KEAMANAN INFORMASI

Article · May 2019

CITATIONS
0

READS
298

1 author:

Gita Oktavianti
Universitas Mercu Buana
27 PUBLICATIONS **6** CITATIONS

SEE PROFILE

TUGAS SISTEM INFORMASI MANAJEMEN:

KEAMANAN INFORMASI DALAM PEMANFAATAN TEKNOLOGI INFORMASI PADA GITA BUSANA

Disusun Oleh: Gita Oktavianti (43217120060)

Dosen Pengampu: Yananto Mihadi Putra, SE., M.Si

ABSTRAK

Pada era pertumbuhan sistem informasi yang sangat cepat saat ini keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan, karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan. Pada dasarnya suatu sistem yang aman akan melindungi data didalamnya seperti identifikasi pemakai (*user identification*), pembuktian keaslian pemakai (*user authentication*), otorisasi pemakai (*user authorization*).

Beberapa kemungkinan serangan (*Hacking*) yang dapat dilakukan, seperti *Intrusion*, *denial of services, joyrider, vandal, hijacking, sniffing, spoofing* dan lain-lain. Ancaman terhadap sistem informasi banyak macamnya, antara lain: pencurian data, penggunaan sistem secara ilegal, penghancuran data secara ilegal, modifikasi data secara ilegal, kegagalan pada sistem, kesalahan manusia (SDM-sumber daya manusia), bencana alam.

Tujuan dari keamanan informasi yaitu mencegah ancaman terhadap sistem serta mendeteksi dan memperbaiki kerusakan yang terjadi pada sistem.

Kata kunci: Sistem informasi, keamanan informasi.

ABSTRACT

In the era of rapid growth of information systems at this time the security of information is something that must be considered, because if an information can be accessed by people who are not entitled or irresponsible, then the accuracy of the information will be doubted, it will even become information misleading. Basically a safe system will protect the data inside such as user identification, proof of authenticity of users, user authorization.

Some possible attacks (Hacking) that can be done, such as Intrusion, denial of services, joyrider, vandalism, hijacking, sniffing, spoofing and others. There are many kinds of threats to information systems, including: data theft, illegal system use, illegal data destruction, illegal data modification, system failure, human error (human resources), natural disasters.

The purpose of information security is to prevent threats to the system and detect and repair damage that occurs on the system.

Keywords: Information systems, information security.

PENDAHULUAN

A. Latar Belakang

Semua organisasi memiliki kebutuhan untuk menjaga agar sumber daya informasi mereka aman. Kalangan industri telah lama menyadari kebutuhan untuk menjaga keamanan dari para kriminal komputer dan sekarang pemerintah telah mempertinggi tingkat keamanan sebagai salah satu cara untuk memerangi terorisme, isu-isu utama mengenai keamanan versus ketersediaan serta keamanan versus hak pribadi harus diatasi.

Keamanan informasi ditujukan untuk mendapatkan kerahasiaan, ketersediaan, serta integritas pada semua sumber daya informasi perusahaan. Manajemen keamanan informasi terdiri atas perlindungan harian, yang disebut manajemen keamanan informasi dan persiapan operasional setelah suatu bencana yang disebut dengan manajemen keberlangsungan bisnis.

Keamanan sistem informasi pada saat ini telah banyak dibangun oleh para kelompok analis dan *programmer* namun pada akhirnya ditinggalkan oleh para pemakainya. Hal tersebut terjadi karena sistem yang dibangun lebih berorientasi pada pembuatnya sehingga berakibat sistem yang dipakai sulit untuk digunakan atau kurang user friendly bagi pemakai, sistem kurang interaktif dan kurang memberi rasa nyaman bagi pemakai, sistem sulit dipahami *interface* dari sistem menu dan tata letak kurang memperhatikan kebiasaan perilaku pemakai, sistem dirasa memaksa bagi pemakai dalam mengikuti prosedur yang dibangun sehingga sistem terasa kaku dan kurang dinamis, keamanan dari sistem informasi yang dibangun tidak terjamin.

Hal-hal yang disebutkan diatas dapat disimpulkan bahwa dalam membangun sebuah keamanan sistem informasi harus memiliki orientasi yang berbasis perspektif bagi pemakai bukan menjadi penghalang atau bahkan mempersulit dalam proses transaksi dan eksplorasi dalam pengambilan keputusan. Terdapat banyak cara untuk mengamankan data maupun informasi pada sebuah sistem. Pengamanan data dapat dibagi menjadi dua jenis yaitu: penecegahan dan pengobatan. Pencegahan dilakukan supaya data tidak rusak, hilang dan dicuri, sementara pengobatan dilakukan apabila data sudah terkena virus, sistem terkena *worm*, dan lubang keamanan sudah diexploitasi.

Keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan. Masalah tersebut penting karena jika sebuah informasi dapat di akses oleh orang yang

tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan.

Dua pendekatan dapat dilakukan untuk menyusun strategi-strategi *Information Security management*-ISM manajemen risiko dan kepatuhan tolak ukur. Perhatian akan ancaman dan resiko berhubungan dengan pendekatan manajemen risiko. Ancaman dapat bersifat internal atau eksternal, tidak disengaja atau disengaja. Risiko dapat mencakup insiden pengungkapan, penggunaan, dan modifikasi yang tidak diotorisasi serta pencurian, penghancuran dan penolakan layanan. Ancaman yang paling ditakuti adalah virus komputer. Ada tiga jenis pengendalian yang tersedia yaitu: pengendalian teknis, pengendalian formal, dan pengendalian informal.

Manajemen keberlangsungan bisnis terdiri atas seperangkat subrencana untuk menjaga keamanan karyawan, memungkinkan keberlangsungan operasional dengan cara menyediakan fasilitas mengembangkan rencana kontinjensi baru tidak harus dari awal; beberapa model berbasis peranti lunak tersedia, seperti halnya garis besar dan panduan dari pemerintah.

B. Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka rumusan masalah dari artikel ini adalah:

1. Apa yang dimaksud dengan keamanan informasi?
2. Apa saja tujuan keamanan informasi?
3. Bagaimana ancaman dan risiko keamanan informasi?
4. Bagaimana pengendalian terhadap ancaman dan risiko keamanan informasi?
5. Bagaimana kebutuhan organisasi akan keamanan dan pengendalian?
6. Bagaimana manajemen keamanan informasi?
7. Apa yang dimaksud dengan ancaman dan apa saja jenis ancaman?
8. Apa yang dimaksud dengan risiko dan bagaimana manajemen risiko?
9. Bagaimana manajemen risiko dan kebijakan keamanan informasi?
10. Bagaimana yang dimaksud dengan pengendalian dan jenis pengendalian?

C. Tujuan Penulisan

Adapun tujuan dari penulisan artikel ini adalah:

1. Untuk memahami tentang apa yang dimaksud keamanan informasi.
2. Untuk memahami tentang tujuan dari keamanan informasi.
3. Untuk memahami tentang ancaman dan risiko dari keamanan informasi.
4. Untuk memahami tentang pengandalian terhadap ancaman dan risiko keamanan informasi.
5. Untuk memahami tentang kebutuhan organisasi akan keamanan dan pengendalian.
6. Untuk memahami tentang manajemen keamanan informasi.
7. Untuk memahami tentang ancaman dan apa saja jenis ancaman.
8. Untuk memahami tentang risiko dan bagaimana manajemen risiko.
9. Untuk memahami tentang manajemen risiko dan kebijakan keamanan informasi.
10. Untuk memahami tentang pengendalian dan jenis pengendalian.

LITERATUR TEORI

A. KEBUTUHAN ORGANISASI AKAN KEAMANAN DAN PENGENDALIAN

Dalam dunia masa kini, banyak organisasi semakin sadar akan pentingnya menjaga seluruh sumber daya mereka, baik yang bersifat virtual maupun fisik agar aman dari ancaman baik dari dalam atau dari luar. Sistem komputer yang pertama hanya memiliki sedikit perlindungan keamanan, namun hal ini berubah pada saat perang viaetnam ketika sejumlah instalasi keamanan komputer dirusak pemrotes. Pengalaman ini menginspirasi kalangan industri untuk meletakkan penjagaan keamanan yang bertujuan untuk menghilangkan atau mengurangi kemungkinan kerusakan atau penghancuran serta menyediakan organisasi dengnan kemampuan untuk melanjutkan kegiatan operasional setelah terjadi gangguan.

Pendekatan-pendekatan yang dimulai di kalangan industri dicontoh dan diperluas. Ketika pencegahan federal ini diimplementasikan, dua isu penting harus diatasi yakni keamana versus hak-hak individu dan keamaan versus ketersediaan.

B. KEAMANAN INFORMASI

Keamanan informasi *(information security)* digunakan untuk mendeskripsikan perlindungan baik peralatan Komputer dan non komputer dan non kompter, fasilitas, data, dan informasi dari penyalahgunaan pihak-pihak yang tidak berwenang.

Saat pemerintah dan kalangan industri menyadari kebutuhan untuk mengamankan sumber daya informasi mereka, perhatian nyaris terfokus secara eksklusif pada perlindungan peranti keras dan data, maka istilah keamanan sistem (*system security*) pun digunakan. Fokus sempit ini kemudian diperluas sehingga mencakup bukan hanya peranti keras dan data, namun juga peranti lunak, fasilitas komputer, dan personel.

Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, dan meningkatkan *return of investment* (ROI) serta peluang bisnis (Chaeikar, etc., 2012).

Menurut (Whitman & Mattord, 2011) informasi merupakan salah satu aset yang penting untuk dilindungi keamanannya. Perusahaan perlu memperhatikan keamanan aset informasinya, kebocoran informasi dan kegagalan pada sistem dapat mengakibatkan kerugian baik pada sisi finansial maupunn produktifitas perusahaan.

Keamanan secara umum dapat diartikan sebagai *'quality or state of being secure-to be free from danger'*. Contoh tinjauan keamanan informasi sebagai berikut:

- *Physical Security*, strategi yang memfokuskan untuk mengamankan anggota organisasi, aset fisik, akses tanpa otorisasi dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran
- *Personal Security*, strategi yang lebih memfokuskan untuk melindungi orang-orang dalam organisasi
- *Operation Security*, strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan ancaman.
- *Communications Security*, strategi yang bertujuan untuk mengamankan media informasi dan teknologi informasi.
- *Network Security*, strategi yang memfokuskan pengamanan peralatan jaringan pada data organisasi.

Keamanan informasi adalah menjaga informasi dari ancaman yang mungkin terjadi dalam upaya menjamin kelangsungan bisnis, mengurangi tingkat risiko dan mempercepat atau memaksimalkan pengambilan keputusan investasi serta peluang bisnis. Tingkat keamanan pada informasi juga bergantung pada tingkat sensitifitas informasi dalam *database,* informasi yang tidak terlalu sensitif sistem keamanannya tidak terlalu ketat sedangkan untuk informasi yang sangat sensitif perlu pengaturan tingkat keamanan yang ketat untuk akses ke informasi tersebut.

Keamanan informasi menurut G. J. Simons adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Aspek-aspek yang harus dipenuhi dalam suatu sistem untuk menjamin keamanan informasi adalah informasi yang diberikan akurat dan lengkap (*right information*), informasi dipegang oleh orang yang berwenang (*right people*), dapat diakses dan digunakan sesuai dengan kebutuhan (*right time*), dan memberikan informasi pada format yang tepat (*right form*).

C. TUJUAN KEAMANAN INFORMASI

Keamanan informasi ditujukan untuk mencapai tiga tujuan utama yaitu:

1. Kerahasiaan

   artinya informasi dijamin hanya tersedia bagi orang yang berwenang sehingga pihak yang tidak berhak tidak bisa mengakses informasi. Contoh kerahasiaan adalah seorang administrator tidak boleh membuka atau membaca email milik pengguna. Selain itu kerahasiaan harus menjamin data-data yang harus dilindungi penggunaan dan penyebarannya baik oleh pengguna maupun administrator, seperti nama, alamat, tempat tanggal lahir, nomor kartu kredit, penyakit yang diderita, dan sebagainya.

2. Integritas

   artinya informasi dijaga agar selalu akurat, untuk menjaga informasi tersebut maka informasi hanya boleh diubah dengan izin pemilik informasi. Virus trojan merupakan contoh dari informasi yang integritasnya terganggu karena virus telah mengubah informasi tanpa izin. Integritas informasi ini dapat dijaga dengan melakukan enkripsi data atau membuat tanda tangan dijital (*digital signature*).

3. Ketersediaan

   artinya adanya jaminan ketika pihak berwenang membutuhkan informasi, maka informasi dapat diakses dan digunakan. Hambatan dalam ketersediaan ini contohnya adalah adanya *Denial of Service Attack* (DoS). DoS merupakan serangan yang ditujukan ke server, di mana banyak sekali permintaan yang dikirimkan ke server dan biasanya permintaan tersebut palsu yang menyebabkan server tidak sanggup lagi melayani permintaan karena tidak sesuai dengan kemampuan sehingga server menjadi *down* bahkan *error*.

D. MANAJEMEN KEAMANAN INFORMASI

Manajemen tidak hanya diharapkan untuk menjaga sumber daya informasi aman, namn jga diharapkan untuk menjaga persahaan tersebut agar tetap berfungsi setelah suatu bencana atau jebolnya sistem keamanan. Aktifitas untuk menjaga agar perusahaan dan sumber daya informasi tetap aman disebut Manajemen keamanan informasi.

CIO adalah orang yang tepat untuk memikul tanggung jawab atas keamanan informasi, namun kebanyakan organisasi mulai menunjuk orang tertentu yang dapat

mencurahkan perhatian penuh terhadap aktivitas ini. Direktur keamanan sistem informasi perusahaan digunakan untuk individu di dalam organisasi, biasanya anggota dari unit sistem informasi, yang bertanggung jawab atas keamanan sistem informasi perusahaan tersebut. Namun saat ini perubahan sedang dibuat untuk mencapai tingkat informasi yang lebih tinggi lagi di dalam perusahaan dengan cara menunjuk seorang Direktur *Assurance* informasi perusahaan (CIAO). Seorang CIAO harus mendapatkan serangkaian sertifikat keamanan dan memiliki pengalaman minimum 10 tahun dalam mengelola suatu fasilitas keamanan informasi.

Pada bentuknya yang paling dasar, manajemen keamanan informasi terdiri atas empat tahap yaitu:

1. Mengidentifikasi ancaman yang dapat menyerang sumber daya informasi perusahaan
2. Mengidentifikasi risiko yang dapat disebabkan oleh ancaman-ancaman tersebut
3. Menentukan kebijakan keamanan informasi
4. Mengimplementasikan pengendalian untuk mengatasi risiko-risiko tersebut

E. STRATEGI DALAM ISM

1. Manajemen Risiko (*Risk Management*)

   Istilah manajemen risiko (*risk management*) dibuat untuk menggambarkan pendekatan ini dimana tingkat keamanan sumber daya informasi perusahaan dibandingkan dengan risiko yang dihadapinya.

   Manajemen Risiko merupakan satu dari dua strategi untuk mencapai keamanan informasi. Risiko dapat dikelola dengan cara mengendalikan atau menghilangkan risiko atau mengurangi dampaknya.

   Tingkat keparahan dampak dapat diklasifikasikan menjadi:

   - Dampak yang parah (*severe impact*) yang membuat perusahaan bangkrut atau sangat membatasi kemampuan perusahaan tersebut untuk berfungsi
   - Dampak signifikan (*significant impact*) yang menyebabkan kerusakan dan biaya yang signifikan, tetapi perusahaan tersebut tetap selamat
   - Dampak minor (*minor impact*) yang menyebabkan kerusakan yang mirip dengan yang terjadi dalam operasional sehari-hari.

2. Tolok Ukur

   Tolak ukur keamanan informasi (*information security benchmark*) adalah tingkat kemanan yang disarankan yang dalam keadaan normal harus menawarkan

perlindungan yang cukup terhadap gangguan yang tidak terotorisasi. Standar atau tolak ukur semacam ini ditentukan oleh pemerintah dan asosiasi industri serta mencerminkan komponen-komponen program keamanan informais yang baik menurut otoritas tersebut.

Ketika perusahaan mengikuti pendekatan ini, yang disebut kepatuhan terhadap tolak ukur (*benchmark compliance*) dapat diasumsikan bahwa pemerintah dan otoritas industri telah melakukan pekerjaan yang baik dalam mempertimbangkan berbagai ancaman serta risiko dan tolak ukur tersebut menawarkan perlindungan yang baik.

F. ANCAMAN KEAMANAN INFORMASI

Ancaman Keamanan Informasi *(Information Security Threat)* merupakan orang, organisasi, mekanisme, atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan. Pada kenyataannya, ancaman dapat bersifat internal serta eksternal dan bersifat disengaja dan tidak disengaja.

Ancaman Internal dan Eksternal

Ancaman internal bukan hanya mencakup karyawan perusahaan, tetapi juga pekerja temporer, konsultan, kontraktor, bahkan mitra bisnis perusahaan tersebut. Ancaman internal diperkirakan menghasilkan kerusakan yang secara potensi lebih serius jika dibandingkan denga ancaman eksternal, dikarenakan pengetahuan anccaman internal yang lebih mendalam akan sistem tersebut.

Ancaman eksternal misalnya perusahaan lain yang memiliki produk yang sama dengan produk perusahaan atau disebut juga pesaing usaha.

Tindakan Kecelakaan dan disengaja

Tidak semua ancaman merupakan tindakan disengaja yang dilakukan dengan tujuan mencelakai. Beberapa merupakan kecelakaan yang disebabkan oelh orang-orang di dalam ataupun diluar perusahaan. sama halnya

Jenis- Jenis Ancaman:

Malicious software, atau *malware* terdiri atas program-program lengkap atau segmen-segmen kode yang dapat menyerang suatu system dan melakukan fungsi-fungsi yang tidak diharapkan oleh pemilik sIstem. Fungsi-fungsi tersebut dapat menghapus file, atau menyebabkan sistem tersebut berhenti. Terdapat beberapa jensi peranti lunak yang berbahaya, yakni:

1. Virus. Adalah program komputer yang dapat mereplikasi dirinya sendiri tanpa dapat diamati oleh si pengguna dan menempelkan salinan dirinya pada program-program dan *boot sector* lain
2. *Worm*. Program yang tidak dapat mereplikasikan dirinya sendiri di dalam sistem, tetapi dapat menyebarkan salinannya melalui e-mail
3. *Trojan Horse*. Program yang tidak dapat mereplikasi atau mendistribusikan dirinya sendiri, namun disebarkan sebagai perangkat
4. *Adware*. Program yang memunculkan pesan-pesan iklan yang mengganggu
5. *Spyware*. Program yang mengumpulkan data dari mesin pengguna

G. RISIKO KEAMANAN INFORMASI

Risiko Keamanan Informasi (*Information Security Risk*) didefinisikan sebagai potensi *output* yang tidak diharapkan dari pelanggaran keamanan informasi oleh Ancaman keamanan informasi. Semua risiko mewakili tindakan yang tidak terotorisasi. Risiko-risiko seperti ini dibagi menjadi empat jenis yaitu:

1. Pengungkapan Informasi yang tidak terotoritasis dan pencurian *(interception)*. Ketika suatu basis data dan perpustakaan peranti lunak tersedia bagi orang-orang yang seharusnya tidak memiliki akses, hasilnya adalah hilangnya informasi atau uang.
2. Penggunaan yang tidak terotorisasi *(fabrication)*. Penggunaan yang tidak terotorisasi terjadi ketika orang-orang yang biasanya tidak berhak menggunakan sumber daya perusahaan mampu melakukan hal tersebut.
3. Penghancuran yang tidak terotorisasi dan penolakan layanan *(interruption)*. Seseorang dapat merusak atau menghancurkan peranti keras atau peranti lunak, sehingga menyebabkan operasional komputer perusahaan tersebut tidak berfungsi.
4. Modifikasi yang terotorisasi *(modification)*. Perubahan dapat dilakukan pada data, informasi, dan peranti lunak perusahaan yang dapat berlangsung tanpa disadari dan menyebabkan para pengguna output sistem tersebut mengambil keputusan yang salah.

H. MANAJEMEN RISIKO

Manajemen Risiko merupakan satu dari dua strategi untuk mencapai keamanan informasi.Risiko dapat dikelola dengan cara mengendalikan atau menghilangkan risiko atau mengurangi dampaknya. Pendefenisian risiko terdiri atas empat langkah:

1. Identifikasi aset-aset bisnis yang harus dilindungi dari risiko

2. Menyadari risikonya
3. Menentukan tingkatan dampak pada perusahaan jika risiko benar-benar terjadi
4. Menganalisis kelemahan perusahaan tersebut

Tabel Tingkat Dampak dan Kelemahan

	Dampak Parah	Dampak Signifikan	Dampak Minor
Kelemahan Tingkat Tinggi	Melaksanakan analisis kelemahan. Harus meningkatkan pengendalian	Melaksanakan analisis kelemahan. Harus meningkatkan pengendalian	Analisis kelemahan tidak dibutuhkan
Kelemahan Tingkat Menengah	Melaksanakan analisis kelemahan. Sebaiknya meningkatkan pengendalian.	Melaksanakan analisis kelemahan. Sebaiknya meningkatkan pengendalian.	Analisis kelemahan tidak dibutuhkan
Kelemahan Tingkat Rendah	Melaksanakan analisis kelemahan. Menjaga Pengendalian tetap ketat.	Melaksanakan analisis kelemahan. Menjaga Pengendalian tetap ketat.	Analisis kelemahan tidak dibutuhkan

Tingkat keparahan dampak dapat diklasifikasikan menjadi:

- dampak yang parah *(severe impact)* yang membuat perusahaan bangkrut atau sangat membatasi kemampuan perusahaan tersebut untuk berfungsi
- dampak signifikan *(significant impact)* yang menyebabkan kerusakan dan biaya yang signifikan, tetapi perusahaan tersebut tetap selamat
- dampak minor *(minor impact)* yang menyebabkan kerusakan yang mirip dengan yang terjadi dalam operasional sehari-hari.

Setelah analisis risiko diselesaikan, hasil temuan sebaiknya didokumentasikan dalam laporan analisis risiko. Isi dari laporan ini sebaiknya mencakup informasi berikut ini, mengenai tiap-tiap risiko:

- diskripsi risiko
- sumber risiko
- tingginya tingkat risiko
- pengendalian yang diterapkan pada risiko tersebut

- para pemilik risiko tersebut
- tindakan yang direkomendasikan untuk mengatasi risiko
- jangka waktu yang direkomendasikan untuk mengatasi risiko

Jika perusahaan telah mengatasi risiko tersebut, laporan harus diselesaikan dengan cara menambahkan bagian akhir: apa yang telah dilaksanakan untuk mengatasi risiko tersebut

KEBIJAKAN KEAMANAN INFORMASI

Suatu kebijakan keamanan harus diterapkan untuk mengarahkan keseluruhan program. Perusahaan dapat menerapkan keamanan dengan pendekatan yang bertahap, diantaranya:

Fase 1, Inisiasi Proyek. Membentuk sebuah tim untuk mengawas proyek kebijakan keamanan tersebut.

Fase 2, Penyusunan Kebijakan. Berkonsultasi dengan semua pihak yang berminat dan terpengaruh.

Fase 3, Konsultasi dan persetujuan. Berkonsultasi dengan manajemen untuk mendapatkan pandangan mengenai berbagai persyaratan kebijakan.

Fase 4, Kesadaran dan edukasi. Melaksanakan program pelatihan kesadaran dan edukasi dalam unit-unit organisasi.

Fase 5, Penyebarluasan Kebijakan. Kebijakan ini disebarluaskan ke seluruh unit organisasi dimana kebijakan tersebut dapat diterapkan.

Kebijakan Keamanan yang terpisah dikembangkan untuk:

- Keamanan Sistem Informasi
- Pengendalian Akses Sistem
- Keamanan Personel
- Keamanan Lingkungan Fisik
- Keamanan Komunikasi data
- Klasifikasi Informasi
- Perencanaan Kelangsungan Usaha
- Akuntabilitas Manajemen

Kebijakan terpisah ini diberitahukan kepada karyawan, biasanya dalam bentuk tulisan, dan melalui program pelatihan dan edukasi. Setelah kebijakan ini ditetapkan, pengendalian dapat diimplementasikan.

I. MACAM-MACAM PENGENDALIAN

I. Pengendalian Teknis

1. Pengendalian Akses

Dasar untuk keamanan melawan ancaman yang dilakukan oleh orang-orang yang tidak diotorisasi adalah pengendalian akses. Alasannya sederhana: Jika orang yang tidak diotorisasi tidak diizinkan mendapatkan akses terhadap sumber daya informasi, maka pengrusakan tidak dapat dilakukan. Dilakukan melalui tiga tahap:

a. Identifikasi Pengguna. Para pengguna pertama-tama mengidentifikasi diri mereka dengan cara memberikan sesuatu yang mereka ketahui, misalnya kata sandi. Identifikasi dapat pula mencakup lokasi pengguna, seperti nomor telepon atau titik masuk jaringan.

b. Autentifikasi Pengguna. Setelah identifkasi awal telah dilakukan, para pengguna memverifikasi hak akses dengan cara memberikan sesuatu yang mereka miliki, seperti *smart card* atau tanda tertentu atau chip identifikasi. Autentifikasi pengguna dapat juga dilaksanakan dengan cara memberikan sesuatau yang menjadi identitas diri, seperti tanda tangan atau suara atau pola suara.

c. Otorisasi Pengguna. Setelah pemeriksaan identifikasi dan autentifikasi dilalui, seseorang kemudian dapat mendapatkan otorisasi untuk memasuki tingkat atau derajat penggunaan tertentu. Sebagai contoh, seorang pengguna dapat mendapatkan otorisasi hanya untuk membaca sebuah rekaman dari suatu file, sementara pengguna yang lain dapat saja memiliki otorisasi untuk melakukan perubahan pada file tersebut.

Identifkasi dan autentifikasi memanfaatkan profil pengguna (*user profile*), atau deskripsi pengguna yang terotorisasi. Otorisasi memanfaatkan file pengendalian akses (*acess control file*) yang menentukan tingkat akses yang tersedia bagi tiap pengguna. Setelah para pengguna memenuhi syarat tiga fungsi pengendalian kases, mereka dapat menggunakan sumber daya informasi yang terdapat di

dlaam batasan file pengendalian akses. Pencatatan audit yang berbasis komputer terus dilakukan pada semua aktivitas pengendalian akses, seperti tanggal dan waktu serta identifikasi terminal, dan digunakan untuk mempersiapkan laporan keuangan.

2. Sistem Deteksi Gangguan

Logika dasar dari sistem deteksi gangguan adalah mengenali upaya pelanggaran keamanan sebelum memiliki kesempatan untuk melakukan perusakan. Salah satu contoh yang baik adalah peranti lunak proteksi virus *(virus protection software)* yang telah terbukti efektif melawan virus yang terkirim melalui e-mail. Peranti lunak tersebut mengidentifikasi pesan pembawa virus dan memperingatkan si pengguna.

Contoh deteksi pengganggu yang lain adalah peranti lunak yang ditujukan untuk mengidentifikasikan calon pengganggu sebelum memiliki kesempatan untuk membahayakan. Peralatan prediksi ancaman dari dalam *(insider threat prediction tool)* telah disusun sedemikian rupa sehingga dapat mempertimbangkan karakteristik seperti posisi seseorang di dalam perusahaan, akses ke dalam data yang sensitive, kemampuan untuk mengubah komponen peranti keras, jenis aplikasi yang digunakan,file yang dimilki, dan penggunaan protocol jaringan tertentu. Hasil pembuatan profilan seperti ini, yang beberapa berbentuk kuantitatif, dapat mengklasifikasikan ancaman internal ke dalam kategori seperti ancaman yang disengaja, potensi ancaman kecelakaan, mencurigakan, dan tidak berbahaya.

3. Firewall

Sumber daya komputer selalu berada dalam resiko jika terhubung ke jaringan. Salah satu pendekatan keamanan adalah secara fisik memisahkan situs Web perusahaan dengan jaringan internal perusahaan yang berisikan data sensitive dan system informasi. Cara lain adalah menyediakan kata sandi kepada mitra dagang yang memungkinkannya memasuki jaringan internal dari Internet.

Pendekatan ketiga adalah membangun dinding pelindung atau firewall. Firewall berfungsi sebagai penyaring dan penghalang yeng membatasi aliran data dari perusahaan tersebut dan Internet. Konsep dibalik firewall adalah dibuatnya suatu pengaman untuk semua komputer pada jaringan perusahaan dan bukannya pengaman terpisah untuk masing-masing komputer. Beberapa

perusahaan yang menawarkan peranti lunak antivirus (seperti McAfee di www.mcafee.com dan www.norton.com) sekarang memberikan peranti lunak firewall tanpa biaya ekstra dengan pembelian produk antivirus mereka. Ada tiga jenis firewall, yaitu:

1. Firewall Penyaring Paket. Router adalah alat jaringan yang mengarahkan aliran lalu lintas jaringan. Jika router diposisikan antara Internet dan jaringan internal, maka router dapat berlaku sebagai firewall. Router dilengkapi dengan table data dan alamat-alamat IP yang menggambarkan kebijakan penyaringan. Untuk masing-masing transmisi, router mengakses table-tabelnya dan memungkinkan hanya beberapa jenis pesan dari beberapa lokasi Internet (alamat IP) untuk lewat. Alamat IP *(IP Address*) adalah serangkaian empat angka (masing-masing dari 0 ke 255) yang secara unik mengidentifikasi masing-masing computer yang terhubung dengan Internet. Salah satu keterbasan router adalah router hanya merupakan titik tunggal keamanan, sehingga jika hacker dapat melampuinya perusahaan tersebut bisa mendapatkan masalah. “IP spoofing”, yaitu menipu table akses router, adalah dalah satu metode yang digunakan untuk pembajak untuk menipu router.
2. Firewall Tingkat Sirkuit. Salah satu peningkatan keamanan dari router adalahfirewall tingkat sirkuit yang terpasang antara Internet dan jaringan perusahaan tapi lebih dekat dengan medium komunikasi (sirkuit) daripada router. Pendekatan ini memungkinkan tingkat autentifikasi dan penyaringan yang tinggi, jauh lebih tinggi dibandingkan router. Namun, keterbatasan dari titik tunggal keamanan tetap berlaku.
3. Firewall Tingkat Aplikasi. Firewall ini berlokasi antara router dan komputer yang menajlankan aplikasi tersebut. Kekuatan penuh pemeriksaan keamanan tambahan dapat dilakukan. Setelah permintaan diautentifikasi sebagai permintaan yang berasal dari jaringan yang diotorisasi (tingkat sirkuit) dan dari komputer yang diotorisasi (penyaringan paket), aplikasi tersebut dapat memnita informasi autentifikasi yang lebih jauh seperti menanyakan kata sandi sekunder, mengonfirmasikan identitas, atau bahkan memeriksa apakah permintaan tersebut berlangsung selama jam-jam kerja biasa. Meskipun merupakan jenis firewall yang paling efektif, firewall ini cenderung untuk mengurangi akses ke sumber daya. Masalah lain adalah

seorang programmer jaringan harus penulis kode program yang spesifik untuk masing-masing aplikasi dan mengubah kode tersebut ketika aplikasi ditambahkan, dihapus, dimodifikasi.

4. Pengendalian Kriptografis

Data dan informasi yang tersimpan dan ditransmisikan dapat dilindungi dari pengungkapan yang tidak terotorisasi dengan kriptografi, yaitu penggunaan kode yang menggunakan proses-proses matematika. Data dan informasi tersebut dapat dienkripsi dalam penyimpanan dan juga ditransmisikan kedalam jaringan. Jika seseorang yang tidak memiliki otorisasi memperoleh akses enkripsi tersebut akan membuat data dan informasi yang dimaksud tidak berarti apa-apa dan mencegah kesalahan penggunaan.

Popularitas kriptografis semakin meningkat karena e-commerce, dan produk khusus ditujukan untuk meningkatkan keamanan e-commerce telah dirancang. Salah satunya adalah SET (*Secure Electronic Transactions*), yang ,melakukan pemeriksaan keamanan menggunakan tanda tangan digital. Tanda tangan ini dikeluarkan kepada orang-orang yang dapat berpartisispasi dalam transaksi *e-commerce* – pelanggan, penjual, dan institusi keuangan. Dua tanda tangan biasanya digunakan menggantikan nomor kartu kredit.

Merupakan penggunaan kode yang menggunakan proses-proses matematika. Meningkatkan keamanan data dengan cara menyamarkan data dalam bentuk yang tidak dapat dibaca. Berfungsi untuk melindungi data dan informasi yang tersimpan dan ditransmisikan, dari pengungkapan yang tidak terotorisasi. Kriptografi terbagi menjadi:

a. Kriptografi Simetris. Dalam kriptografi ini, kunci enkripsi sama dengan kunci dekripsi.
b. Kriptografi Asimetris. Dalam kriptografi kunci enkripsi tidak sama dengan kunci dekripsi.
c. Kriptografi Hybrid. Menggabungkan antara kriptografi simetris dan asimetris, sehingga mendapatkan kelebihan dari dua metode tersebut. Contoh: SET (Secure Electronic Transactions) pada E-Commerce

5. Pengendalian Fisik

Peringatan pertama terhadap gangguan yang tidak terotorisasi adalah mengunci pintu ruangan computer. Perkembangan seterusnya menghasilkan kunci-kunci

yang lebih canggih yaitu dibuka dengan cetakan telapak tangan dan cetakan suara, serta kamera pengintai dan alat penjaga keamanan. Perusahaan dapat melaksanakan pengendalian fisik hingga pada tahap tertinggi dengan cara menempatkan pusat komputernya ditempat terpencil yang jauh dari kota dan jauh dari wilayah yang sensitive terhadap bencana alam seperti gempa bumi, banjir, dan badai.

II. Pengendalian Formal

Pengendalian formal mencakup penentuan cara berperilaku, dokumentasi prosedur dan praktik yang diharapkan, dan pengawasan serta pencegahan perilaku yang berbeda dari panduan yang berlaku. Pengendalian ini bersifat formal karena manajemen menghabiskan banyak waktu untuk menyusunnya, mendokumentasikannya dalam bentuk tulisan, dan diharapkan untuk berlaku dalam jangka panjang.

III. Pengendalian Informal

Pengendalian informal mencakup program-program pelatihan dan edukasi serta program pembangunan manajemen.Pengendalian ini ditunjukan untuk menjaga agar para karyawan perusahaan memahami serta mendukung program keamanan tersebut.

J. PENTINGNYA KEAMANAN INFORMASI

Sistem Informasi diperlukan karena:

- Teknologi komunikasi modern yang membawa beragam dinamika dari dunia nyata ke dunia virtual
- Kurangnya keterampilan pengamanan yang dimiliki oleh pemakai
- Untuk menjaga objek kepemilikan dari informasi yang memiliki nilai ekonomis.

Lalu mengapa informasi perlu dilakukan pengamanan? Karena informasi adalah salah satu aset bagi suatu perusahaan atau organisasi. Seperti aset yang lain, informasi memiliki nilai tertentu bagi perusahaan atau organisasi tersebut sehingga harus dilindungi atau diberikan keamanan untuk :

a. Menjamin kelangsungan perusahaan atau organisasi.
b. Meminimalisir kerusakan karena kebocoran sistem keamanan informasi.
c. Mempercepat kembalinya investasi.

d. Memperluas peluang usaha.

Keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan. Masalah tersebut penting karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan.

K. DUKUNGAN PEMERINTAH DAN INDUSTRI

Beberapa organisasi pemerintah dan internasional telah menentukan standar-standar yang ditunjukan untuk menjadi panduan bagi organisasi yang ingin mendapatkan keamanan informasi.Beberapa standar ini berbentuk tolak ukur, yang telah diidentifikasisebelumnya sebagai penyedia strategi alternative untuk manajemen resiko. Beberapa pihak penentu standar menggunakan istilah *baseline* (dasar) dan bukannya *benchmark* (tolak ukur). Organisasi tidak diwajibkan mengikuti standar ini.Namun, standar ini ditunjukan untuk memberikan bantuan kepada perusahaan dalam menentukan tingkat target keamanan.

L. MANAJEMEN KEBERLANGSUNGAN BISNIS

Manajemen keberlangsungan bisnis (*business continuity management*-BCM) adalah aktivitas yang ditujukan untuk menentukan operasional setelah terjadi gangguan sistem informasi. Subrencana yang umum mencakup:

1. Rencana darurat (*emergency plan*): terdiri dari cara-cara yang akan menjaga keamanan karyawan jika bencana terjadi. Co: Alarm bencana, prosedur evakuasi
2. Rencana cadangan: menyediakan fasilitas computer cadangan yang bisa dipergunakan apabila fasilitas computer yang biasa hancur atau rusak hingga tidak bisa digunakan.
3. Rencana catatan penting (*vital records plan*): merupakan dokumen kertas, microform, dan media penyimpanan optis dan magnetis yang penting untuk meneruskan bisnis perusahaan.

PEMBAHASAN

IMPLEMENTASI KEAMANAN INFORMASI PADA GITA BUSANA

Setiap organisasi memiliki beberapa bentuk informasi yang sensitif, untuk melindungi informasi yang bersifat sensitif seperti informasi pembayaran pelanggan, data karyawan atau informasi strategi bisnis maka sangat penting untuk mengambil langkah-langkah untuk mengamankan data sensitif organisasi dan memastikan bahwa informasi tersebut tidak pernah memasuki akses publik. Berikut ini adalah cara penerapan untuk mengamankan informasi sebuah organisasi seperti Gita Busana:

1. **Buat kebijakan untuk menangani informasi.**

   Sebuah sistem klasifikasi data yang bertingkat dapat membantu untuk membedakan antara informasi sensitif dan non-sensitif. Langkah-langkah keamanan diberlakukan untuk setiap tingkat data, tingkat pertama yaitu data yang sangat sensitif yang dapat menyebabkan kerusakan parah membutuhkan tingkat keamanan tertinggi dan akses diperbolehkan atas dasar kebutuhan khusus. Tingkat ke-dua yaitu data cukup sensitif yang dapat menimbulkan risiko yang relatif rendah membutuhkan kontrol keamanan yang lebih sedikit dan hak akses internal. Dan tingkat yang ke-tiga yaitu data non-sensitif yang tidak menimbulkan risiko untuk sebuah organisasi, dan membutuhkan keamanan yang sedikit atau tidak ada pembatasan akses.

2. **Pilih *software* yang aman.**

   Tentukanlah perangkat lunak yang direkomendasikan oleh ahli sistem keamanan informasi untuk standar keamanan yang digunakan. Perangkat lunak yang Anda gunakan mungkin tidak mengikuti prosedur keamanan yang handal dan dapat menyebabkan meningkatnya kemungkinan *Hacker* mengakses informasi sensitif. Hal ini menjadi masalah serius terutama ketika menangani dan menyimpan informasi pembayaran pelanggan melalui perangkat lunak akuntansi. Namun jangan khawatir, karena ada beberapa langkah dasar bagi organisasi untuk dapat memilih dan mengidentifikasi software yang aman. Hindari penggunaan layanan keamanan dan *software anti-malware* gratis: biasanya usaha kecil mengharapkan fitur keamanan dasar dalam solusi gratis yang ditawarkan sudah mencukupi. Solusi keamanan gratis memang memberikan perlindungan dasar, tetapi seringnya mereka gagal untuk memberikan dukungan keamanan yang berlapis. Sebaliknya, lihatlah solusi khusus: mereka

sesungguhnya tidak membutuhkan dana yang besar, tetapi mampu memberikan tingkat perlindungan yang lebih tinggi.

3. **Tingkatkan keamanan *password*.**

   Penggunaan password yang lemah merupakan masalah yang sangat umum dan merupakan salah satu keamanan yang secara signifikan dapat ditingkatkan dengan pelatihan dan pengenalan berbagai aplikasi manajemen *password*. Kebanyakan pencurian data sensitif disebabkan oleh segelintir kesalahan keamanan informasi dasar.

4. **Gunakan komputer pribadi**

   Penggunaan komputer atau perangkat pribadi merupakan bagian yang tak terpisahkan dari kehidupan dan pekerjaan, selain membawa manfaat bagi produktivitas dan efektivitas biaya, juga dapat mengamankan data sensitif dari akses yang tidak sah. Adalah tindakan yang tepat untuk menggunakan komputer pribadi untuk mencegah data sensitif diakses dan disimpan oleh orang lain yang tidak berhak.

5. **Menerapkan Sistem Manajemen Keamanan Informasi**

   Sistem Manajemen Keamanan Informasi atau ISO/IEC 27001:2005 merupakan sebuah metode khusus yang terstruktur tentang pengamanan informasi yang diakui secara internasional. ISO/IEC 27001:2005 merupakan dokumen sistem manajemen keamanan informasi yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan maupun organisasi dalam usaha mereka untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi dimiliki berdasarkan ”*best practise*” dalam pengamanan informasi.

6. **Membuat cadangan salinan dari semua file penting secara reguler.**

   Perusahaan harus memiliki dua backup: satu di *cloud* (misalnya *Dropbox, Google Drive,* dll), dan satu lagi di *server* tambahan atau pada *removable medium* jika volume data tidak terlalu besar.

7. **Membackup data**

   Apabila perusahaan terjadi pemadaman listrik mendadak ataupun koneksi internet yang hilang seringkali membuat tugas maupun data informasi menjadi hilang. Meskipun komputer merupakan teknologi canggih, namun hal seperti ini seringkali terjadi sehingga harus tetap sering melakukan backup secara berkala untuk mencegah hal ini terjadi. Serta diperlukan juga salinan yang diletakkan dalam flash disk maupun juga hardisk.

KESIMPULAN

Dapat disimpulkan bahwa Keamanan informasi (*information security*) digunakan untuk mendeskripsikan perlindungan baik peralatan komputer dan non komputer dan non komputer, fasilitas, data, dan informasi dari penyalahgunaan pihak-pihak yang tidak berwenang. Keamanan informasi ditujukan untuk mencapai tiga tujuan utama yaitu: kerahasiaan, ketersediaan, dan integritas.

Dalam dunia masa kini, banyak organisasi semakin sadar akan pentingnya menjaga seluruh sumber daya mereka, baik yang bersifat virtual maupun fisik agar aman dari ancaman baik dari dalam atau dari luar. Istilah keamanan sistem digunakan untuk mengambarkan perlindungna baik peralatan komputer dan nonkomputer, fasilitas,data dan informasi dari penyalahgunaan pihak-pihak yang tidak berwenang. Aktivitas untuk menjaga agar sumber daya informasi tetap aman disebut manajemen keamanan informasi (*information security management* – ISM), sedangkan aktivitas untuk menjaga agar perusahaan dan sumber daya informasinya tetap berfungsi setelah adanya bencana disebut manajemen keberlangsungan bisnis (*bussiness continuity management* – BCM). Istilah manajemen risiko (*risk management*) dibuat untuk menggambarkan pendekatan ini dimana tingkat keamanan sumber daya informasi perusahaan dibandingkan dengan risiko yang dihadapinya.

Ancaman keamanan sistem informasi adalah orang, organisasi, mekanisme, atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan. Ancaman itu terdiri dari ancaman internal dan eksternal. Resiko keamanan informasi dapat Didefinisikan sebagai potensi output yang tidak Diharapkan dari pelanggaran keamanan informasi oleh Ancaman keamanan informasi. Semua risiko mewakili tindakan yang tidak terotorisasi. Untuk mengendalikan Ancaman serta risiko keamanan informasi itu dapat dilakukan dengan berbagai pengendalian yaitu: pengendalian teknis, kriptografis, fisik, formal dan informal.

Risiko Keamanan Informasi (*Information Security Risk*) didefinisikan sebagai potensi output yang tidak diharapkan dari pelanggaran keamanan informasi oleh ancaman keamanan informasi.

DAFTAR PUSTAKA

Putra, Y. M. (2018). Keamanan Informasi. *Modul Kuliah Sistem Informasi Manajemen.* Jakarta: FEB-Universitas Mercu Buana

Purwanto, Eko (2014). Keamanan Informasi [Online] tersedia di https://bpptik.kominfo.go.id/2014/03/24/404/keamanan-informasi/ [diakses pada 27 Mei 2019]

Retnowardhani, Astari (2017). Keamanan Informasi [Online] tersedia di https://mmsi.binus.ac.id/2017/11/17/keamanan-informasi/ [diakses pada 27 Mei 2019]

Raymond Mcleod, Jr., George P. Schell (2009). Sistem Informasi Manajemen. Jakarta: Salemba Empat.

Zaidun, Achmad (2013). Keamanan Informasi [Online] tersedia di http://achmadzaidun.blogspot.com/2013/12/keamanan-informasi.html [diakses pada 27 Mei 2019]

Grace (2014). Keamanan Informasi [Online] tersedia di http://kumpulanmakalahsim.blogspot.com/2014/05/keamanan-informasi.html [diakses pada 27 Mei 2019]

Anggraini, Magy (2013). Sistem Informasi Manajemen Keamanan Informasi [Online] tersedia di http://megyanggraini.blogspot.com/2013/07/sistem-informasi-manajemen-keamanan.html [diakses pada 27 Mei 2019]