dan keandalan sumber daya informasi.
4. Tujuan keamanan informasi adalah untuk memastikan kelangsungan bisnis dan meminimalkan kerusakan bisnis dengan membatasi dampak insiden keamanan, dengan tepat mengacu pada tujuan keamanan secara umum yaitu *integrity, availability, confidentiality.*
5. Evaluasi risiko keamanan informasi adalah proses yang dapat membantu Anda memenuhi tujuan keamanan informasi itu sendiri.

Tes Formatif 2

Pilihlah satu jawaban yang paling tepat!

1) Prinsip .... dari keamanan sistem informasi berkaitan dengan tujuan waktu pemulihan.
   A. kerahasiaan
   B. integritas
   C. ketersediaan
   D. risiko

2) Produsen perangkat lunak membatasi tanggung jawab mereka saat menjual perangkat lunak, menggunakan manakah dari berikut ini?
   A. *End User Licency Agreement*
   B. Perjanjian kerahasiaan
   C. Perjanjian pengembangan perangkat lunak
   D. Dengan mengembangkan *error free software and code* sehingga tidak ada

kewajiban

3) Organisasi yang memerlukan perwakilan layanan pelanggan untuk mengakses data pelanggan pribadi dapat melindungi privasi pelanggan dan membuatnya mudah untuk mengakses data pelanggan lainnya dengan menggunakan kontrol keamanan mana dari berikut ini?
   A. Mencegah perwakilan layanan pelanggan mengakses data pelanggan pribadi
   B. Memblokir detail data pribadi pelanggan dan mengizinkan akses hanya ke empat digit terakhir nomor jaminan sosial atau nomor rekening
   C. Mengenkripsi semua data pelanggan
   D. Menerapkan *second-tier authentication* saat mengakses *database* pelanggan

4) Anda dapat membantu memastikan kerahasiaan dengan menerapkan ....
   A. sebuah standar klasifikasi data
   B. kerangka kebijakan keamanan TI
   C. jaringan pribadi virtual untuk akses jarak jauh
   D. kontrol akses yang aman

5) Kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi serta aset pengguna adalah pengertian dari ....
   A. keamanan *cyber*
   B. keamanan informasi
   C. keamanan teknologi informasi
   D. evaluasi risiko keamanan informasi

6) Memaksimalkan ketersediaan utama yang terlibat untuk meminimalkan ....
   A. jumlah waktu henti untuk pulih dari bencana
   B. waktu rata-rata untuk memperbaiki sistem atau aplikasi
   C. waktu henti dengan menerapkan rencana kesinambungan bisnis
   D. tujuan waktu pemulihan

7) Keamanan informasi khusus untuk mengamankan informasi, sedangkan keamanan sistem informasi adalah difokuskan pada keamanan sistem informasi rumah.
   A. Benar
   B. Salah

8) Menggunakan kebijakan keamanan, standar, prosedur, dan pedoman membantu organisasi mengurangi risiko dan ancaman.
   A. Benar
   B. Salah

9) Memastikan kelangsungan bisnis dan meminimalkan kerusakan bisnis dengan membatasi dampak insiden keamanan adalah pengertian dari ....
   A. keamanan *cyber*
   B. keamanan informasi
   C. keamanan teknologi informasi
   D. tujuan keamanan informasi

10) Audit sistem informasi adalah bentuk implementasi dari ....
   A. *confidentiality*
   B. evaluasi keamanan informasi
   C. *integrity*
   D. *availability*

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.

$$\text{Tingkat Penguasaan} = \frac{\text{Jumlah Jawaban yang Benar}}{\text{Jumlah Soal}} \times 100$$

Arti tingkat penguasaan

<70%	70% - 79%	80% - 89%	90% - 100%
kurang	cukup	baik	baik sekali

Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan meneruskan modul selanjutnya. Bagus! Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 2, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

1) C
2) A
3) C
4) B
5) D
6) C
7) A
8) A
9) B
10) B

Tes Formatif 2

1) C
2) A
3) B
4) A
5) A
6) A
7) B
8) A
9) D
10) B

Daftar Pustaka

https://cyberthreat.id. (2020, 8 mei). 13 *Kasus peretasan data terbesar sepanjang masa,* diakses pada 9 maret 2021, dari https://cyberthreat.id/read/6570/13-Kasus-Peretasan-Data-Terbesar-Sepanjang-Masa.

https://www.kompas.com. (2020, 3 mei). *Tokopedia diretas, Ini 3 upaya peretasan e-commerce yang pernah terjadi*, diakses pada 9 maret 2021, dari https://www.kompas.com/tren/read/2020/05/03/162700365/tokopedia-diretas-ini-3-upaya-peretasan-e-commerce-yang-pernah-terjadi?page=all.

https:// malwarebytes.com/. (2020, 23 juni). *A zero-day guide for 2020: Recent attacks and advanced preventive techniques*, diakses pada 9 maret 2021, dari https://blog.malwarebytes.com/exploits-and-vulnerabilities/2020/06/a-zero-day-guide-for-2020/.

https://owasp.org. (2021). *OWASP top ten*, diakses pada tanggal 13 maret 2021, dari https://owasp.org/www-project-top-ten/.

https://www.hukumonline.com. (2020, 4 agustus). *Dasar hukum perlindungan data pribadi pengguna internet*, diakses pada tanggal 15 maret 2021, dari https://www.hukumonline.com/klinik/detail/ulasan/lt4f235fec78736/dasar-hukum-perlindungan-data-pribadi-pengguna-internet/.

Glosarium

Penetration testing : suatu kegiatan dimana seseorang mencoba mensimulasikan serangan yang bisa dilakukan terhadap jaringan organisasi/ perusahaan tertentu untuk menemukan kelemahan yang ada pada sistem jaringan tersebut. Orang yang melakukan kegiatan ini disebut penetration tester (disingkat pentester).

Software Patch : sebuah program kecil yang digunakan untuk menutup celah *code* yang ada di *software* tersebut.