



Tugas Mata Kuliah Proteksi dan Keamanan Sistem Informasi
(IKI-838408T)

Praktek Manajemen Keamanan Komputer pada Usaha Kecil dan Menengah

Disusun Oleh:

Adri Praharja Tejoyuwono – 7204000438

Jeffry O.A. Ambarita – 7204000276

Dosen:

Rahmat M. Samik-Ibrahim

Johny Moningka

Arrianto Mukti Wibowo

Daftar Isi

Daftar Isi	i
Daftar Tabel	ii
1. Pendahuluan	1
1.1. Latar Belakang	1
1.1.1. Sistem informasi sebagai aset bagi UKM	1
1.1.2. Motivasi perlindungan sistem informasi pada UKM	2
1.2. Tujuan keamanan dan perlindungan sistem informasi	3
1.3. Konsep dasar manajemen keamanan sistem informasi	4
1.3.1. Prinsip fundamental keamanan sistem informasi pada UKM	4
1.3.2. Kebijakan keamanan sistem informasi pada UKM	5
1.3.3. Perbedaan metode kualitatif dan kuantitatif analisa resiko keamanan sistem informasi pada UKM	6
2. Kebutuhan Keamanan Sistem Informasi pada UKM	8
2.1. Klasifikasi kebutuhan keamanan sistem informasi UKM	8
2.2. Klasifikasi perlindungan informasi yang dimiliki usaha kecil dan menengah	10
2.2.1. Proses klasifikasi tingkat keamanan sistem informasi pada UKM	11
2.3. Manajemen resiko sistem informasi	13
2.3.1. Manajemen resiko keamanan komputer pada UKM	13
2.3.2. Metode menganalisa resiko keamanan sistem informasi pada UKM	16
2.3.3. Tahapan melakukan analisa resiko keamanan sistem informasi pada UKM	18
3. Model Ekonomis Keamanan Sistem Informasi pada UKM	21
3.1. Memperkirakan potensi kerugian pada keamanan sistem informasi pada UKM	21
3.2. Proses pengumpulan informasi aset keamanan sistem informasi pada UKM	21
3.3. Analisis ekonomi perancangan dan penerapan keamanan sistem informasi pada UKM	22
4. Implementasi Keamanan Sistem Informasi pada UKM	25
4.1. Tanggung Jawab keamanan sistem informasi UKM	25
4.1.1. Peran-peran pada keamanan sistem informasi UKM	25
4.1.2. Peran dan tanggung jawab implementasi kebijakan keamanan sistem informasi pada UKM	25
4.2. Kegiatan mengumpulkan status keamanan sistem informasi	27
4.2.1. Kriteria evaluasi tingkat keamanan sistem informasi pada UKM	27
4.2.2. Tindak lanjut status keamanan sistem informasi	32
4.3. Teknologi keamanan sistem informasi pada UKM	33
4.4. Implementasi kebijakan keamanan sistem informasi pada UKM	38
5. Kesimpulan dan Saran	44
5.1. Kesimpulan	44
5.1.1. Tingkat kesadaran pentingnya keamanan sistem informasi pada UKM	44
5.2. Saran	44
5.2.1. Pelatihan keamanan sistem informasi pada UKM	44
Daftar Pustaka	45

Daftar Tabel

Tabel 1.1 Perbandingan Analisa Resiko Kuantitatif dengan Kualitatif.....	7
Tabel 2.1 Skema Sederhana Klasifikasi Informasi Sektor Swasta/Komersial	11
Tabel 2.2 Rumusan-Rumusan analisis risiko.....	16
Tabel 2.3 Skala Exposure yang Sederhana	17
Tabel 4.1 Contoh Daftar Resiko yang diisi.....	29
Tabel 4.2 Contoh Daftar Resiko yang kosong	30
Tabel 4.3 Penomoroan dan Penamaan Resiko serta Deskripsinya	32

1. Pendahuluan

1.1. Latar Belakang

1.1.1. Sistem informasi sebagai aset bagi UKM

Ancaman terhadap keamanan sistem informasi memiliki dampak hilangnya data dan informasi, terganggunya komunikasi jaringan komputer misalnya dengan habisnya *bandwidth* yang terpakai oleh *worm* untuk menggandakan dirinya atau lumpuhnya sistem *e-mail*. Atas ancaman keamanan sistem informasi, dari pengalaman penulis, usaha kecil menengah atau UKM, terutama di Indonesia, memiliki sikap:

1. Tidak memperdulikan keamanan sistem informasi misalnya menghubungkan komputer dengan LAN yang memiliki akses membagi data dari *mobile disk* atau internet tanpa dilengkapi software security seperti *firewall* atau antivirus, atau
2. Memiliki keamanan minimal misalnya bersikap reaktif terhadap masalah keamanan sistem informasi yang muncul.

Sikap-sikap seperti ini justru memicu semakin maraknya masalah-masalah keamanan sistem informasi mulai dari virus hingga penyusupan sistem. Demikian tulisan ini dibuat melihat situasi kesadaran pentingnya keamanan sistem informasi. Tulisan ini ditujukan bagi manajemen keamanan sistem informasi bagi UKM di Indonesia.

Sasaran penulisan adalah UKM di Indonesia. UKM di Indonesia merupakan tulang punggung perekonomian. Secara implisit tanpa melihat data yang ada atau mesti dicari, UKM di Indonesia mampu bertahan dalam berbagai keadaan kesulitan ekonomi tanpa hutang pada pihak manapun yang dapat semakin mempersulit keadaan ekonomi. Kemampuan bertahan dalam kesulitan ekonomi juga memberikan efek sosial penting pengadaan lapangan pekerjaan.

Lingkup penulisan bagi manajemen usaha kecil menengah di Indonesia adalah karena akan ditunjukkan dalam bab-bab selanjutnya bahwa kebijakan keamanan sistem informasi yang baik adalah yang berupa kebijakan *top-down*. Tujuan penulisan adalah untuk memberikan ilustrasi praktis secara langsung bagaimana menerapkan keamanan sistem informasi bagi kelompok usaha kecil menengah di Indonesia.

Hal yang diungkapkan dalam tulisan ini adalah bagaimana kesadaran merupakan awal dari penerapannya keamanan sistem informasi bagi kelompok usaha kecil menengah.

Pertanyaan yang paling mendasar sepanjang masa bagi kehidupan manusia adalah mengapa keamanan menjadi salah satu perhatian utama? Siapapun juga yang mempelajari keamanan, dalam konteks tulisan ini adalah keamanan komputer secara umum atau keamanan sistem informasi pada khususnya, mestilah mempelajarinya dari suatu materi belajar, seperti buku, pelatihan, rekan kerja senior atau bahkan melalui kegiatan perkuliahan. Tak seorangpun secara alami lahiriah memiliki informasi tentang keamanan baik keamanan secara umum ataupun keamanan komputer dan sistem informasi secara khusus, salah seorang penulis mulai mempelajari keamanan komputer saat mulai mempelajari komputer semasa SMP pada tahun 1992-an.

Keamanan komputer dan keamanan sistem informasi merupakan bidang yang kompleks bermula dari manajemen keamanan sistem informasi dan berakhir pada algoritma matematika enkripsi data yang rumit didukung pengetahuan keamanan komputer hingga penggunaan perangkat lunak keamanan khusus. Jadi dapat saja seseorang memiliki pertanyaan-pertanyaan tentang keamanan sistem informasi dan tidak memahami beberapa hal tentang keamanan sistem informasi. Pertanyaan mendasar perlunya keamanan bagi sistem informasi usaha kecil dan menengah dicoba dijawab dengan mempelajari manfaat sistem informasi bagi usaha kecil dan menengah.

Sistem informasi yang diterapkan kegiatan usaha kecil dan menengah layak dilindungi. Sistem informasi yang dikembangkan usaha kecil dan menengah merupakan model bagi bisnis usaha kecil dan menengah. Banyak proses bisnis dibantu bahkan dijalankan dengan teknologi informasi yang dimiliki misalnya penghitungan gaji karyawan atau pengelolaan tagihan (*account receivable*) usaha kecil dan menengah tersebut.

1.1.2. Motivasi perlindungan sistem informasi pada UKM

Manajer pada kegiatan usaha kecil dan menengah dapat memutuskan prioritas manajemen atau manfaat keamanan sistem informasi dengan mempertanyakan beberapa pertanyaan berikut:

- Untuk apa anda menggunakan komputer atau sistem informasi? Apakah untuk kegiatan pembelian secara *online*? *Electronic banking*? *Electronic trading*? *E-mail* perusahaan? Apakah anda tahu bagaimana tingkat kematangan keamanan layanan-layanan ini? Apa artinya bagi manajer usaha kecil dan menengah bila akses menggunakan fungsi-fungsi ini diambil alih oleh pihak-pihak yang tidak berwenang? Harus tetap diingat bahwa terdapat faktor-faktor bukan finansial yang dimiliki tiap gangguan atau masalah keamanan sistem informasi. Penyalahgunaan identitas dimanfaatkan oleh *hacker* untuk merusak reputasi pengguna sesungguhnya.
- Kemana sajakah komputer anda terhubungkan? Banyak orang menghubungkan komputer mereka ke internet, selain beberapa orang yang menghubungkan komputer dengan jaringan pribadi seperti akses jarak jauh korporat yang dimiliki perusahaan tempat bekerja.
- Bagaimana komputer-komputer pada usaha kecil dan menengah terhubung dengan jaringan? Apa komputer tersambung terus menerus pada jaringan atau anda mengendalikan koneksi (dan pemutusan koneksi) komputer anda ke jaringan? Hubungan komputer melalui modem analog telah menjadi satu-satu metode yang tersedia bagi banyak pengguna layanan internet, namun teknologi yang lebih baru seperti DSL dan modem kabel memberikan kemudahan bagi banyak pengguna layanan internet untuk terhubungkan melalui jaringan dengan kecepatan akses lebih tinggi. Penggunaan teknologi-teknologi baru ini memberikan pertimbangan keamanan tertentu.
- Siapa saja yang memiliki akses fisik terhadap komputer pada usaha kecil dan menengah? Apakah manajer memberikan kewenangan bagi orang-orang yang memiliki akses fisik terhadap komputer pada usaha kecil dan menengah untuk menggunakan komputer pada usaha kecil dan menengah tersebut? Apakah manajer ingin mengendalikan akses yang dimiliki orang-orang ini terhadap komputer pada usaha kecil dan menengah atau layanan-layanan pada jaringan lokal yang dimanfaatkan usaha kecil menengah?

- Siapa yang dipercayai? karyawan dan manajer usaha kecil dan menengah? dalam komunikasi data komputer atau saling menukarkan informasi? Apakah karyawan dan manajer membuka *attachment* pada sebuah *e-mail* dari teman? Atau dari seseorang yang tidak dikenal? Bagaimana karyawan dan manajer memilih situs *web* yang aman untuk berbelanja secara *online*?

Bila manajer usaha kecil dan menengah menjawab pertanyaan-pertanyaan ini, maka hal tersebut merupakan upaya awal untuk mengamankan sistem informasi yang dimanfaatkannya. Upaya-upaya untuk memahami bagaimana usaha kecil dan menengah memanfaatkan komputer dan sistem informasi menjadikan manajer mampu melakukan pembobotan resiko yang akan dibuka terhadap kenyamanan penggunaan komputer dan sistem informasi yang dibutuhkan usaha kecil dan menengah. Tulisan ini bertujuan membantu manajer usaha kecil dan menengah untuk menjawab pertanyaan-pertanyaan di atas sehingga mampu memilih resiko yang sesuai antara keamanan dan penggunaan komputer dan sistem informasi bagi usaha kecil dan menengah.

Saat usaha kecil dan menengah mendapatkan komputer-komputer, baik dari pembelian atau menyewa, yang umumnya diatur pada konfigurasi umum. *Vendor* melakukan pengaturan umum dengan instalasi sistem operasi dan memilih semua pengaturan umum yang ditawarkan sistem operasi pada saat instalasi. *Vendor* umumnya lebih memusatkan pada kegiatan penjualan komputer dibandingkan layanan keamanan komputer. *Vendor* mengasumsikan, sebagai model penjualan produknya, tentang hal-hal umum yang pengguna komputer lakukan dan perlukan dari keamanan (*security*) dan penggunaan (*usability*).

Untuk memenuhi kebutuhan keamanan usaha kecil dan menengah, administrator harus mengatur ulang keamanan sistem operasi menjadi lebih ketat (lebih aman) atau lebih longgar (kurang aman). Administrator komputer usaha kecil dan menengah juga mungkin akan menginstal perangkat lunak tambahan untuk menambah fungsionalitas dan keamanan sistem operasi yang dipergunakan. *Vendor* komputer menyerahkan semua masalah keamanan pada pengguna. *Vendor* melakukan hal tersebut karena mengasumsikan pengguna lebih memilih penggunaan (*usability*) ketimbang keamanan (*security*). Umumnya pengguna tidak memahami masalah keamanan komputer atau merasa sebagai target ancaman keamanan komputer. Tujuan penulisan ini juga menunjukkan pada manajer usaha kecil dan menengah pentingnya keamanan komputer dan sistem informasi dan selanjutnya membantu memperoleh informasi yang diperlukan untuk mencapai keamanan tersebut.

1.2. Tujuan keamanan dan perlindungan sistem informasi

Tujuan keamanan komputer dan perlindungan sistem informasi pada usaha kecil dan menengah adalah:

- Memberikan tingkat kesadaran dan pengetahuan keamanan kepada usaha kecil dan menengah pentingnya keamanan komputer dan sistem informasi.
- Memberikan metode praktis upaya memperoleh keamanan komputer dan sistem informasi bagi usaha kecil dan menengah, termasuk pertimbangan ekonomi upaya keamanan komputer.
- Membimbing pelaksanaan upaya memperoleh keamanan komputer dan sistem informasi pada usaha kecil dan menengah.

- Memberikan cara praktis untuk mengevaluasi sistem keamanan komputer usaha kecil dan menengah.

1.3. Konsep dasar manajemen keamanan sistem informasi

Keamanan sistem informasi merupakan upaya manajemen. Manajemen keamanan sistem informasi dapat diterapkan dengan baik bila manajer usaha kecil dan menengah mengetahui beberapa hal dasar keamanan sistem informasi usaha kecil dan menengah, kebijakan keamanan yang perlu dikembangkan dan perbedaan metode yang terutama digunakan untuk menganalisa resiko keamanan sistem informasi yang dibahas dalam tulisan ini.

1.3.1. Prinsip fundamental keamanan sistem informasi pada UKM

Pada bagian ini akan dibahas prinsip perlindungan keamanan komputer. Pertanyaan utama menyangkut perlindungan sistem keamanan adalah apa yang harus dilindungi. Hal pertama dan yang paling jelas adalah data finansial bagi usaha kecil dan menengah. Hampir setiap orang memikirkan hal ini pertama-tama. Data finansial merupakan data yang harus dilindungi dan memiliki analogi yang langsung pada dunia nyata. Dimana dalam dunia nyata, orang melindungi uang sebagai upaya penting – walaupun bukan yang utama – dalam kehidupannya.

Manajer usaha kecil dan menengah seharusnya juga melindungi data milik usaha kecil dan menengah itu sendiri. Informasi, sebagai hasil pengolahan data, merupakan perangkat baru yang amat ampuh dewasa ini dan mungkin anda belum menyadari berapa orang yang ingin mendapatkan, mengubah dan menghancurkan data yang dimiliki usaha kecil dan menengah. Data milik usaha kecil dan menengah bagaikan harta bagi beberapa orang, seperti teka-teki yang harus dipecahkan dan hadiah untuk memperoleh informasi usaha kecil dan menengah adalah dapat membaca informasi pribadi usaha kecil dan menengah. Mungkin hal tersebut terasa membosankan atau tak bermakna. Untuk meyakinkan anda, terdapat banyak orang di dunia ini yang melakukan pembobolan informasi secara teratur. Godaan untuk melakukan hal ini adalah, para pembobol informasi tersebut menerobos sistem dan kadang kala mereka mendapat sesuatu yang berharga, misalnya mungkin berupa dokumen yang anda bawa ke rumah atau pesan *e-mail* pribadi.

Hal lain yang pengguna komputer perlu lindungi adalah sebuah konsep dalam dunia internet, yakni melindungi identitas pengguna komputer. Secara *online*, kebanyakan sistem tidak memiliki cara mudah untuk “membuktikan” siapa identitas pengguna komputer sesungguhnya. Orang yang pintar dapat memperoleh beberapa potongan informasi dan berpura-pura bertindak sebagai seorang pengguna komputer yang diambil identitasnya. Orang-orang tersebut menyampaikan pesan pada *online bulletin board* sebagai pengguna komputer yang diambil identitasnya atau menggunakan identitas pengguna komputer yang diambil identitasnya untuk melakukan transaksi pembelian atau membuat kartu kredit palsu atas nama seorang pengguna komputer. Kasus-kasus pencurian identitas seorang pengguna komputer menjadi kasus yang umum di internet, karena kebanyakan pengguna komputer tidak berhati-hati dengan informasi pribadi jenis ini.

Yang berhubungan dengan identitas adalah privasi. Pengguna komputer harus melindungi privatisasi *online*-nya. Semakin banyak informasi tentang seorang pengguna komputer yang terdapat di internet, semakin banyak cara yang dapat dipergunakan orang untuk menggunakan informasi tersebut. Penulis merasa hal ini sedikit paranoid, tetapi pikirkanlah tentang perusahaan pemasaran yang menjaring

informasi alamat *e-mail* di internet sehingga dapat mengirim *junk e-mail* atau mendapatkan nomer telpon untuk dimasukkan ke daftar telemarketing. Perusahaan pemasaran tersebut tidak mencuri identitas pengguna komputer, tapi mereka akan menggunakan informasi identitas pengguna komputer untuk mencoba menghubungi pengguna komputer tersebut. Mungkin beberapa orang tidak peduli. Namun secara pribadi kedua penulis tidak menyukainya, sehingga penulis melindungi privasinya di dunia internet.

Hal terakhir yang mudah dimanfaatkan dalam perhatian tentang uang dan hal yang sejenisnya adalah melindungi komputer yang dimanfaatkan usaha kecil dan menengah. Tidak semua orang yang meng-*crack* sistem melakukannya untuk memperoleh data pada sistem tersebut. Beberapa orang ingin meng-*crack* sistem yang dimanfaatkan usaha kecil dan menengah untuk memanfaatkan akses sistem usaha kecil dan menengah untuk tindakan jahat berikutnya. Situs-situs milik perusahaan besar seperti Yahoo!, eBay dan beberapa perusahaan besar lainnya mengalami serangan *Denial of Service* (DoS). Serangan ini terjadi karena cracker memasang perangkat lunak di sejumlah komputer dan membuat komputer-komputer tersebut melakukan serangan ke perusahaan yang menjadi sasaran. Beberapa dari komputer tersebut adalah komputer pengguna di rumah.

1.3.2. Kebijakan keamanan sistem informasi pada UKM

Sebuah pertanyaan yang seringkali diajukan dalam keamanan komputer dan sistem informasi dapat diringkas menjadi: apakah berharga untuk melakukan semua kesulitan dalam upaya-upaya perlindungan komputer dan sistem informasi? Pertanyaan ini adalah merupakan pertanyaan mengandung makna ganda. Untuk menjawab secara tepat, manajer usaha kecil dan menengah perlu mengetahui sistem informasi apa yang manajer usaha kecil dan menengah lindungi, bagaimana manajer usaha kecil dan menengah perlu melindungi sistem informasinya dan seberapa usaha dan biaya diperlukan dalam melindungi sistem informasi. Tulisan ini akan membahas secara rinci beberapa hal dalam pertanyaan-pertanyaan tersebut, namun yang menjadi pusat perhatian dalam bagian ini adalah manfaat keamanan komputer dan sistem informasi terhadap biaya mengimplementasikan keamanan komputer dan sistem informasi bagi usaha kecil dan menengah tersebut.

Pertama, sadarilah bahwa nilai adalah sesuatu yang subjektif. Apa yang penting bagi seseorang mungkin tidak berharga bagi orang lainnya. Faktor biaya juga bersifat subjektif atau relatif pentingnya bagi orang yang berbeda. Pengguna komputer pada usaha kecil dan menengah mungkin tidak mampu membeli implementasi penuh solusi *firewall*, tetapi untungnya, kebanyakan pengguna komputer pada usaha kecil dan menengah tidak perlu perlindungan yang demikian canggih. Penulis hanya dapat memberikan bimbingan dan saran dalam buku ini. Manajer usaha kecil dan menengah harus memahami sendiri perbandingan biaya dan manfaat pada tiap hal dalam perlindungan komputer dan sistem informasi dan membuat keputusan tepat yang sesuai.

Hal kedua, pastikan bahwa manajer usaha kecil dan menengah melibatkan pemahaman resiko (*risk assessment*) saat menjawab pertanyaan ini. Beberapa data mungkin sangat kritis sifatnya dan jelas amat berharga dilindungi. Tetapi jika data tersebut memiliki resiko yang kecil, membelanjakan biaya yang besar untuk menambah sedikit keamanan menjadi tidak masuk akal dan tidak dapat diterima. Hal ini menjadi masalah nyata tingkat keamanan dan apa yang cocok bagi manajer usaha kecil dan menengah.

Hal melindungi data sesuai dengan pemahaman resiko (*risk assessment*) memberikan konsep resiko yang dapat diterima. Secara sederhananya, konsep resiko yang dapat diterima ini membagi resiko menjadi tingkatan resiko yang membuat manajer usaha kecil dan menengah relatif merasa nyaman terhadap data atau sistem informasi yang manajer usaha kecil dan menengah coba lindungi. Tingkatan tersebut berbeda untuk tiap penerapan bahkan berbeda untuk tiap *directory* dalam *hard disk* di komputer-komputer usaha kecil dan menengah. Tingkatan resiko tidak bersifat tetap dan dapat berubah sepanjang waktu. Hal ini rasanya sulit untuk dilakukan, tetapi kenyataannya tidak sulit dilakukan. Tiap orang melakukan pengambilan keputusan serupa setiap hari saat menyebrangi jalan atau mengendarai mobil, dan manajer usaha kecil dan menengah dapat menggunakan logika yang serupa saat membagi tingkatan resiko untuk menerapkan konsep resiko yang dapat diterima. Cukup tanyakan pertanyaan “apakah pengaruh data ini bila rusak atau hilang? Jika memiliki dampak serius, apa yang saya lakukan untuk mencegah atau melakukan mitigasi kerusakan atau kehilangan data?” Jika manajer usaha kecil dan menengah merasa nyaman dengan pikiran bahwa data dapat hilang, manajer tersebut mungkin merasa nyaman dengan tingkat keamanan yang manajer usaha kecil dan menengah tersebut miliki untuk data itu. Tetapi jika manajer usaha kecil dan menengah berpikir memperoleh kembali suatu data atau menyusun data tersebut adalah suatu upaya keras, maka manajer usaha kecil dan menengah berada di daerah persimpangan dimana administrasi komputer dan sistem informasi usaha kecil dan menengah harus mempertimbangkan upaya memperketat keamanan komputer dan sistem informasi. Jika manajer usaha kecil dan menengah berpikir suatu data yang sedang dikerjakan oleh salah satu karyawan atau manajer usaha kecil dan menengah tidak dapat tergantikan dan manajer tidak akan pernah dapat memperoleh kembali data tersebut saat terjadi kehilangan data, manajer usaha kecil dan menengah harus mempertimbangkan mengamankan data tersebut dan meyakinkan bahwa administrasi komputer atau sistem informasi usaha kecil dan menengah dapat melindungi atau memperoleh data tersebut bila data tersebut hilang. Tingkatan ini serupa dengan tingkat data “data lain”, “penting” dan “kritis” yang penulis bahas sebelumnya. Tingkat “dapat digantikan” sering kali tidak digunakan untuk data yang telah karyawan atau manajer usaha kecil dan menengah ciptakan terkecuali administrasi komputer atau sistem informasi secara teratur membuat cadangan data atau sistem secara menyeluruh. Setiap data yang diciptakan karyawan dan manajer usaha kecil dan menengah secara teoritis dapat digantikan karena karyawan dan manajer usaha kecil dan menengah menciptakan data tersebut untuk mulai bekerja dengan data tersebut, namun harus ditentukan saat menggantikan data menjadi tidak praktis dilakukan.

1.3.3. Perbedaan metode kualitatif dan kuantitatif analisa resiko keamanan sistem informasi pada UKM

Terdapat beberapa unsur dari suatu proses yang menentukan nilai dari suatu asset. Prosedur-prosedur analisis resiko, baik kuantitatif maupun kualitatif (dan Penilaian Dampak Bisnis) memerlukan suatu penilaian yang dibuat berdasarkan aset-aset berharga bagi usaha kecil dan menengah. Penilaian ini adalah satu langkah pokok pada setiap metodologi audit keamanan. Suatu kekeliruan umum yang universal yang

sering dilakukan oleh usaha kecil dan menengah adalah tidak mengidentifikasi nilai dari informasi secara teliti sebelum menerapkan pengendalian keamanan. Situasi ini sering mengakibatkan adanya kendali atau kontrol yang kurang cocok untuk perlindungan aset, tidak efektif secara ekonomis, atau melindungi aset yang tidak tepat. Tabel berikut menjelaskan perbandingan antara Analisis Resiko kuantitatif dan kualitatif.

Tabel 1.1 Perbandingan Analisa Resiko Kuantitatif dengan Kualitatif

Properti	Kuantitatif	Kualitatif
Analisa biaya/manfaat	Ya	Tidak
Biaya finansial	Ya	Tidak
Dapat diotomasi	Ya	Tidak
Melibatkan penebakan	Rendah	Tinggi
Melibatkan perhitungan kompleks	Ya	Tidak
Jumlah dari informasi yang dibutuhkan	Tinggi	Rendah
Waktu / Pekerjaan yang dilibatkan	Tinggi	Rendah
Kemudahan berkomunikasi	Tinggi	Rendah

2. Kebutuhan Keamanan Sistem Informasi pada UKM

2.1. Klasifikasi kebutuhan keamanan sistem informasi UKM

Proses pengklasifikasian informasi berhubungan dengan domain *Business Continuity Planning* dan *Disaster Recovery Planning*. Keduanya memiliki fokus terhadap resiko bisnis dan penilaian data, walaupun demikian proses pengklasifikasian informasi merupakan suatu konsep dasar yang harus dimengerti untuk manajemen keamanan komputer dan sistem informasi usaha kecil dan menengah.

Terdapat beberapa alasan untuk mengklasifikasikan informasi. Untuk keperluan manajemen keamanan komputer dan sistem informasi usaha kecil dan menengah, alasan-alasan tersebut antara lain adalah tidak semua data mempunyai nilai yang sama kepada suatu usaha kecil dan menengah. Beberapa data memiliki nilai lebih bagi manajemen usaha kecil dan menengah untuk membuat keputusan-keputusan strategis, sebab data tersebut membantu manajer usaha kecil dan menengah dalam membuat keputusan strategis jangka panjang maupun jangka pendek. Beberapa data, seperti rahasia perniagaan, rumusan-rumusan, dan informasi mengenai produk baru, menjadi sangat berharga, sehingga jika data tersebut hilang, akan mendatangkan kerugian besar dengan memanfaatkan data tersebut untuk mensabotase bagi usaha kecil dan menengah yang bersangkutan. Selain itu, jika data hilang dan berpindah tangan ke pihak yang tidak bertanggung jawab, usaha kecil dan menengah yang memiliki data tersebut dapat dipermalukan dan kehilangan kepercayaan dari masyarakat.

Alasan-alasan tersebut menunjukkan beberapa kegunaan dan keuntungan yang didapatkan dari pengklasifikasian informasi untuk tujuan keamanan komputer usaha kecil dan menengah. Informasi dapat memberi suatu dampak terhadap bisnis secara keseluruhan, tidak hanya pada unit bisnis atau pada level operasional. Tujuan utama dari pengklasifikasian informasi adalah untuk meningkatkan kerahasiaan, integritas, dan ketersediaan, juga untuk memperkecil resiko-resiko terhadap informasi. Sebagai tambahan, dengan memberi focus terhadap mekanisme perlindungan dan mekanisme kontrol pada area-area informasi yang paling memerlukan, akan dicapai suatu perbandingan *cost-to-benefit* yang lebih efisien.

Pengklasifikasian informasi seringkali digunakan pada sektor pemerintahan, terutama pemerintah Amerika Serikat. Manfaatnya sudah lama disadari, dan pengklasifikasian informasi adalah merupakan komponen penting yang dibutuhkan ketika mengamankan suatu system yang terpercaya. Pada sektor ini, pengklasifikasian informasi lebih banyak digunakan untuk mencegah pengakesan dokumen-dokumen rahasia secara tidak sah.

Pengklasifikasian informasi juga dapat digunakan untuk mematuhi hukum, khususnya *privacy*, dimana diperlukan perlindungan atas informasi-informasi pribadi. Usaha kecil dan menengah dapat menerapkan pengklasifikasian informasi untuk mendapatkan keunggulan kompetitif, dan juga untuk melindungi informasi bisnis yang berharga.

Selain upaya mengklasifikasikan informasi untuk melindungi keamanan komputer usaha kecil dan menengah, perlu juga mengetahui pihak-pihak yang dapat merugikan keamanan komputer usaha kecil dan menengah. Sekarang untuk menjawab

pertanyaan dari siapa anda melindungi data. Jawabannya relatif gampang: setiap orang bahkan pengguna komputer itu sendiri. Jika pengguna komputer dapat membuat kesalahan, pengguna dapat secara tidak diinginkan mengubah data atau pengguna komputer dapat menyebabkan masalah sistem yang menghapus atau merusak data. Pekerja lainnya di kantor atau binatang dapat melakukan hal serupa. Mungkin satu penyebab terbesar kehilangan data dari sistem komputer adalah kesalahan manusia. Kebanyakan pengguna komputer pada akhirnya membuat kesalahan yang dapat secara mahal bahkan fatal jika mereka bekerja dengan data yang sensitif dalam waktu yang lama. Dengan pemulihan data yang baik, pengguna komputer cukup menggandakan ulang untuk memperbaiki kerusakan data dan melanjutkan pekerjaan. Tanpa adanya rencana pemulihan data, pekerjaan, dalam usaha kecil dan menengah khususnya, dapat tertunda bahkan tidak dilakukan sama sekali dalam waktu yang sangat singkat. Inilah mungkin rahasia terbesar keamanan data komputer yang usaha kecil dan menengah dapatkan dari tulisan ini: usaha kecil dan menengah biasanya melindungi data komputer dari kesalahan pengguna komputer itu sendiri atau kesalahan yang ceroboh. Jenis pengguna komputer yang mengincar keamanan komputer secara aktif mungkin dapat digolongkan ke dalam kategori berikut:

- *Cracker*: melakukan akses sistem komputer tanpa izin pengguna yang berwenang. Biasanya mereka diketahui menerobos penggunaan sistem dan melakukannya untuk mengambil alih hak atau kemungkinan memiliki niat jahat.
- *Hacker*: Melakukan eskplorasi sistem komputer untuk tujuan keingintahuan semata, biasanya tanpa niat merusak sesuatu.
- *Script kiddies*: memiliki keterampilan *hacking* komputer yang rendah tetapi menggunakan perangkat lunak bantuan yang dibuat oleh programer berbakat untuk menerobos sistem komputer.
- *Collectors*: Orang atau perangkat lunak yang mengakses komputer pengguna lainnya dalam upaya mengumpulkan informasi tertentu.
- *Spammer*: Orang atau program komputer yang mencoba mengirim atau menyebarkan pesan *e-mail* yang tak diinginkan melalui atau ke sistem anda.

Ancaman *cracker* nyata. Pembahasan mengenai ancaman *cracker* amat menyenangkan dan indah dan meskipun peluang serangan kecil, seseorang yang berada di rimba internet di sana dapat menjadi ancaman serius bagi pengguna komputer. Persiapan menghadapi tergantung dari kewaspadaan anda. Jadi siapakah *cracker* ini? Apa penyebab seseorang menginginkan data anda? Pertanyaan-pertanyaan tersebut sulit dijawab. *Cracker* umumnya adalah orang pintar yang bekerja di industri komputer, walau tidak terdapat profil unik yang menjelaskan *cracker* tersebut. *Cracker* dapat memiliki deskripsi fisik dan sosial yang luas jangkauannya. Banyak persepsi yang muncul bahwa *cracker* adalah orang muda jenius yang mengambil data untuk kesenangan dan mengacaukan situasi. Meskipun banyak tipe demikian di luar sana, orang muda yang demikian tidak lazim ditemukan. Lebih sering lagi, dibicarakan mengenai orang berkemampuan biasa yang memiliki beberapa keahlian komputer, yang mungkin memiliki motivasi tidak jauh dari sekedar iseng tanpa merusak.

2.2. Klasifikasi perlindungan informasi yang dimiliki usaha kecil dan menengah

Sebagai tambahan terhadap alasan-alasan pengklasifikasian informasi yang telah dibahas sebelumnya, pengklasifikasian informasi memberi beberapa manfaat-manfaat terhadap usaha kecil dan menengah. Sebagian dari manfaat-manfaat tersebut adalah sebagai berikut:

- Menunjukkan komitmen dari suatu usaha kecil dan menengah terhadap perlindungan keamanan komputer dalam upaya mewujudkan baik *good corporat governance* maupun *good IT governance*.
- Membantu mengidentifikasi informasi mana yang dianggap paling sensitive atau penting terhadap suatu usaha kecil dan menengah.
- Mendukung prinsip-prinsip kerahasiaan, integritas, dan ketersediaan, karena dapat melindungi data.
- Membantu mengidentifikasi perlindungan-perlindungan mana yang berlaku bagi informasi.
- Dapat dibutuhkan untuk mematuhi peraturan dan hukum yang berlaku.

Konsep-konsep pengklasifikasian informasi

Informasi yang dihasilkan atau diproses oleh suatu usaha kecil dan menengah harus diklasifikasikan sesuai dengan kepekaan usaha kecil dan menengah terhadap kehilangan data atau akses ilegal terhadap data. Pemilik-pemilik data ini bertanggung jawab untuk mendefinisikan level kepekaan dari data. Pendekatan ini memberdayakan kendali-kendali keamanan untuk dapat menerapkannya sesuai dengan skema klasifikasi.

Terminologi pengklasifikasian

Definisi-definisi berikut menguraikan beberapa level pengklasifikasian data pada bidang pemerintahan, yang dikelompokkan dari level terendah hingga level tertinggi.

1. Tidak diklasifikasi. Informasi dianggap tidak sensitif, sehingga tidak perlu dirahasiakan. Informasi tidak bersifat rahasia, sehingga penyebarannya tidak perlu dibatasi.
2. Sensitif tapi tidak dirahasiakan. Informasi dianggap sebagai rahasia kecil, tetapi tidak akan memberi dampak kerusakan jika disebarluaskan. Contohnya, jawaban dari ujian adalah dan informasi mengenai pelayanan kesehatan.
3. Konfidensial. Informasi dianggap memiliki sifat konfidensial. Penyingkapan tidak syah dari informasi ini dapat mengakibatkan beberapa kerusakan terhadap tingkat keamanan suatu negara.
4. Rahasia. Informasi menunjuk dari sifat rahasia. Penyingkapan tidak syah dari informasi ini bisa berakibat pada kerusakan serius terhadap tingkat keamanan nasional suatu negara.
5. Paling Rahasia (*Top Secret*). Ini merupakan level yang tertinggi dari pengklasifikasian informasi. Penyingkapan tidak syah dari informasi *Top Secret* dapat menyebabkan kerusakan fatal terhadap tingkat keamanan negara.

Pada setiap kategori tersebut, selain mendapatkan hak yang sesuai untuk mengakses informasi, seseorang atau suatu proses harus memiliki informasi “yang perlu diketahui”. Dengan begitu, perorangan yang memiliki akses terhadap informasi Rahasia atau dibawahnya, tidak dapat mengakses materi Rahasia yang tidak diperlukannya dalam menjalankan tugas-tugasnya.

Tabel 2.1 Skema Sederhana Klasifikasi Informasi Sektor Swasta/Komersial

DEFINISI	KETERANGAN
Bersifat Publik	Informasi yang aman untuk dipublikasikan
Bersifat Internal	Informasi yang aman untuk disebarakan secara internal saja tapi tidak secara eksternal
Rahasia Perusahaan	Informasi yang paling sensitif untuk perlu diketahui

Sebagai tambahan, berikut adalah terminologi klasifikasi juga dapat digunakan pada sektor swasta (lihat Tabel 2.1):

1. Publik. Informasi ini adalah yang serupa dengan informasi yang tak bersifat rahasia; setiap informasi pada suatu perusahaan yang tidak sesuai dengan kategori-kategori berikut (2, 3, 4) masuk ke dalam kategori publik. Informasi pada kategori ini tidak perlu untuk disebarluaskan, namun jika harus disingkapkan seharusnya tidak memberi dampak serius atau negatif terhadap perusahaan.
2. Sensitif. Informasi pada level sensitif memerlukan satu tingkat perlindungan yang lebih tinggi dari data biasa. Informasi ini perlu dilindungi dari hilangnya kerahasiaan, dan juga dari hilangnya integritas yang dikerenakan oleh perubahan yang tidak syah.
3. Privat. Informasi dalam kategori ini memiliki sifat privat, yang ditujukan untuk digunakan hanya untuk kepentingan usaha kecil dan menengah. Penyingkapan informasi tersebut dapat berpengaruh buruk terhadap usaha kecil dan menengah maupun karyawan usaha kecil dan menengah. Sebagai contoh, tingkatan gaji dan informasi medis pasien.
4. Konfidensial. Informasi dalam kategori konfidensial dianggap sangat sensitif dan ditujukan untuk digunakan untuk kepentingan internal usaha kecil dan menengah. Penyingkapan yang tidak syah dapat berdampak serius dan negative terhadap usaha kecil dan menengah. Sebagai contoh, informasi tentang pengembangan produ baru, rahasia perniagaan, dan negosiasi-negosiasi penggabungan dianggap konfidensial.

2.2.1. Proses klasifikasi tingkat keamanan sistem informasi pada UKM

Terdapat beberapa ukuran untuk menentukan pengklasifikasian dari suatu obyek informasi yang akan dibahas pada tulisan ini:

- Nilai. Nilai adalah kriteria yang paling sering digunakan untuk mengklasifikasikan data. Jika informasi dianggap berharga oleh suatu usaha kecil dan menengah atau pesaingnya, perlu dirahasiakan.
- Usia. Pengklasifikasian informasi dapat diturunkan jika nilai dari informasi menurun dari waktu ke waktu. Di dalam Departemen Pertahanan Amerika Serikat, dokumen-dokumen rahasia masuk ke dalam kategori tidak rahasia secara otomatis setelah batas waktu tertentu.
- Masa Penggunaan. Jika informasi telah usang karena adanya informasi baru, perubahan-perubahan substansiil di dalam perusahaan, atau pertimbangan lain, informasi dapat berubah status menjadi tidak rahasia.
- Asosiasi Pribadi. Jika informasi secara pribadi dihubungkan dengan individu spesifik atau ditujukan oleh satu hukum *privacy*, informasi tersebut perlu dirahasiakan. Sebagai contoh, informasi investigasi yang mengungkapkan nama-nama pelaku asli mungkin harus tetap dirahasiakan.

Prosedur Pengklasifikasian Informasi

Terdapat beberapa langkah ketika menetapkan suatu sistem pengklasifikasian. Langkah-langkah prosedural menurut urutan prioritas adalah sebagai berikut:

1. Mengidentifikasi administrator/penanggung jawab.
2. Menetapkan beberapa kriteria untuk mengklasifikasikan dan memberi label pada informasi.
3. Klasifikasikan data menurut pemiliknya, siapa yang perlu ditinjau kembali oleh penyelia
4. Menetapkan dan mendokumentasikan perkecualian-perkecualian peraturan pengklasifikasian.
5. Menetapkan kendali-kendali yang akan diberlakukan terhadap tiap level klasifikasi.
6. Menetapkan prosedur penghentian untuk menyatakan bahwa informasi tidak lagi bersifat rahasia atau untuk memindahkan pertanggung jawaban informasi kepada penanggung jawab lain.
7. Membuat pendekatan terhadap anggota usaha kecil dan menengah agar mereka sadar akan penggunaan pengklasifikasian.

Distribusi Informasi yang dirahasiakan

Distribusi eksternal dari informasi yang dirahasiakan sering kali diperlukan, dan ancaman-ancaman terhadap perlindungan informasi tersebut perlu dipertimbangkan. Penyebaran informasi ini dapat dilakukan pada saat terjadi beberapa hal seperti berikut:

- Perintah dari Pengadilan. Informasi yang dirahasiakan mungkin perlu untuk disingkapkan untuk mematuhi perintah dari pengadilan.

- Kontrak Pemerintah. Kontraktor pemerintah mungkin harus menyingkapkan informasi rahasianya.
- Persetujuan dari level senior. Seorang pada tingkat eksekutif senior mungkin memberi hak akses terhadap informasi rahasia kepada pihak eksternal yang berhubungan dengannya. Pemberian hak akses tersebut mungkin memerlukan persetujuan kerahasiaan oleh pihak eksternal.

2.3. Manajemen resiko sistem informasi

Komponen penting dari keamanan sistem informasi adalah manajemen resiko. Fungsi utama dari manajemen resiko adalah untuk mengurangi resiko. Mengurangi resiko berarti mengurangi resiko sampai resiko itu mencapai suatu tingkatan yang dapat diterima oleh suatu usaha kecil dan menengah. Manajemen resiko dapat didefinisikan sebagai mengidentifikasi, menganalisa, mengendalikan, dan meminimalkan kerugian yang berhubungan dengan suatu kejadian.

Identifikasi resiko pada suatu usaha kecil dan menengah memerlukan penjelasan unsur-unsur dasar berikut:

- Ancaman nyata
- Konsekuensi-konsekuensi dari ancaman yang terjadi
- Frekuensi kejadian dari suatu ancaman
- Tingkat keyakinan terhadap ancaman akan terjadi

Banyak proses-proses dan rumusan-rumusan yang dirancang untuk membantu memberikan beberapa kepastian ketika menjawab pertanyaan-pertanyaan di atas. Namun perlu disadari bahwa tidak semua kemungkinan dapat dipertimbangkan. Manajemen resiko berusaha sedapat mungkin untuk melihat masa depan dan untuk menurunkan kemungkinan ancaman-ancaman yang memberi dampak pada suatu usaha kecil dan menengah.

2.3.1. Manajemen resiko keamanan komputer pada UKM

Manajemen resiko keamanan komputer memiliki beberapa unsur, khususnya sebagai berikut:

- Melakukan Analisis Resiko, termasuk analisa biaya-manfaat dari perlindungan-perlindungan.
- Menerapkan, meninjau ulang, dan melakukan pemeliharaan terhadap perlindungan-perlindungan.

Untuk memberdayakan proses ini, perlu ditentukan beberapa properti dari berbagai unsur-unsur, seperti nilai dari asset-asset, ancaman-ancaman, dan kerentanan (*vulnerabilitie*) dan kemungkinan terjadinya suatu kejadian. Suatu bagian utama dari proses manajemen resiko adalah menentukan nilai kerugian yang diakibatkan dari ancaman-ancaman dan menafsir seberapa sering (atau tingkat kemungkinan) terjadinya ancaman-ancaman tersebut. Untuk melaksanakan tugas ini, beberapa terminologi dan rumusan-rumusan telah dikembangkan, dan manajer usaha kecil dan menengah harus secara penuh memahami ancaman-ancaman tersebut. Daftar dari definisi-definisi dan terminologi terdapat pada bagian berikut dan diurutkan menurut sebagaimana didefinisikan pada saat Analisis Risiko.

Tujuan dari Analisis Risiko

Tujuan utama tentang melakukan Analisis Risiko adalah untuk mengukur dampak dari ancaman-ancaman yang berpotensi untuk berdampak terhadap sistem, serta untuk menafsir harga atau nilai terhadap kemampuan bisnis yang hilang akibat ancaman-ancaman tersebut. Kedua hasil utama dari suatu analisis resiko adalah the identifikasi dari resiko-resiko dan pertimbangan kerugian / keuntungan dari pengantisipasi ancaman-ancaman tersebut - merupakan hal yang sangat penting pada saat pembuatan suatu strategi peringatan resiko.

Terdapat beberapa manfaat dari melakukan Analisis Resiko, antara lain adalah dapat membuat satu perbandingan kerugian/keuntungan yang jelas untuk perlindungan keamanan. Selain itu, juga mempengaruhi proses pengambilan keputusan yang bersangkutan dengan konfigurasi perangkat keras dan desain sistem perangkat lunak. Selain itu, juga membantu usaha kecil dan menengah untuk memberi focus terhadap dimana sumber daya keamanannya paling diperlukan. Dan juga dapat mempengaruhi keputusan-keputusan konstruksi dan perencanaan.

Definisi-definisi dan terminologi

Berikut adalah terminology Analisis Resiko yang perlu diketahui oleh manajer usaha kecil dan menengah:

Aset. Aset adalah suatu sumber daya, proses, produk, infrastruktur komputasi, dan sebagainya yang dimiliki oleh suatu usaha kecil dan menengah, dan yang harus dilindungi olehnya. Hilangnya asset bisa mempengaruhi kerahasiaan, integritas, atau ketersediaan ('CIA: *Confidentiality, integrity, or availability*'); atau juga dapat memberi dampak keseluruhan; atau juga dapat menyebabkan hilangnya nilai dari aset tersebut, dalam bentuk yang dapat terukur, maupun tidak terukur. Kehilangan aset juga dapat mempengaruhi kemampuan suatu usaha kecil dan menengah dalam menjalankan bisnisnya. Nilai dari suatu asset terdiri dari semua unsur-unsur yang berkaitan dengan asset tersebut, yang mencakup pembuatan, pengembangan, dukungan, penggantian, kredibilitas publik, biaya-biaya yang dipertimbangkan, dan nilai kepemilikan.

Ancaman. Secara singkat, ancaman adalah kehadiran akan segala peristiwa-peristiwa potensial yang menyebabkan suatu dampak yang tidak diinginkan pada usaha kecil dan menengah. Suatu ancaman bisa adalah alami atau buatan manusia, dan dampak yang kecil maupun besar terhadap keamanan atau kelangsungan dari suatu usaha kecil dan menengah.

Kerentanan. Kerentanan disebabkan oleh kelemahan atau tidak adanya upaya pengamanan terhadap sistem. Suatu ancaman kecil memiliki potensi untuk menjadi suatu ancaman lebih besar, atau satu ancaman lebih sering terjadi, oleh karena kerentanan. Kerentanan dapat dianggap sebagai suatu ancaman dapat melewati pengamanan dari sistem. Jika dikombinasikan dengan aset dan ancaman, kerentanan adalah bagian ke tiga dari suatu unsur yang disebut sebagai manajemen resiko.

Upaya Pengamanan. Upaya pengamanan adalah tindakan balasan atau kontrol yang dipekerjakan untuk mengurangi resiko yang terkait dengan satu ancaman spesifik atau kelompok dari ancaman-ancaman.

Exposure Factor (EF). *Exposure Factor* merepresentasikan persentase dari kerugian yang dipengaruhi oleh suatu peristiwa ancaman terhadap suatu aset spesifik. Nilai ini diperlukan untuk menghitung Perkiraan Kerugian Tunggal (SLE: *Single Loss Expectancy*), yang akan diperlukan untuk menghitung Perkiraan Kerugian Gabungan (ALE: *Annualized Loss Expectancy*). *Exposure Factor* dapat merupakan suatu persentase kecil, seperti efek dari hilangnya beberapa perangkat keras, atau satu persentase sangat besar, seperti karena hilangnya semua sumberdaya komputer.

Perkiraan Kerugian Tunggal (SLE). Suatu perkiraan kerugian tunggal adalah nilai uang yang diberikan terhadap suatu peristiwa tunggal. Perkiraan ini merepresentasikan suatu kerugian usaha kecil dan menengah yang disebabkan oleh suatu ancaman tunggal dan diperoleh dari rumusan berikut:

$$\text{Nilai Asset} * \text{Exposure Factor (EF)} = \text{SLE}$$

Sebagai contoh, suatu aset dihargai \$100,000 yang memiliki *exposure factor* sebesar 30 persen akan menghasiklan Perkiraan Kerugian Tunggal sebesar \$30,000. Figur ini adalah didefinisikan untuk menghitung Perkiraan Kerugian Gabungan (ALE), yang sering digunakan untuk menguraikan satu peristiwa kerusakan untuk suatu Penilaian Dampak Bisnis (BIA).

Tingkat Kejadian Gabungan (ARO: Annualized Rate of Occurrence). Tingkat Kejadian Gabungan adalah suatu angka yang merepresentasikan perkiraan frekuensi dari kejadian suatu ancaman. Nilainya berkisar antara 0.0 (tidak pernah) hingga angka yang besar (untuk ancaman-ancaman kecil, seperti salah mengeja nama-nama ketika memasukkan data). Bagaimana angka ini diperoleh dapat menjadi amat rumit. Angka tersebut biasanya dihasilkan berdasarkan kemungkinan terjadinya suatu peristiwa dan banyaknya karyawan yang dapat membuat suatu kesalahan terjadi. Kerugian yang terjadi oleh peristiwa ini belum menjadi perhatian di sini, hanya seberapa sering ancaman itu terjadi.

Sebagai contoh, suatu meteor yang merusak pusat data bisa diperkirakan untuk terjadi hanya sekali dalam 100,000 tahun mempunyai Tingkat Kejadian Gabungan (ARO) sebesar 0.00001. Sebaliknya, 100 operator *data entry* yang mencoba untuk mengakses sistem dengan cara tidak sah dapat diperkirakan enam kali dalam satu tahun per operator, dan akan mempunyai Tingkat Kejadiang Gabungan (ARO) sebesar dari 600.

Perkiraan **Kerugian Gabungan (ALE).** Perkiraan Kerugian Gabungan adalah suatu nilai uang yang diperoleh dari rumusan sebagai berikut:

$$\text{Perkiraan Kerugian Tunggal (SLE)} * \text{Tingkat Kejadian Gabungan (ARO)} = \text{Perkiraan Kerugian Gabungan (ALE)}$$

Dalam kata-kata lain, Perkiraan Kerugian Gabungan (ALE) adalah perkiraan kerugian keuangan per tahun terhadap suatu usaha kecil dan menengah yang

diakibatkan oleh suatu ancaman. Sebagai contoh, suatu ancaman dengan nilai uang \$100,000 (SLE) diperkirakan terjadi hanya sekali dalam 1,000 tahun (AROnya 0.001) akan mengakibatkan ALE sebesar \$ 100. Contoh ini membantu untuk menghasilkan analisa biaya-manfaat yang lebih dipercaya. Ingat bahwa SLE diperoleh dari nilai asset dan *Exposure Factor*. Tabel 2.2 menunjukkan rumusan-rumusan ini.

Tabel 2.2 Rumusan-Rumusan analisis risiko

KONSEP	RUMUSAN
<i>Exposure Factor</i> (EF)	Persentase dari kerugian aset yang disebabkan oleh ancaman
Perkiraan Kerugian Tunggal (SLE: <i>Single Loss Expectancy</i>)	Nilai Aset * <i>Exposure Factor</i> (EF)
Tingkat Kejadian Gabungan (ARO: <i>Anualized Rate of Occurrence</i>)	Frekuensi kejadian ancaman per tahun
Perkiraan Kerugian Gabungan (ALE: <i>Annualized Loss Expectancy</i>)	Perkiraan Kerugian Tunggal (SLE) * Tingkat Kejadian Gabunga (ARO)

2.3.2. Metode menganalisa resiko keamanan sistem informasi pada UKM

Terdapat empat unsur dasar dalam proses Analisis Resiko:

1. Analisis Resiko Kuantitatif
2. Analisis Resiko Kualitatif
3. Proses Penilaian Aset
4. Pemilihan Upaya Pengamanan

Analisis Resiko Kuantitatif

Perbedaan antara Analisis Resiko Kuantitatif dan Kualitatif adalah sederhana: Analisis Resiko Kuantitatif mencoba untuk memberi nilai objektif atau murni secara independen (sebagai contoh, nilai rupiah) untuk komponen penilaian resiko dan untuk penilaian nilai kerugian potensial. Analisis Resiko Kualitatif lebih berkaitan dengan nilai-nilai aset *intangible* dan memberi fokus terhadap aspek-aspek lain.

Ketika setiap unsur-unsur (nilai aset, dampak, frekuensi ancaman, keefektifan upaya dan biaya pengamanan, ketidak-pastian dan probabilitas) diukur, dinilai, dan diberi nilai, proses tersebut dianggap menjadi kuantitatif secara lengkap. Walaupun begitu, adalah tidak mungkin untuk melakukan Analisis Resiko Kuantitatif dengan lengkap, karena ukuran-ukuran kualitatif harus diterapkan. Dengan begitu, perlu disadari bahwa nilai yang ada pada kertas laporan tidak berarti dapat meramalkan masa depan.

Proses analisis resiko kuantitatif adalah suatu proyek utama, oleh karenanya memerlukan seorang manajer proyek untuk mengatur unsur-unsur utama dari analisis. Suatu bagian terbesar dari perencanaan awal untuk analisis resiko kuantitatif adalah penilaian waktu yang diperlukan untuk melaksanakan analisis. Sebagai tambahan, diperlukan juga untuk membuat suatu perencanaan proses secara rinci dan memberi peran-peran kepada tim resiko analisis.

Pengujian Keamanan Awal (PSE: *Preliminary Security Examination*). Pengujian Keamanan Awal diselenggarakan sebelum kegiatan Analisis Resiko Kuantitatif. Pengujian Keamanan Awal membantu mengumpulkan unsur-unsur yang di perlukan untuk Analisis Resiko Kuantitatif. Aktivitas ini akan membantu arah fokus dari Analisis Resiko. Unsur-unsur yang digambarkan pada tahap ini meliputi nilai-nilai dan biaya-biaya aset, suatu daftar dari berbagai ancaman terhadap suatu usaha kecil dan menengah (dalam hal ancaman-ancaman terhadap personil dan lingkungan), dan dokumentasi ukuran-ukuran keamanan ada. Pengujian Keamanan Awal juga perlu ditinjau ulang oleh suatu manajemen usaha kecil dan menengah sebelum Analisis Resiko dimulai.

Analisis Resiko Kualitatif

Analisis Resiko Kuantitatif tidak mencoba untuk memberi biaya-biaya mutlak terhadap unsur-unsur kerugian. Analisis Resiko lebih berorientasi terhadap skenario, dan berlawanan dengan Analisis Resiko Kuantitatif, Analisis Resiko Kualitatif yang murni adalah mungkin untuk dilakukan.

Frekuensi dari ancaman dan data dampak diperlukan untuk melakukan Analisis Resiko Kuantitatif. Dalam penafsiran resiko kualitatif, keseriusan dari ancaman-ancaman dan kepekaan relatif dari aset-aset diberi suatu urutan, atau penilaian kualitatif, dengan menggunakan suatu pendekatan skenario dan menciptakan suatu skala *exposure* untuk masing-masing skenario.

Dalam penjelasan mengenai pendekatan skenario, diperlukan untuk mencocokkan berbagai ancaman terhadap aset-aset yang diidentifikasi. Suatu skenario menguraikan jenis dari ancaman dan kerugian potensial terhadap aset tertentu, dan memilih upaya pengamanan untuk mengurangi resiko.

Prosedur Skenario Kualitatif

Setelah membuat daftar ancaman, mendefinisikan aset-aset yang perlu dilindungi, dan memberi skala *exposure*, skenario penafsiran resiko kualitatif dapat dimulai. Tabel berikut menampilkan contoh dari skala *exposure* yang sederhana.

Tabel 2.3 Skala Exposure yang Sederhana

Skala	Persentase <i>Exposure</i>
Kosong atau 0	Tidak ada kerugian yang dapat diukur
1	20% kerugian
2	40% kerugian
3	60% kerugian
4	80% kerugian
5	100% kerugian

Prosedur-prosedur dalam melaksanakan skenario tersebut adalah sebagai berikut:

- Suatu skenario harus menuliskan tiap ancaman
- Skenario ditinjau oleh para manajer unit bisnis untuk memastikan hal yang dikerjakan sesuai dengan kenyataan.
- Tim Analisis Resiko merekomendasikan dan mengevaluasi berbagai upaya pengamanan untuk masing-masing ancaman.
- Tim Analisis Resiko menelusuri tiap skenario dengan mempertimbangkan ancaman, aset dan upaya pengamanan.
- Tim menyiapkan temuan mereka dan menyerahkannya kepada pihak manajemen.

Setelah tiap skenario telah ditelusuri dan temuan-temuan diterbitkan, pihak manajemen harus menerapkan upaya pengamanan yang dipilih sebagai hal yang bisa diterima dan mulai mencari alternatif-alternatif untuk upaya-upaya pengamanan yang kurang efektif.

2.3.3. Tahapan melakukan analisa resiko keamanan sistem informasi pada UKM

Ketiga tahapan utama dalam melaksanakan satu analisis risiko adalah serupa dengan tahapan-tahapan dalam melaksanakan satu Penilaian Dampak Bisnis. Analisis resiko biasanya jauh lebih menyeluruh, dan dirancang untuk digunakan untuk mengukur skenario resiko yang banyak dan rumit.

Ketiga tahapan-tahapan utama adalah sebagai berikut:

1. Menafsir kerugian potensial terhadap aset-aset dengan menentukan nilai mereka.
2. Melakukan analisa terhadap ancaman-ancaman potensial terhadap aset-aset.
3. Mendefinisikan Perkiraan Kerugian Gabungan (ALE)

1. Menafsir Kerugian Potensial

Untuk menafsir kerugian potensial yang terjadi sepanjang kejadian dari suatu ancaman, aset-aset harus diberi nilai dengan menggunakan beberapa macam proses penilaian. Proses ini mengakibatkan suatu pemberian nilai keuangan terhadap asset, dengan melakukan perhitungan *Exposure Factor* (EF) dan perhitungan Perkiraan Kerugian Tunggal (SLE).

2. Meneliti Ancaman-ancaman Potensial

Untuk menggambarkan ancaman-ancaman, perlu dipahami kerentanan dari suatu aset, dan perlu dilakukan perhitungan ARO terhadap ancaman dan kerentanan.

Beberapa kategori ancaman adalah sebagai berikut:

- Klasifikasi Data. Pengumpulan data yang mengakibatkan inferensi data, manipulasi kanal terlindung, kode berbahaya: virus, *Trojan*, *worm*, bom logis, atau pengkonsentrasian tanggung jawab (kurangnya pembagian tugas).
- Peperangan informasi. Terorisme berorientasi teknologi, kode berbahaya atau bom logis atau penghalangan hubungan untuk militer atau spionase ekonomi.
- Personil. Akses sistem yang tak terkendalikan atau yang tidak sah, penyalahgunaan teknologi oleh para pengguna yang tidak memiliki hak, perusakan oleh karyawan yang tidak puas, atau data input yang dipalsukan.
- Aplikasi / Operasional. Satu aplikasi keamanan yang tidak efektif yang mengakibatkan kesalahan prosedur atau input data yang salah.
- Tindakan Kriminal. Kerusakan fisik, pencurian informasi atau aset-aset, pencurian oleh orang dalam usaha kecil dan menengah yang terorganisir, perampokan bersenjata, atau ancaman fisik yang merugikan personil.
- Ancaman terhadap Lingkungan. Kegagalan utilitas, penghentian pelayanan, bencana-bencana alam, atau resiko-resiko berdekatan.
- Infrastruktur komputer. Perangkat keras / peralatan yang gagal, kegagalan program, kekurangan-kekurangan sistem operasi, atau kegagalan sistem komunikasi.
- Pengolahan yang tertunda. Pengurangan produktivitas atau pengumpulan dana yang tertunda yang dapat mengurangi pendapatan, biaya yang ditingkatkan, atau keterlambatan pembayaran.

3. Mendefinisikan Perkiraan Kerugian Gabungan (ALE)

Setelah menentukan SLE dan ARO, ALE dapat diestimasi dengan menggunakan rumusan yang sebelumnya telah diuraikan.

Hasil-hasil

Setelah melaksanakan Analisis Resiko, pada hasil-hasil akhir perlu ada:

- Penilaian aset-aset kritis dalam biaya nyata
- Daftar yang terperinci dari ancaman-ancaman penting
- Kemungkinan terjadinya setiap ancaman, dan frekuensi dari kejadian.
- Potensi kerugian yang diakibatkan oleh suatu ancaman, yaitu dampak dari terjadinya ancaman terhadap suatu aset (dalam nilai uang).
- Pendekatan tindakan perbaikan yang disarankan dan upaya perlindungan atau tindakan balasan.

Perbaikan-perbaikan

Terdapat tiga perbaikan-perbaikan umum yang dapat diwujudkan oleh satu atau kombinasi dari tiga bentuk sebagai berikut:

- Pengurangan Resiko. Mengambil langkah untuk mengubah atau meningkatkan posisi resiko dari suatu aset di dalam keseluruhan perusahaan.
- Pemindahan Resiko. Memindahkan biaya potensial dari suatu kerugian ke pihak lain (misalnya kepada perusahaan asuransi).

- Penerimaan Resiko. Menerima tingkat kerugian yang akan terjadi dan menanggung kerugian itu.

Perbaikan yang dipilih biasanya yang menghasilkan pengurangan resiko yang terbesar, dan yang mengeluarkan biaya tahunan terendah dalam pemeliharannya.

3. Model Ekonomis Keamanan Sistem Informasi pada UKM

3.1. *Memperkirakan potensi kerugian pada keamanan sistem informasi pada UKM*

Berikut adalah beberapa alasan tambahan akan pentingnya mendefinisikan biaya atau nilai dari suatu asset:

- Penilaian aset diperlukan untuk melaksanakan analisa biaya-manfaat.
- Nilai asset dianggap penting untuk keperluan asuransi.
- Nilai asset mendukung keputusan-keputusan pemilihan upaya pengamanan.
- Penilaian asset dapat diperlukan untuk mencukupi “kepedulian” dan mencegah ketidakpekaan terhadap kewajiban hukum.

Unsur-unsur yang Menentukan Nilai dari suatu Asset

Ketiga unsur-unsur dasar yang menentukan nilai dari suatu aset informasi adalah:

1. Biaya awal dan biaya yang berkelanjutan (terhadap suatu usaha kecil dan menengah) mengenai pembelian, perijinan, pengembangan, dan pendukung pada aset informasi
2. Nilai asset untuk operasi produksi, riset dan pengembangan, dan kelangsungan hidup model bisnis
3. Nilai aset pada pasar eksternal dan nilai yang diperkirakan dari *intellectual property* properti-properti cendekiawan (rahasia perniagaan, hak paten, hak cipta, dan sebagainya)

3.2. *Proses pengumpulan informasi aset keamanan sistem informasi pada UKM*

Saat anda memikirkan tentang data yang rahasia, anda akan memikirkan mata-mata bukan? Hal inilah yang mirip dengan yang akan dibahas penulis di sini. Pengguna komputer memiliki data dalam hard disk yang pribadi, rahasia dan penting bagi anda dan keluarga anda. Banyak orang memanfaatkan layanan perbankan *online*, membeli dari toko *online*, membuat pembukuan keuangan dan menghitung pajak menggunakan komputer mereka. Jika anda memiliki kamera digital, anda mungkin juga memiliki beberapa foto dalam hard disk – yang tidak penting, namun berharga. Beberapa hal yang anda hargai mungkin sesederhana data game favorit anda yang disimpan.

Penulis tidak menasihatkan manajer usaha kecil dan menengah untuk melakukan klasifikasi data secara istimewa. Namun manajer usaha kecil dan menengah wajib memikirkan data apa yang penting dan seberapa pentingnya data tersebut untuk dilindungi. Jika tidak terdapat data pada komputer yang berharga untuk dilindungi, maka pengamanan data komputer tidak diperlukan. Dengan cara berpikir yang demikian, manajer usaha kecil dan menengah tidak memerlukan sistem klasifikasi data yang kompleks, namun cukup menggunakan cara intuitif yang tidak

menyebabkan kebingungan. Manajer usaha kecil dan menengah dapat mencoba kategori berikut:

Dapat digantikan: Data yang disimpan dalam CD atau media permanen lainnya dan dapat digantikan dengan instalasi ulang atau menggandakan kembali ke hard disk komputer. Data yang dapat digantikan juga termasuk perangkat lunak yang dapat diunduh dari internet. Namun, perlu diperhatikan bahwa perangkat lunak yang demikian mungkin tidak berkualifikasi sebagai data yang tidak dapat digantikan, bila pengguna tidak dapat dengan mudah mengingat URL untuk mencapai tempat mengunduh atau tidak memiliki *back up* atau kode sumbernya.

Kritis: Data yang manajer usaha kecil dan menengah yakini harus dapat dipulihkan atau dilindungi seperti dokumen pajak atau informasi finansial.

Penting: Data yang ingin dilindungi, meskipun data tersebut tidak benar-benar penting. Yang termasuk dalam kategori ini adalah resep lembar kerja yang telah dibuat atau data lain yang sulit dibuat atau membutuhkan waktu untuk digantikan.

Lainnya: Hal-hal lainnya yang tersisa selain ketiga kategori pertama di atas. Data ini tidak cukup penting untuk dikategorikan atau diketahui tidak berharga untuk dilindungi atau disimpan.

Menggunakan kategori-kategori ini, manajer usaha kecil dan menengah dapat membentuk gagasan yang tidak kaku mengenai apa yang patut disimpan dan dilindungi dalam hard disk. Manajer usaha kecil dan menengah tidak perlu menulis lokasi data dan kategori data atau bahkan melacaknya. Yang terpenting adalah manajer usaha kecil dan menengah telah memikirkan mengenai data dan tahu apa yang dilindungi.

3.3. Analisis ekonomi perancangan dan penerapan keamanan sistem informasi pada UKM

Setelah analisis resiko dilaksanakan, upaya pengamanan harus diteliti dan direkomendasikan. Terdapat beberapa prinsip-prinsip baku yang digunakan dalam pemilihan upaya pengamanan untuk memastikan bahwa suatu upaya pengamanan dapat dicocokkan dengan suatu ancaman dan memastikan bahwa upaya perlindungan menerapkan kontrol yang diperlukan dan paling efisien. Ukuran-ukuran penting yang harus diuji sebelum memilih suatu tindakan balasan efektif.

Analisa biaya / keuntungan

Kriteria seleksi upaya pengamanan yang utama adalah keefektifan pembiayaan dari kendali (kontrol) yang diterapkan, yang diperoleh melalui proses analisis biaya keuntungan. Untuk menentukan total biaya upaya pengamanan, banyak unsur-unsur yang perlu untuk dipertimbangkan, termasuk yang disajikan berikut:

- Pembelian, pengembangan, dan/atau biaya-biaya perijinan untuk upaya pengamanan
- Biaya instalasi fisik dan gangguan terhadap produksi normal selama instalasi dan uji coba upaya pengamanan dilaksanakan.
- Biaya operasi normal, alokasi sumber daya, dan biaya pemeliharaan.

Kalkulasi yang paling sederhana untuk menghitung biaya / manfaat untuk upaya pengamanan adalah sebagai berikut:

$$(ALE \text{ sebelum menerapkan upaya pengamanan}) - (ALE \text{ setelah implementasi upaya pengamanan}) - (\text{Biaya upaya pengamanan}) = \text{Nilai dari upaya pengamanan bagi usaha kecil dan menengah}$$

Sebagai contoh, jika suatu ALE dari suatu ancaman adalah \$10,000, ALE setelah implementasi upaya pengamanan adalah \$1,000, dan biaya tahunan untuk mengoperasikan upaya pengamanan adalah \$500, kemudian nilai dari upaya pengamanan adalah \$ 8,500 per tahun. Jumlah ini kemudian adalah dibandingkan terhadap biaya-biaya awal, kemudian ditentukan bila upaya pengamanan yang ditentukan akan bermanfaat atau tidak.

Nilai ini dapat diperoleh untuk satu upaya pengamanan atau dapat diperoleh untuk suatu gabungan dari upaya-upaya pengamanan melalui rangkaian dari perhitungan yang kompleks. Selain rasio biaya-manfaat keuangan, faktor-faktor lain dapat mempengaruhi keputusan untuk menerapkan suatu upaya pengamanan yang spesifik. Sebagai contoh, suatu usaha kecil dan menengah berkewajiban secara hukum jika biaya upaya pengamanan lebih kecil dari biaya yang dibutuhkan untuk mengantisipasi realisasi suatu ancaman ketika usaha kecil dan menengah tidak menerapkan upaya pengamanan.

Tingkat Operasi Manual

Jumlah dari intervensi manual memerlukan untuk mengoperasikan upaya pengamanan juga menjadi salah satu faktor dalam pemilihan upaya pengamanan. Dalam berbagai kasus, kerentanan disebabkan oleh kesalahan manusia atau ketidak-konsistenan pada aplikasi. Sistem otomatis membutuhkan ukuran standar yang aman untuk memungkinkan pemberhentian sistem aplikasi secara manual jika terjadi suatu kerentanan.

Suatu upaya pengamanan seharusnya tidak terlalu sulit untuk dioperasikan, dan seharusnya tidak bertentangan produksi dari operasi normal. Karakteristik-karakteristik ini adalah penting untuk penerimaan kendali oleh para personil dan untuk memperoleh dukungan dari pihak manajemen yang dibutuhkan untuk memastikan keberhasilan dari upaya pengamanan.

Fitur Akuntabilitas dan Auditabilitas

Upaya pengamanan harus mempertimbangkan fungsi akuntansi dan audit. Upaya pengamanan juga harus mempunyai kemampuan yang baik sehingga dapat diuji dan diaudit oleh para auditor, dan akuntabilitasnya harus diterapkan agar secara efektif dapat menelusuri masing-masing individu yang mengakses tindakan balasan atau fitur-fiturnya.

Kemampuan untuk perbaikan

Tindakan balasan bagi upaya pengamanan harus dievaluasi dengan kaitannya terhadap status dari fungsinya setelah pengaktifannya. Selama dan setelah batasan kondisi tertentu, upaya pengamanan harus menyediakan:

- Tidak ada perusakan asset selama pengaktifan atau *reset*
- Tidak ada jalur terlindung yang mengakses ke atau melalui kontrol selama *reset*
- Tidak ada kerugian pengamanan atau peningkatan *exposure* setelah aktivasi atau *reset*.
- Status *default* seharusnya tidak memberi hak atau akses apapun atau akses sampai kendali-kendali beroperasi secara penuh.

Hubungan-hubungan Vendor

Kredibilitas, kehandalan, dan kinerja masa lalu dari *vendor* upaya pengamanan harus dinilai. Sebagai tambahan, keterbukaan (*open source*) dari pemrograman aplikasi seharusnya juga dikenal untuk menghindari kerahasiaan desain yang mencegah modifikasi-modifikasi pada kemudian hari atau mengizinkan aplikasi yang tak dikenal untuk mempunyai satu pintu belakang (*back door*) ke dalam sistem. Dukungan tambahan dari vendor, serta dokumentasi perlu juga dipertimbangkan.

Keterangan mengenai ‘Pintu Belakang’

‘Pintu belakang’ (*Back Door*) adalah suatu unsur pemrograman yang memberi kesempatan kepada *programmer* untuk mengakses sampai komponen-komponen internal dari suatu aplikasi, dengan demikian melewati pengendalian keamanan dari suatu aplikasi.

4. Implementasi Keamanan Sistem Informasi pada UKM

4.1. *Tanggung Jawab keamanan sistem informasi UKM*

Konsep keamanan sistem informasi usaha kecil dan menengah perlu mendefinisikan peran-peran yang terlibat dan bertanggung jawab dalam manajemen sistem keamanan tersebut. Peran-peran dalam sistem keamanan komputer dalam usaha kecil dan menengah tidak sama dengan atribut pegawai dan manajer yang berlaku dalam usaha kecil dan menengah. Satu peran dapat dipegang oleh beberapa orang dan satu orang dapat memegang beberapa peran, tetapi peran-peran tersebut harus fleksibel sesuai dengan kebutuhan keamanan komputer usaha kecil dan menengah.

4.1.1. Peran-peran pada keamanan sistem informasi UKM

Beberapa peran yang bertanggung jawab dalam keamanan komputer usaha kecil dan menengah:

- Pemilik, merupakan peran yang membuat suatu data pada sistem informasi pada usaha kecil dan menengah.
- Penanggung jawab, merupakan peran yang bertanggung jawab untuk menjaga dan merawat integritas data sistem informasi pada usaha kecil dan menengah.
- Pengguna, merupakan peran yang memanfaatkan data untuk melaksanakan suatu proses bisnis di usaha kecil dan menengah.

4.1.2. Peran dan tanggung jawab implementasi kebijakan keamanan sistem informasi pada UKM

Kesadaran akan keamanan seringkali menjadi unsur yang terlewatkan pada manajemen keamanan, sebab waktu dari perancang upaya pengamanan kebanyakan tersita untuk merancang control, mendeteksi gangguan, menafsirkan risiko, dan secara proaktif atau secara reaktif mengatur keamanan. Manusia adalah mata rantai paling lemah dalam rantai keamanan sebab mereka tidak terlatih atau secara umum sadar akan pentingnya keamanan. Karyawan harus memahami bagaimana tindakan-tindakan mereka, tindakan-tindakan sepertinya tidak penting, dapat berdampak terhadap keseluruhan posisi keamanan dari suatu usaha kecil dan menengah.

Karyawan harus sadar akan harus menjamin/mengamankan informasi dan untuk melindungi asset-asset informasi dari suatu perusahaan. Operator memerlukan pelatihan di dalam ketrampilan-ketrampilan yang diperlukan untuk memenuhi fungsi pekerjaan mereka dengan aman, dan pelatihan kebutuhan praktisi-praktisi keamanan untuk menerapkan dan memelihara keamanan perlu mengendalikan.

Setiap karyawan memerlukan pendidikan akan konsep-konsep dasar dari keamanan dan manfaat-manfaatnya untuk usaha kecil dan menengah dimana ia

bekerja. Keuntungan-keuntungan ketiga tiang dari pelatihan akan kesadaran keamanan : kesadaran, pelatihan, dan pendidikan, akan membantu mereka untuk meningkatkan sikap dan perilaku para personil, dan menghasilkan peningkatan yang signifikan bagi keamanan usaha kecil dan menengah.

Kesadaran

Berbeda dengan pelatihan, kesadaran akan keamanan mengacu secara umum terhadap kesadaran kolektif dari para personil yang bekerja di dalam usaha kecil dan menengah, akan pentingnya keamanan dan control keamanan. Selain dari manfaat dan tujuan yang telah dibahas sebelumnya, program kesadaran akan keamanan juga memiliki manfaat-manfaat sebagai berikut:

- Membuat suatu pengurangan terukur dalam tindakan-tindakan yang tidak syah yang dicoba dilakukan oleh personil.
- Meningkatkan efektivitas dari pengendalian perlindungan
- Membantu menghindari tipuan, penyalahgunaan, dan penyalahgunaan sumber daya komputer.

Personil dipertimbangkan sebagai “sadar akan keamanan” bila mereka dengan jelas memahami kebutuhan akan keamanan, bagaimana keamanan komputer berdampak pada kelangsungan hidup usaha kecil dan menengah dan terhadap resiko yang terjadi tiap harinya terhadap sumber daya komputer.

Adalah penting untuk memiliki sesi-sesi kesadaran berkala untuk memberi wawasan kepada karyawan baru dan menyegarkan pengetahuan para karyawan senior. Materi perlu selalu lugas, sederhana, dan jelas. Sebaiknya tidak menggunakan terlalu banyak kata-kata jargon yang berkaitan dengan teknologi, dan menyesuaikan materi dengan peserta yang ditargetkan, sehingga akan menjadi lebih mudah untuk dipahami. Materi perlu menunjukkan bagaimana keamanan merupakan hal yang penting terhadap usaha kecil dan menengah dan bagaimana pentingnya pengamanan itu.

Berikut adalah beberapa cara untuk meningkatkan kesadaran akan keamanan dalam perusahaan, tanpa harus menghabiskan biaya dan sumberdaya:

- Mengadakan presentasi secara langsung, melalui ceramah, kuliah, video-video, dan pelatihan berbasis komputer.
- Melalui publikasi, dengan menempelkan poster-poster, majalah perusahaan, dan penggunaan intranet.
- Memberi insentif. Pemberian sertifikat dan anugerah-anugerah untuk prestasi terkait dengan keamanan.
- Peringatan-Peringatan. Melalui banner yang muncul pada saat masuk ke sistem, atau pesan-pesan dalam berupa tulisan pada alat-alat tulis kantor.

Namun perlu dipertimbangkan untuk tidak memberi peringatan yang berlebihan, penting sekali untuk mempertimbangkan keseimbangan dalam upaya untuk menyadarkan para anggota usaha kecil dan menengah terhadap pentingnya keamanan. Suatu program kesadaran harus kreatif dan sering diperbaharui.

Pendidikan dan pelatihan

Pelatihan berbeda dengan kesadaran, karena menggunakan ruang kelas spesifik atau pelatihan per orang. Jenis-jenis pelatihan sebagai berikut dapat dihubungkan dengan InfoSec:

- Pelatihan yang terkait dengan keamanan untuk operator dan para pengguna yang spesifik.
- Pelatihan kesadaran untuk departemen-departemen spesifik atau personil yang memiliki posisi yang sensitif terhadap keamanan.
- Pelatihan keamanan teknis untuk personil *IT Support* dan administrator sistem informasi.
- Pelatihan InfoSec tingkat mahir untuk auditor-auditor sistem informasi dan praktisi-praktisi keamanan
- Pelatihan keamanan untuk para manajer senior, para manajer fungsional, dan para manajer unit bisnis

Pendidikan dan pelatihan yang mendalam untuk personil sistem, auditor-auditor, dan para profesional keamanan adalah perlu dipertimbangkan untuk pengembangan karir. Sebagai tambahan, pelatihan produk yang spesifik untuk perangkat keras dan perangkat lunak keamanan adalah juga hal penting untuk perlindungan perusahaan.

Satu titik awal baik untuk mempersiapkan suatu program pelatihan keamanan bisa adalah topik-topik mengenai kebijakan-kebijakan, standar-standar, petunjuk, dan prosedur-prosedur yang digunakan pada satu usaha kecil dan menengah. Diskusi mengenai resiko-resiko alami atau lingkungan atau suatu diskusi mengenai peristiwa-peristiwa kesalahan dalam pengamanan sistem dapat dilakukan. Satu teknik pelatihan umum adalah untuk membuat skenario hipotetis mengenai kerentanan dari suatu sistem, dan memberi para siswa tugas untuk memberi rekomendasi akan beberapa pemecahan

Kebutuhan akan pelatihan mengenai keamanan sistem kepada para pengguna

Semua personil yang menggunakan satu sistem seharusnya pernah mengikuti pelatihan keamanan yang dapat dikerjakan secara spesifik, maupun konsep-konsep keamanan secara umum. Pelatihan adalah terutama penting untuk yang para pemakai yang sedang menangani data kritis atau sensitif. Kedatangan teknologi komputer sudah menciptakan suatu kesempatan untuk terjadinya kegagalan-kegagalan serius pada aspek kerahasiaan, integritas, dan ketersediaan.

4.2. Kegiatan mengumpulkan status keamanan sistem informasi

4.2.1. Kriteria evaluasi tingkat keamanan sistem informasi pada UKM

Berikut terdapat beberapa hal yang dapat membantu manajer usaha kecil dan menengah memahami resiko keamanan komputer atau sistem keamanan. Tabel 4-1

merupakan contoh daftar apa yang mungkin berharga untuk dilindungi pada komputer atau sistem informasi dan peringkat resiko dari inventori yang beresiko tersebut. Tabel 4-2 merupakan tabel kosong. Manajer usaha kecil dan menengah dapat menggunakannya atau membuat tabel serupa untuk memahami resiko secara menyeluruh. Daftar resiko hanyalah tempat mencatat dan mengkonsolidasikan daftar hal-hal yang anda perlukan untuk melindungi komputer dan sistem informasi usaha kecil dan menengah. Isilah dengan informasi berikut:

- **What Am I Protecting?:** Cantumkan semua hal yang ingin dilindungi. Mungkin anda memiliki lebih dari satu entri untuk setiap item bila item tersebut menghadapi lebih dari satu resiko.
- **Risk Number/Description:** Nama atau nomor resiko dari tabel 4-3 yang diberikan pada entri ini.
- **Exposure:** Nilai 1 hingga 10 menyatakan keterbukaan data (*exposure*) terhadap ancaman yang dicantumkan (1 untuk resiko rendah; 10 untuk resiko tinggi).
- **Cost:** Nilai 1 hingga 10 menyatakan biaya kerugian akibat kehilangan data ini (1 untuk biaya yang rendah; 10 untuk biaya yang tinggi).
- **Mitigation:** Deskripsi singkat apa yang dilakukan untuk mengurangi dampak resiko pada item tersebut.
- **Classification and Classification Value:** Jika anda mengklasifikasikan data anda, anda dapat menggunakan kolom ini untuk mencatat klasifikasi data dan nilai relatif yang diberikan. Misalnya disini *critical* (nilai 10), *important* (nilai 6), *replaceable* (value 2) dan *other* (nilai 0).

Tabel 4-3 merupakan deskripsi resiko umum yang biasanya dialami sistem informasi, dengan deskripsi singkat. Sekali lagi, tabel-tabel ini hanyalah contoh. Manajer usaha kecil dan menengah dapat menggunakan tabel ini secara bebas sesuai kebutuhannya.

Bagaimana daftar resiko ini membantu manajer usaha kecil dan menengah? Manajer usaha kecil dan menengah dapat menggunakan daftar resiko ini untuk memahami resiko ini secara cepat. Tidak terdapat satu metode yang cocok bagi setiap orang dan memahami tiap item pada daftar jauh lebih penting dari memberikan “nilai” pada keseluruhan resiko yang dialami. Namun mendapatkan sekilas informasi resiko yang dimiliki sistem informasi usaha kecil dan menengah bermanfaat saat manajer usaha kecil dan menengah memutuskan untuk membelanjakan pengeluaran atau mencoba memilih teknologi yang ada. Pada akhirnya, coba gunakan pada daftar kosong (atau buat salinannya) dan ikuti langkah-langkah berikut untuk mendapatkan informasi lengkap resiko yang anda hadapi

1. Untuk setiap entri pada daftar resiko, berikan resiko nama atau nomor, nilai *exposure* (1-10) dan *cost* (1-10). Deskripsikan tiap *Mitigating factors*. Jika anda sedang mengklasifikasikan data, tambahkan *Classification* pada kolom berikut.
2. Untuk tiap resiko, berikan nilai 2 jika diklasifikasikan sebagai *replaceable*, 6 jika *important* dan 10 jika *critical*. Tempatkan nilai tersebut pada kolom *Classification Value*.
3. Pada kolom paling kanan, jumlahkan nilai-nilai *exposure*, *cost* dan *classification* untuk tiap resiko.
4. Selanjutnya jumlahkan semua nilai resiko yang ada dalam daftar untuk mendapatkan nilai *Overall Risk*.
5. Pada bagian bawah tabel, hitung jumlah resiko yang dicantumkan dan masukan nilai tersebut.
6. Hitung *Minimum Risk Value* dengan mengalikan jumlah resiko dengan 4.

7. Hitung *Maximum Risk Value* dengan mengalikan jumlah resiko dengan 30 jika menggunakan klasifikasi data. Jika tidak mengklasifikasikan data, kalikan dengan 20.
8. Sekarang hitung *Overall Risk Percentage* dengan membagi Overall Risk Value dengan Maximum Risk Value dan mengalikannya dengan 100. (Dua kotak ditampilkan, satu untuk memasukkan nilai bila tidak mengklasifikasikan data dan satu lagi untuk nilai bila klasifikasi data dilakukan).

Tabel 4.1 Contoh Daftar Resiko yang diisi

What Am I Protecting?	Risk Number	Exposure	Cost	Mitigation	Classification	Classification Value	Row Risk Value
Data Internet Banking	3	4	9	UPS or line-conditioning device	Critical	10	23
Data Internet Banking	4	2	7	Backups	Critical	10	19
Polis Asuransi	4	2	5	Backups	Important	6	13
Polis Asuransi	10	7	4	Backups	Important	6	17
E-mail	7	8	6	Virus scanner	Important	6	20
E-mail	8	6	8	Firewall or secured e-mail server	Important	6	20
User ID Online Service(s)	4	3	3	Recoverable through the online service	Replaceable	2	8
Data Pengguna Sistem Informasi Internal	9	3	10	None	Critical	10	23
Data Finansial dan Pajak	3	2	9	Backups	Critical	10	21
Informasi Kartu Kredit	8	5	8	Fraud protection through credit card company	Important	6	19
Data Pribadi	3	1	6	None	Replaceable	2	9
Foto dan Film Digital							0
Informasi Konfigurasi Aplikasi							0

Alamat <i>e-mail</i> dan buku telepon							0	
Informasi lainnya							0	
Informasi Bisnis							0	
Data Kerja Karyawan/Manajer di Rumah							0	
Informasi Lainnya Identitas Pengguna Komputer							0	
			Nilai Total Resiko					192
Jumlah resiko terdaftar	18							
Nilai Minimum Resiko	72		<i>Gunakan kotak bagian atas bila mengklasifikasikan data dan kotak bagian bawah jika tidak mengklasifikasikan data</i>					
Nilai Resiko Maksimum (dengan klasifikasi)	540		Persentasi Total Resiko (dengan klasifikasi)		35.56			
Nilai Resiko Maksimum (tanpa klasifikasi)	360		Persentasi Total Resiko (tanpa klasifikasi)		53.33			

Tabel 4.2 Contoh Daftar Resiko yang kosong

What Am I Protecting?	Risk Number	Exposure	Cost	Mitigation	Classification	Classification Value	Row Risk Value
Data Internet <i>Banking</i>				UPS or line-conditioning device	Critical		
Data Internet <i>Banking</i>				Backups	Critical		
Polis Asuransi				Backups	Important		
Polis Asuransi				Backups	Important		
<i>E-mail</i>				<i>Virus scanner</i>	Important		
<i>E-mail</i>				<i>Firewall or secured e-mail server</i>	Important		

User ID Online Service(s)				Recoverable through the online service	Replaceable			
Data Pengguna Sistem Informasi Internal				None	Critical			
Data Finansial dan Pajak				Backups	Critical			
Informasi Kartu Kredit				Fraud protection through credit card company	Important			
Data Pribadi				None	Replaceable			
Foto dan Film Digital								
Informasi Konfigurasi Aplikasi								
Alamat e-mail dan buku telepon								
Informasi lainnya								
Informasi Bisnis								
Data Kerja Karyawan/Manajer di Rumah								
Informasi Lainnya Identitas Pengguna Komputer								
			Nilai Total Resiko					
Jumlah resiko terdaftar								
Nilai Minimum Resiko			<i>Gunakan kotak bagian atas bila mengklasifikasikan data dan kotak bagian bawah jika tidak mengklasifikasikan data</i>					
Nilai Resiko Maksimum (dengan klasifikasi)			Persentasi Total Resiko (dengan klasifikasi)					
Nilai Resiko Maksimum (tanpa klasifikasi)			Persentasi Total Resiko (tanpa klasifikasi)					

Tabel 4.3 Penomoran dan Penamaan Resiko serta Deskripsinya

Number	Name	Description
1	Tegangan kejut/sambaran petir	Interupsi dan kejutan daya listrik lokal menyebabkan kegagalan kerja hardware atau kerusakan data
2	Bencana Alam	Salah satu kelompok kejadian tak terduga dan terencana karena kejadian alam.
3	Fluktuasi daya listrik yang menyebabkan kerusakan data	Kejutan dan perubahan tegangan listrik dapat menyebabkan kerusakan data tanpa menyebabkan kerusakan sistem.
4	Kegagalan normal pemakaian perangkat keras	Bagian bergerak gagal berfungsi, <i>drives</i> atau kipas berhenti berputar dan lain sebagainya.
5	Kegagalan perangkat lunak akibat bencana	Menjatuhkan komputer saat memindahkannya.
6	Kegagalan atau cacat perangkat lunak	Kegagalan perangkat lunak merusak atau menghancurkan data.
7	Virus	Virus komputer atau <i>e-mail</i> mengubah atau menghancurkan data.
8	Pengubahan data (<i>tampering</i>)	Seseorang mengubah data tanpa wewenang secara sengaja.
9	Penghancuran data (<i>malicious destruction</i>)	Seseorang menghancurkan data tanpa wewenang secara sengaja.
10	Kesalahan manusia	Seseorang mengubah atau menghancurkan data tanpa sengaja.
11	Listrik Padam	Listrik padam dalam jangka waktu singkat atau lama sehingga sistem padam secara tidak normal atau tidak dapat dipergunakan.

4.2.2. Tindak lanjut status keamanan sistem informasi

Hasil dari proses tersebut adalah nilai persentase keseluruhan resiko yang menyatakan resiko keseluruhan keamanan usaha kecil dan menengah. Jika nilai persentase keseluruhan resiko keamanan usaha kecil dan menengah di bawah 30 persen, keamanan komputer dan sistem informasi usaha kecil dan menengah tersebut termasuk dalam kelompok rendah. Nilai persentase keseluruhan resiko keamanan usaha kecil dan menengah di antara 31 persen hingga 80 persen tergolong kelompok resiko keamanan komputer dan sistem informasi tergolong menengah, sedangkan nilai persentase keseluruhan resiko keamanan usaha kecil dan menengah diatas 81 persen hingga 100 persen termasuk kategori resiko keamanan komputer dan sistem informasi yang tinggi. Metode ini merupakan metode sangat sederhana yang dirancang untuk memberikan ringkasan yang luas tentang resiko keamanan komputer dan sistem informasi usaha kecil dan menengah anda. Jika manajer usaha kecil dan menengah memilih beberapa kelompok data yang dikualifikasikan sebagai *critical*, manajer

usaha kecil dan menengah mungkin akan memilih untuk mengamankan komputer dan sistem informasi usaha kecil dan menengah anda tanpa memperdulikan keseluruhan nilai resiko. Inti dari penjelasan metode ini adalah keputusannya tergantung manajer usaha kecil dan menengah itu sendiri. Perangkat tabel ini hanya memberikan manajer usaha kecil dan menengah pandangan sekilas tentang resiko keamanan komputer dan sistem informasi yang dimilikinya.

Setelah manajer usaha kecil dan menengah mengetahui resiko keamanan dan sistem informasi usaha kecil dan menengahnya, manajer usaha kecil dan menengah dapat mulai membuat keputusan tentang ukuran keamanan komputer dan sistem informasi apa yang perlu untuk melindungi data. Penulis mulai membahas ukuran keamanan keamanan dan sistem informasi usaha kecil dan menengah yang dapat dipergunakan manajer usaha kecil dan menengah untuk memperoleh keamanan komputer dan sistem informasi yang diinginkan.

4.3. Teknologi keamanan sistem informasi pada UKM

Sistem Operasi Windows merupakan sistem operasi klien yang terbanyak pemakaiannya. Sejumlah besar sistem *server* juga diinstalasi di seluruh dunia. Sesuatu yang digunakan ratusan juta orang secara alamiah menjadi sasaran empuk *hacking* dan upaya pembobolan sistem keamanan komputer dan sistem informasi, jika hanya memandang jumlah yang besar sebagai kesempatan yang besar untuk mencapai kesuksesan eksploitasi untuk memperoleh sesuatu yang berharga. Sangat mudah dipercaya bahwa seseorang setiap saat berupaya menerobos keamanan sistem Windows.

Selain faktor internal dari komputer harus dipertimbangkan faktor eksternal di luar komputer misalnya koneksi komputer ke internet. Jumlah pengguna sistem komputer di dunia semakin banyak, dan sebagian besar terhubung dengan Internet. Menurut *Computer Industry Almanac*, populasi pengguna Internet di dunia sudah mencapai 1.08 milyar (ClickZ Stats 2005, online <<http://www.clickz.com/stats/sectors/geographics/article.php/151151>>, accessed 13 December 2005). Hal ini memberi kesempatan yang tinggi untuk para *hacker* untuk berupaya untuk menembus upaya pengamanan suatu sistem. Upaya pengamanan sistem menjadi suatu permainan *push/pull* eksploitasi dan perbaikan sistem. Setiap perubahan pada suatu sistem operasi akan memberi kesempatan baru bagi para *hacker* untuk melakukan eksploitasi dan kerusakan terhadap sistem. Suatu UKM yang menggunakan sistem komputer (apalagi yang terhubung dengan Internet) tentunya akan menghadapi masalah ini, sehingga perlu mempertimbangkan upaya pengamanan yang lebih untuk sistem komputer yang digunakan, agar upaya eksploitasi dan pengrusakan yang dilakukan oleh para hacker dapat dicegah.

Menentukan apakah sistem komputer menjadi target para *hacker*

Probabilitas suatu sistem komputer menjadi target para *hacker* adalah cukup tinggi. Namun jika suatu sistem dianggap kurang menarik, atau sulit untuk ditembus, mereka biasanya mencari target yang lebih mudah untuk ditembus. Apa yang mendeteksi bahwa suatu sistem dieksploitasi oleh para *hacker*? Jawabannya tergantung terhadap *hacker*-nya, sistem operasi yang digunakan, dan teknik-teknik yang digunakan untuk mendeteksi adanya eksploitasi. Jika suatu sistem mendukung ACL (*Access Control List*) dan *auditing*, disarankan untuk mengaktifkan ACL dan

auditing tersebut pada level yang sesuai. Jika sistem yang digunakan tidak mendukung ACL dan *auditing*, disarankan untuk menggunakan *firewall* atau *proxy software* yang dapat mencegah upaya serangan oleh para *hacker*. Ketiga teknik tersebut berguna untuk menelusuri upaya penyerangan terhadap sistem.

Seberapa jauh pengamanan yang dibutuhkan untuk sistem komputer

Pengamanan yang terlalu ketat akan mengakibatkan penurunan kinerja, dan *log* akan menjadi terlalu penuh dengan data yang tidak dibutuhkan. Dibutuhkan *logging* yang ada pada level yang tepat. Pertama-tama, kemampuan *logging* dan *auditing* dari suatu sistem operasi perlu dipahami. Yang perlu diketahui adalah:

1. Siapa yang mengakses sistem (*logging on to the system*)
2. Siapa yang mencoba untuk mengubah *setting* pengamanan
3. Apa yang diakses pada sistem

Penyerangan dan Penetrasi

Sulit sekali untuk mengetahui apakah suatu sistem sedang dalam penyerangan. Namun sekarang tersedia berbagai macam alat yang berupa *personal firewall* yang dapat digunakan pada suatu sistem komputer. Alat-alat tersebut dapat memberi pemberitahuan kepada pengguna jika sistem sedang dalam penyerangan.

Untuk mengetahui kejadian abnormal terhadap sistem, perlu diketahui keadaan normal dari sistem. Juga perlu diketahui kinerja dari jaringan sistem, serta *disk drive* dan CPU. Berikut adalah beberapa tanda yang mengindikasikan bahwa ada *hacker* yang mencoba untuk mengakses sistem:

- Penggunaan sumber daya sistem yang abnormal: jika sistem tiba-tiba menjadi lambat, atau ditemui aplikasi yang tidak pernah muncul sebelumnya, hal ini dapat mengindikasikan bahwa ada *hacker* yang sedang mencoba mengakses sistem, atau ada *Trojan horse* pada sistem
- Upaya koneksi terhadap jaringan: jika sistem mencoba untuk mengakses Internet pada waktu yang seharusnya tidak terjadi, kemungkinan terdapat *intruder* pada sistem
- Ditemui *files* yang biasanya tidak ada: *files* aneh, atau munculnya program yang tidak diinginkan memberi indikasi adanya upaya pengaksesan sistem secara tidak sah.
- Perubahan atau penghilangan *files* atau *folders*: jika ditemui *files* atau *folder* yang berubah nama, dipindahkan atau diubah tanpa sepengetahuan pengguna, ini dapat mengindikasikan adanya pengaksesan oleh pihak-pihak yang tidak berwenang.

Social Engineering

Kasus penipuan dimana suatu pihak mempergunakan pihak lain untuk mencapai keuntungan yang berkaitan dengan sistem komputer sering dijuluki '*social engineering*'. Contoh kasus yang sering terjadi adalah seorang administrator sistem memberi *username* dan *password* Administrator sistem kepada orang yang mengaku sebagai orang yang berwenang. Contoh lain adalah kasus penyebaran *worm* melalui *e-mail*.

Tanda-tanda penyerangan melalui *Social Engineering*

- *False sense of urgency*: berpura-pura untuk memerlukan informasi dengan terburu-buru, sehingga korban tidak sempat berpikir ketika memberi informasi yang seharusnya tidak diberikan
- *Too good to be true*: penawaran yang terlalu baik, yang akan mempengaruhi orang untuk melakukan sesuatu yang seharusnya tidak ia lakukan.
- Mengambil keuntungan dari orang-orang yang dipercaya: mendapatkan akses terhadap sistem melalui orang-orang dalam usaha kecil dan menengah.
- Verifikasi yang kurang lengkap atau tidak lengkap: pihak penipu tidak dapat memberi verifikasi atau identitas yang benar.

Virus, Trojan Horses & Penipuan (Hoaxes)

Virus Komputer dan Trojan Horses

Berikut adalah beberapa definisi yang berkaitan dengan virus komputer dan *Trojan Horses*:

- **Virus Komputer**: Suatu kode piranti lunak yang sulit untuk dideteksi, yang dirancang untuk *self-replicate* (membuat replika dari dirinya ‘berkembang-biak’) dan dapat melakukan sesuatu yang destruktif (mengganggu maupun merusak) terhadap suatu sistem komputer, juga bisa menjadi *polymorphic*
- *Stealth, Stealthy*: Memiliki kemampuan untuk menyembunyikan diri dari pendeteksian
- *Self-replication*: Kemampuan untuk membuat salinan dari dirinya sendiri, dan mengganggu *file* lain pada sistem
- *Payload*: Kode yang membuat virus melakukan sesuatu, bisa jadi melakukan sederhana, seperti menampilkan suatu pesan, ataupun menghapus seluruh *hard drive*.
- *Polymorphic*: Kemampuan virus untuk mengubah diri selama virus tersebut (menginfeksi) mengganggu berbagai *file* yang ada pada sistem. Hal ini membuat virus tersembunyi dari pendeteksian.
- *Infection (infeksi)*: Ketika virus menjadi aktif pada sistem atau *file*
- *Trojan Horse*: Piranti lunak yang membawa kode yang tidak dikenal, dan tidak untuk tujuan yang sebenarnya. Biasanya digunakan untuk menembus pengamanan dari suatu sistem atau untuk melakukan instalasi piranti lunak tanpa diketahui oleh penggunanya
- *Worm*: Kode piranti lunak yang di-desain untuk menyebar secara otomatis dari satu sistem ke sistem lain, biasanya tanpa diketahui oleh penggunanya
- **Sistem yang bersih**: Sistem yang tidak memiliki virus pada *file* atau *memory*-nya
- *“In the wild”*: Digunakan untuk menjuluki virus yang dilaporkan muncul pada sistem yang digunakan di rumah atau bisnis.

Virus komputer seringkali digambarkan dengan menggunakan istilah yang mirip dengan istilah yang berkaitan dengan virus yang menginfeksi manusia. Keduanya

memiliki kesamaan, yaitu kemampuan untuk membuat salinan dari dirinya sendiri ('berkembang-biak'), dan melakukan sesuatu yang destruktif. Juga mirip dengan virus yang menginfeksi manusia, 'penyembuhan' dari suatu virus dapat lebih mudah diketahui jika terdapat beberapa obyek (sistem) yang terkena virus tersebut.

Namun, virus komputer juga memiliki perbedaan dengan virus yang menginfeksi manusia, dimana virus komputer biasanya baru bisa aktif jika pengguna komputer melakukan sesuatu terhadap virus tersebut. Pengaktifan virus dapat dilakukan dengan membaca atau membuka *file* yang telah terinfeksi dengan suatu virus, atau dengan mengakses suatu situs web. Berikut adalah beberapa tipe infeksi yang dapat terjadi pada suatu sistem:

- *Master Boot Record (MBR)*: Virus yang di-desain untuk menginfeksi *Master Boot Record* atau *Boot Sector* dari disk, sehingga ketika disk digunakan, virus akan berpindah ke *memory*
- *File Infector*: Virus yang di-desain untuk menginfeksi suatu *file*. Virus diaktifkan pada saat *file* dibuka atau dijalankan
- *Virus Macro*: Virus yang ditulis dalam bahasa *macro* dan bergantung pada program tertentu atau sistem operasi. Contoh yang paling umum adalah virus *macro* dari Microsoft Word
- *Virus e-mail / worm*: Biasanya tipe khusus dari virus *macro* yang menjalankan aktivitas *script* pada program *e-mail*. Beberapa virus *e-mail / worm* yang terkenal adalah virus 'I love you', 'Code Red' dan 'I love you'.

Pengaruh Virus terhadap Sistem Komputer yang digunakan pada UKM

Orang mendistribusikan virus dengan alasannya masing-masing, dari suatu eksperimen yang sederhana (yang mungkin tidak disengaja) sampai suatu espionase bertaraf internasional. Banyak virus yang tidak berbahaya dan mudah dikendalikan, namun banyak juga yang berdampak fatal. Masalah terbesar dari virus komputer ialah sifat 'indiskriminatif'-nya, yang menyerang dapat menyerang siapa saja.

Jika sistem komputer yang digunakan tidak diberi pengamanan, pada suatu saat sistem tersebut akan menjadi korban dari virus-virus tersebut. Oleh karena itu adalah sangat penting untuk melakukan kedua langkah berikut: menggandakan data secara reguler (*back-up*) dan melakukan instalasi *antivirus software* pada sistem. Kemudian juga perlu dilakukan *update* terhadap *software* tersebut secara terus-menerus. Tersedia berbagai macam *antivirus software* yang mudah digunakan, membutuhkan memori yang kecil, dan menyediakan pilihan untuk melakukan *update* secara terus menerus.

Melindungi sistem dari ancaman-ancaman

Walaupun ancaman dari virus dan *trojan* terus menerus berubah, melindungi terhadap keduanya tidak terlalu sulit. Berikut adalah beberapa cara:

- Gunakan *antivirus software*
- Jangan membuka *file* atau menjalankan program dari sumber-sumber yang tidak dikenal. *E-mail* juga dapat berisi virus dan *Trojan*
- Baca *e-mail* dalam *plain text*. HTML memungkinkan *scripting* yang dapat digunakan untuk mengumpulkan data dari sistem atau mentransfer kode *Trojan* pada sistem

- *Download software* hanya dari sumber yang terpercaya, *software* dari sumber yang tidak dikenal dapat dengan mudah diubah dengan kode *Trojan Horse*
- *Upgrade browser* versi terbaru dan *software Office Suite*.
- Non-aktifkan *Windows Scripting Host* jika tidak diperlukan. *Windows Scripting Host* adalah suatu program yang dapat menjalankan *script* yang ditulis dalam beberapa bahasa pemrograman pada sistem Windows.
- Lakukan penggandaan data (*back up*) secara reguler.
- Sediakan *boot disk* yang bersih dengan *software antivirus* pada disk tersebut.

Antivirus Software

Tersedia berbagai perlindungan *antivirus*, dan banyak vendor *software* yang mencoba untuk menyediakan suatu paket *tool* untuk mencegah, mendeteksi, dan membersihkan virus dan *Trojan*, dan juga cara-cara untuk memperbaharui *tool* tersebut tersebut dengan informasi yang terbaru. Berikut adalah beberapa fungsi yang dilakukan oleh paket *tool* tersebut:

- Deteksi virus: Merupakan inti dari semua paket *antivirus*. *Software* ini melakukan inspeksi pada *hard drive* untuk mencari *file* yang mungkin terinfeksi, dengan memberi peringatan dan laporan atau membersihkan virus selama program dijalankan. Disarankan untuk melakukan *scan* untuk virus terhadap sistem sedikitnya satu kali seminggu.
- Membersihkan virus: Program ini berfungsi untuk membersihkan virus dari sistem.
- Deteksi *Trojan Horse*: Mirip dengan deteksi virus, namun mendeteksi *Trojan Horse*.
- Memperbaharui definisi virus: Mengambil file-file definisi virus yang terbaru mengenai virus dan *Trojan Horses* yang terdapat pada memori, pada file, atau pada *e-mail* dan *attachments*.

Cara penggunaan *software antivirus* tergantung terhadap vendor *antivirus* yang dipilih. Namun, berikut adalah beberapa aturan yang dapat membantu untuk menjalankan *antivirus* dengan lebih lancar:

1. Pilih *software antivirus* dari vendor yang dapat memberi jaminan perlindungan dan dukungan jangka panjang
2. Atur *setting* dari *software* tersebut untuk secara otomatis melakukan *scan* pada sistem dan mengambil definisi virus yang terbaru
3. Disarankan tidak menjalankan aplikasi lain saat *scan* dilakukan

Penipuan (*Hoax*) dan dampaknya

Contoh *Hoax* yang sering tersebar adalah suatu *e-mail* yang isinya menceritakan ancaman dari virus dan memberi instruksi untuk memberi tahu orang lain mengenai ancaman tersebut. Jika *e-mail* tersebut berasal dari sumber yang tidak dikenal dan dipercaya, kemungkinan besar pesan pada *e-mail* tersebut adalah *Hoax*.

Active Content pada Web

Active Content digunakan dengan tujuan untuk memberi pengalaman yang lebih menarik bagi pengguna Internet ketika mengakses suatu situs yang memiliki *active content*. Namun, *active content* juga seringkali disalah gunakan oleh *hacker* untuk mendapatkan akses ke suatu sistem komputer. *Active content* dapat saja di-*block*, tetapi jika di-*block*, pengguna akan kehilangan layanan tambahan yang telah diprogram pada situs tertentu yang dapat memudahkan pengguna.

Yang dapat dilakukan adalah mengatur *browser* untuk dapat mengatur level akses dari program, berdasarkan 'zona'-nya. Sebaiknya tidak mengakses Internet pada saat menggunakan *account* Administrator, karena jika suatu situs web mencoba untuk melakukan sesuatu terhadap sistem, situs web tersebut akan menggunakan dengan *access permission* penggunanya. Oleh karena itu, gunakan *account* dengan akses minimal ketika menelusuri Internet.

4.4. Implementasi kebijakan keamanan sistem informasi pada UKM

Dalam keamanan komputer dan sistem informasi dikenal konsep keamanan berlapis (*layered security*) atau keamanan yang mendalam (*security in-depth*). Dalam istilah sederhananya, setiap ukuran keamanan yang dirancang manajer usaha kecil dan menengah untuk menjaga keamanan komputer dan sistem informasi usaha kecil dan menengah pada akhirnya dapat dibobol atau ditembus, sehingga untuk mendapatkan tingkat keamanan komputer dan sistem informasi yang berlapis. Konsep ini juga menjamin adanya perubahan dan perkembangan teknik dan teknologi keamanan komputer dan sistem informasi, kelemahan baru di suatu faktor keamanan komputer dan sistem informasi tidak akan mempengaruhi keseluruhan sistem.

Saat konsep keamanan berlapis diterapkan pada keamanan komputer dan sistem informasi usaha kecil dan menengah, konsep tersebut harus diakui nyaris terlalu berlebihan. Seberapa tangguh seharusnya keamanan komputer dan sistem informasi usaha kecil dan menengah? Dalam bagian ini akan diberikan contoh menerapkan konsep keamanan berlapis pada keamanan komputer dan sistem informasi usaha kecil dan menengah dan melihat apa yang terjadi jika keamanan komputer dan sistem informasi usaha kecil dan menengah ditembus.

Beberapa tahun silam kelompok *hacker* Jerman sukses mengetahui enkripsi data finansial program Quicken. Kelompok tersebut juga berhasil mengetahui file-file mana saja yang digunakan program untuk menyimpan informasi pembukuan akutansi dan data finansial seperti saldo bank, pembayaran tagihan dan sebagainya. Memanfaatkan informasi ini, kelompok ini sukses menemukan komputer-komputer yang tidak memiliki keamanan yang menggunakan fitur-fitur *online* program Quicken dan menyerang komputer-komputer untuk mendapatkan file-file dari sistem sasaran. Dengan cara ini kelompok tersebut mendapatkan nomor rekening bank dan saldo beberapa rekening. Berita baik dari kejadian ini adalah orang-orang tersebut tidak tergiur untuk mencuri rekening atau uang, tetapi menggunakan aktifitas ini untuk menunjukkan betapa tidak amannya program akutansi tersebut dan praktek komputasi saat itu. Yang penting diperhatikan bahwa pembuat Quicken yakni Intuit memberikan respon yang cepat dan memperbaiki program dan fitur online sehingga eksploitasi ini tidak dapat dilakukan lagi. Di lain pihak pengguna komputer pada usaha kecil dan

menengah tidak mengetahui bagaimana memperbaiki keamanan sistem informasi mereka atau tidak mengetahui apa yang pengguna komputer pada usaha kecil dan menengah itu perlukan, sehingga celah-celah keamanan tersebut masih ada dalam beberapa sistem hingga *patch* tersedia. Jika usaha kecil dan menengah anda menggunakan Quicken saat ini, janganlah khawatir – Intuit telah memperbaiki celah ini sejak lama. Pengguna hanya akan terekspos jika menggunakan versi 10 tahun silam (yang mungkin tidak digunakan sekarang ini).

Seperti yang pembaca dapat ketahui, kurang baiknya keamanan komputer dan sistem informasi memberikan konsekuensi. Mari perhatikan bagaimana keamanan mendalam membantu situasi dalam kasus Quicken. Pertama, program Quicken memiliki enkripsi dan pengalihan penyimpanan untuk memberikan keamanan. Pengalihan penyimpanan bukanlah keamanan yang sesungguhnya – artinya data tersembunyi atau ditempatkan di tempat yang tidak semestinya, yang hanya menghentikan *hacker* yang sungguh-sungguh pemula. Jika *hacker* tidak memiliki akses ke file-file yang menyimpan data kritis (file-file itu dapat disimpan di server atau data dapat diminta tiap kali saat dipakai), *hacker* tidak pernah dapat menjebol skema enkripsi. Enkripsi yang digunakan Quicken saat terjadi pembobolan tidak terlalu kuat, namun mungkin saat kuat sewaktu program dituliskan menggunakan enkripsi tersebut. Seiring perjalanan waktu dan revolusi PC berlanjut, komputer yang rata-rata digunakan pengguna menjadi semakin kuat secara signifikan dan waktu yang diperlukan untuk membongkar enkripsi semakin sedikit. Satu tingkat keamanan komputer-*patch* keamanan komputer-belum tersedia kala itu atau diterapkan untuk memperbaiki kebutuhan enkripsi yang lebih kuat seiring berjalannya waktu. Jika enkripsi saat itu dibuat lebih sulit untuk dibongkar atau diperbahai lebih sering, *hacker* mungkin tidak dapat membongkar enkripsi dan permasalahan keamanan program tersebut dapat dihindari. Setelah membongkar enkripsi, *hacker* perlu mengumpulkan *file-file*, jadi *hacker* membuat halaman *web* dengan pemrograman khusus yang mengumpulkan *file-file* yang kelompok *hacker* tersebut butuhkan dari halaman *web* pada mesin pengguna. Jika komputer milik pengguna diamankan dengan baik oleh *vendor* atau pengguna itu sendiri, *hacker* dapat ditolak mengakses *file* pada mesin pengguna dan tidak pernah memiliki kesempatan untuk menjebol *file-file* tersebut, bahkan kalau *hacker* mampu membongkar enkripsi.

Seperti yang pembaca dapat ketahui dari analisis yang sangat sederhana ini, *hacker* harus menembus 3 lapis keamanan untuk mendapatkan informasi yang *hacker* inginkan. Lapisan pertama, *hacker* membongkar enkripsi; lapisan kedua, *hacker* menemukan dimana data sensitif disimpan; dan lapisan ketiga, *hacker* mendapatkan akses ke sistem pengguna untuk mendapatkan file yang *hacker* inginkan. Yang menakjubkan adalah bahwa *hacker* sukses melakukannya. Jika salah satu lapisan tersebut ditutup, *hacker* mungkin gagal. Atau jika *hacker* terus berupaya, *hacker* mungkin dapat menemukan celah keamanan lainnya dan mampu menempus keamanan tersebut.

Grant All versus Deny All

Agar memperbolehkan hak akses pengguna mengerjakan fasilitas komputasi di sistem komputer usaha kecil dan menengah, terdapat 2 model umum yang sering digunakan. Model pertama adalah *Grant All*, *Deny Explicit* yakni mengizinkan semua akses dan menolak akses tertentu, dan model lainnya adalah *Deny All*, *Grant Explicit* yakni menolak semua akses dan mengizinkan akses tertentu. Seperti yang pembaca dapat tebak dari uraian istilahnya, model akses tersebut berlawanan akhiran spektrum yang sama untuk mengizinkan akses. *Grant All*, *Deny Explicit* merupakan akses yang

mengizinkan semua pengguna untuk memiliki semua akses pada awalnya dan menolak akses tertentu pada pengguna yang telah diketahui. *Deny All, Grant Explicit* mengambil pendekatan yang berbeda, yakni administrator menolak hak akses semua pengguna kecuali pengguna tertentu yang diizinkan memiliki akses terbatas. Model kedua, *Deny All, Grant Explicit*, umumnya digunakan secara luas untuk sistem informasi yang membutuhkan keamanan yang tinggi, namun bagaimana menerapkan model keamanan ini pada pengguna komputer di sistem informasi yang dimanfaatkan usaha kecil menengah? Ingatlah bahwa keputusan ini didasarkan seluruhnya pada dua faktor: resiko sistem yang terekspos dan bagaimana penggunaan dan melakukan manajemen seperti yang diinginkan oleh administrator komputer dan sistem informasi usaha kecil dan menengah. Sistem informasi yang lebih aman umumnya membutuhkan kerja yang lebih berat untuk memanajemen dan merawatnya. Manajer usaha kecil dan menengah harus memasukan faktor upaya manajemen dan perawatan tersebut dalam keputusan keamanan komputer dan sistem informasi usaha kecil dan menengah, karena manajer harus menghindari situasi mengamankan komputer dan sistem informasi pada posisi yang tidak dapat digunakan atau dilakukan manajemen.

Pada model *Grant All*, semua pengguna komputer memiliki hak untuk melakukan semua kegiatan komputasi kecuali administrator komputer dan sistem informasi menolak hak-hal tertentu. Model ini memberikan resiko karena setiap celah keamanan dan *exposure* yang tidak diketahui administrator komputer usaha kecil dan menengah tidak dilindungi dan dengan demikian kelauman-kelemahan keamanan akan tetap ada hingga administrator komputer usaha kecil dan menengah sadar akan kelemahan yang sebelumnya tidak disadari itu dan memperbaikinya. Walaupun kelemahan yang diberikan model keamanan *Grant All*, model keamanan *Grant All* merupakan sistem yang memberikan lebih banyak fungsionalitas penggunaan dan memberikan lebih sedikit upaya perawatan pengaturan keamanan komputer dan sistem informasi. Administrator komputer dan sistem informasi usaha kecil dan menengah juga tidak perlu tahu dalam upaya perencanaan keamanan bagaimana pengguna komputer pada usaha kecil dan menengah tersebut akan memanfaatkan sistem. Secara standar, pengguna komputer dalam sistem informasi usaha kecil dan menengah dapat memanfaatkan fasilitas komputasi apa saja yang diinginkan pengguna komputer tersebut, namun hal ini dapat memicu bencana. Pengguna komputer pada sistem informasi usaha kecil dan menengah dapat melakukan kegiatan komputasi apa saja yang tidak diantisipasi administrator komputer dan sistem informasi usaha kecil dan menengah, termasuk tindakan secara sengaja atau kecelakan yang mengubah data atau pengaturan sistem, perubahan pengaturan aplikasi dan mengakses kebanyakan *file* yang ada pada sistem komputer di usaha kecil dan menengah, termasuk *file-file* yang digunakan oleh sistem operasi komputer. Biasanya hal ini bukanlah termasuk masalah besar. Pengguna komputer pada usaha kecil dan menengah umumnya tidak memiliki niat secara sengaja mengubah atau menghancurkan data yang pengguna komputer tersebut kerjakan; namun mereka dapat secara tidak sengaja melakukan perubahan dan perusakan data tersebut-bahkan tanpa menyadari atau juga dengan sengaja karena memiliki niat yang tidak baik. Dengan membatasi beberapa hak akses ke *file* sistem dan data penting, administrator komputer usaha kecil dan menengah dapat melindungi *file-file* penting sehingga tidak dapat diubah oleh pihak yang tidak memiliki wewenang untuk mengakses *file-file* tersebut.

Sebaliknya model *Deny All* mengasumsikan hanya aktifitas dipilih yang diberikan hak aksesnya oleh sistem dan menolak akses semua aktifitas lainnya. Model ini digunakan untuk sistem dengan tingkat keamanan tinggi karena administrator komputer dan sistem informasi usaha kecil dan menengah tahu dengan tepat apa hak

penggunaan fasilitas komputasi apa yang dapat diberikan dan apa yang tidak dapat diberikan. Administrator komputer dan sistem informasi usaha kecil dan menengah dapat mengasumsikan hal-hal yang administrator komputer dan sistem informasi tersebut tidak ketahui atau tidak memprediksikan akses yang tidak ditolak yang berarti akses tersebut tidak dilindungi. Kebenaran yang terjadi adalah beberapa hal dapat menjadi masalah, tetapi umumnya model keamanan ini bekerja dengan semestinya. Kesulitan terbesar memanfaatkan model keamanan *Deny All* ini adalah besarnya beban pekerjaan administratif komputer dan sistem informasi yang diperlukan untuk merawat tingkat keamanan komputer dan sistem informasi yang demikian tinggi tersebut. Administrator komputer dan sistem informasi harus terus memperbaharui *patch*, *service pack* sistem operasi, aplikasi dan pengembangan keamanan komputer dan sistem informasi. Kembali penulis ungkapkan bahwa keputusan memilih model keamanan yang tepat antara *Grant All* atau *Deny All* untuk komputer dan sistem informasi usaha kecil dan menengah tergantung dari waktu dan upaya yang manajer usaha kecil dan menengah tepat untuk tingkat keamanan komputer dan sistem informasi yang diperlukan sistem informasi usaha kecil dan menengah.

Mari lihat contoh dari daftar resiko keamanan komputer dan sistem informasi pada bab 1 untuk memperjelas gagasan konsep model keamanan komputer ini. Asumsikan perangkat lunak *internet banking* yang digunakan usaha kecil dan menengah menyimpan data yang dipergunakannya pada *hard disk* komputer yang dimanfaatkan usaha kecil dan menengah-bukan terdiri dari informasi rekening tetapi informasi tertentu bagi perangkat lunak *internet banking* tersebut yang memberikan fasilitas pembayaran tagihan secara *online*. Dalam kasus umum, komputer tempat terdapatnya perangkat lunak *internet banking* tersebut dapat diakses dari komputer lainnya menggunakan LAN. Dengan menerapkan model keamanan komputer *Grant All*, administrator secara eksplisit menolak hak mengubah atau menghapus data tersimpan untuk pengguna komputer yang tidak seharusnya melakukan aktifitas mengubah atau menghapus data dari perangkat lunak *internet banking* tersebut. Dengan asumsi awal bahwa petugas pembukuan dapat mengubah dan mengakses data untuk perangkat lunak *internet banking* dan pegawai lainnya tidak dapat mengubah dan mengakses data untuk perangkat lunak *internet banking*. Bila resiko kesalahan manusia administrator komputer usaha kecil dan menengah meningkat karena setiap orang yang menggunakan komputer dapat mengubah dan menghapus data secara ceroboh karena tidak mengetahui pentingnya data tersebut. Dalam model keamanan komputer *Deny All*, tidak seorang pun dapat mengubah atau menghapus data yang tersimpan itu karena hak akses akan melarang aktifitas mengubah atau menghapus kecuali administrator komputer dan sistem informasi usaha kecil dan menengah secara khusus memberikan hak akses tersebut pada pengguna komputer tertentu. Demikian bila administrator menghilangkan hak akses *file* atau *directory* atau menolak akses dari setiap orang, perubahan hak akses juga berpengaruh pada administrator dan administrator juga tidak dapat mengakses data tersebut. Salah satu gagasan yang baik adalah memberikan hak akses kepada administrator komputer dan pemilik data sehingga bagi administrator komputer dapat memperbaiki kesalahan yang dibuat saat mengatur kembali hak akses dan bagi pemilik data untuk mengubah data sesuai kewenangannya.

Enskripsi atau Tidak Menggunakan Enskripsi

Enskripsi dapat dijelaskan secara sederhana sebagai pengkodean atau mengkaburkan data sehingga hanya penerima yang diinginkan atau pemilik informasi

tertentu saja yang dapat membaca data tersebut. Praktek enkripsi agak sulit dijelaskan dengan gamblang karena membutuhkan pengetahuan matematika tertentu yang mudah dilakukan satu arah tetapi tidak mudah untuk membalikkan operasi tersebut dan dengan menggunakan sifat tertentu dari operasi tersebut pengguna enkripsi dapat melakukan enkripsi dan mengembalikan enkripsi itu kemudian. Konsep enkripsi terasa sedikit rumit, jadi akan diberikan contoh yang sederhana. Melakukan operasi kuadrat suatu bilangan merupakan operasi yang banyak orang anggap lumayan mudah, tetapi melakukan operasi akar kuadrat suatu bilangan dianggap rumit. Kebanyakan orang dapat mencari nilai purata kuadrat hanya pada bilangan tertentu, dengan tanpa menggunakan komputer dan kalkulator, tetapi kelompok orang yang sama akan merasa kesulitan mencari nilai purata kuadrat bilangan-bilangan lainnya.

Saat membicarakan soal enkripsi, satu pertanyaan yang muncul adalah seberapa kekuatan enkripsi yang cukup. Jawaban pertanyaan tersebut tidak mudah. Cukup kuat untuk keperluan atau hal apa? Cara memandang yang lebih baik adalah melihat kekuatan enkripsi dengan melihat data apa yang pengguna komputer hendak lindungi. Apakah umur data (didefinisikan sebagai panjangnya waktu data berguna atau bermanfaat) secara nyata lebih pendek ketimbang waktu untuk membongkar enkripsi yang melindunginya, maka enkripsi yang melindungi data tersebut cukup kuat. Jika umur data lebih panjang dari waktu untuk membongkar enkripsi yang melindungi data tersebut, enkripsi yang melindungi data tersebut belum cukup kuat. Kekuatan enkripsi dinyatakan dengan banyaknya bit kunci enkripsi. Standar kekuatan kunci enkripsi yang diterima saat ini berkisar 128-256 bit. Hal ini berarti berbagai industri dan instalasi pemerintahan menentukan 128-256 bit "cukup" kuat untuk keperluan keamanan komputer mereka serta industri dan instalasi pemerintahan mengusulkan jumlah bit kunci enkripsi ini pada pihak lainnya. Kekuatan enkripsi diperoleh dari dua faktor utama, algoritma yang dipergunakan (seperti RSA, BlowFish, DES, 3DES) dan panjangnya kunci. Algoritma merupakan operasi matematika kompleks untuk melakukan enkripsi dan kekuatan kunci adalah kekuatan pengacakan data. Kunci enkripsi yang amat panjang pada algoritma yang lemah mungkin tidak memberikan keamanan data lebih baik dari pada kunci enkripsi yang pendek pada algoritma yang lebih baik. Kebanyakan komunikasi *Secure Socket Layer* (SSL) yang digunakan browser *Web* memiliki panjang kunci enkripsi 128 atau 256 bit, tergantung versi browser yang digunakan.

Menentukan Hak Akses

Kebanyakan sistem informasi bagi usaha kecil dan menengah dibangun dengan asumsi tidak terdapat keamanan komputer yang akan diterapkan. Kebutuhan tersebut cukup hingga kemajuan teknologi jaringan umumnya dan internet pada khususnya dan peningkatan penggunaan koneksi yang terus tersambung seperti xDSL dan model kabel. Koneksi ke internet yang selalu tersambungkan ini berarti komputer dapat diketahui dengan mudah oleh hacker, karena keberadaan komputer relatif lebih mudah diprediksi dan alamat IP yang stabil-yang berarti baik alamat IP yang statis atau bentuk pool kecil alamat yang berdekatan. Jika alamat IP koneksi komputer pengguna ke internet statis, komputer tersebut cukup ditemukan satu kali saja; jika alamat IP koneksi komputer pengguna ke internet diberikan secara dinamis, *hacker* harus mencari tiap kali ingin mengetahui lokasi komputer tersebut tetapi sering kali pencarian tersebut hanya pada sejumlah kecil alamat dari koleksi alamat yang telah diketahui. Begitu sebuah komputer telah ditemukan alamatnya, *cracker* atau *hacker* dapat mulai mencari informasi atau menyerang komputer pengguna tersebut. Hal

inilah yang menjelaskan mengapa saat pengguna komputer lebih sering terhubung ke internet, kebutuhan keamanan pengguna komputer tersebut juga meningkat.

Satu cara utama untuk memperoleh keamanan komputer adalah mengizinkan atau membatasi akses ke *file* atau *directory* atau sumber daya komputasi yang dipergunakan pengguna komputer pada suatu komputer. Dengan pembatasan akses tersebut, administrator komputer dapat mengetahui siapa yang atau yang tidak melakukan suatu aktifitas pada sistem yang diaturnya. Hal yang lebih penting, administrator dapat mengendalikan siapa saja yang melakukan aktifitas tertentu. Konsep ini dikenal dengan *Access Control*. Istilah hak pengguna komputer dan *privilege* pengguna komputer menunjukkan siapa yang diizinkan melakukan aktifitas tertentu. Hak dan *privilege* mendefinisikan apa yang pengguna dapat dan tidak dapat lakukan, lihat, tulis atau hapus.

Akses *file* atau *directory* dikendalikan melalui penggunaan *Access Control List* (ACL). ACL pada dasarnya berupa daftar nama pengguna yang diberikan hak mengakses *file* atau *directory* dan daftar hak yang diberikan atau dilarang. ACL tersimpan di *file system*. Saat pengguna komputer perlu melakukan akses, ACL diperiksa untuk menentukan apakah terdapat hak yang tepat sebelum akses diberikan pada pengguna komputer.

Backup Data

Data komputer yang dimiliki usaha kecil dan menengah tidak benar-benar aman jika telah melakukan semua pengamanan logika yang ada tetapi terjadi kegagalan fungsi *hard disk* dan tidak tersedianya *backup* atau cadangan. Jika manajer usaha kecil dan menengah memiliki data yang dianggap penting atau kritis, manajer perlu melakukan beberapa aktifitas *backup*. Cadangan tersebut tidak mesti mewah, tetapi haruslah berupa cadangan yang melindungi usaha kecil dan menengah dalam kasus kegagalan perangkat keras atau kerusakan data. Umumnya media yang digunakan untuk membuat cadangan data adalah media penyimpanan *removable* seperti *tape drive*, *removable disk* atau media optikal seperti cd atau dvd dan pengguna komputer menjadwalkan cadangan setiap malam atau setiap minggu. Jika data yang dimiliki bersifat kritis seperti data finansial usaha kecil dan menengah, manajer harus mempertimbangkan memiliki penyimpanan terpisah untuk menyimpan cadangan penuh atau bila memungkinkan manajer usaha kecil dan menengah harus selalu memiliki data terbaru pada media penyimpanan yang berada terpisah tersebut. Untuk menjaga selalu memiliki data terkini, administrator dapat merotasi *tape* atau media penyimpanan lainnya setiap minggunya. Lakukan *backup* total saat hari terakhir bekerja pada satu minggu, yakni jumat atau sabtu, dan tinggalkan *tape* atau media penyimpanan lainnya di kantor, ambil cadangan *tape* atau media penyimpanan minggu lalu ke tempat penyimpanan terpisah dan ambil *tape* atau media penyimpanan dari tempat penyimpanan terpisah untuk digunakan saat melakukan *backup* berikutnya. Menggunakan cara ini maka proses membuat cadangan data untuk usaha kecil dan menengah tidak berusia lebih dari seminggu. Jika diperlukan untuk memiliki periode cadangan data yang lebih singkat, cukup rotasikan dengan frekuensi lebih sering. Terdapat banyak metode *backup* yang dapat digunakan, namun untuk usaha kecil dan menengah kesederhanaan dan kejelasan rutinitas *backup* harus dipertahankan untuk menjamin terdapat proses *backup* pada periode yang direncanakan misalnya seminggu sekali.

5. Kesimpulan dan Saran

5.1. Kesimpulan

5.1.1. Tingkat kesadaran pentingnya keamanan sistem informasi pada UKM

Inti dari tulisan ini adalah bagaimana kesadaran merupakan titik awal upaya melakukan manajemen keamanan komputer usaha kecil dan menengah. Kesadaran selanjutnya adalah menyadari resiko ancaman keamanan komputer usaha kecil dan menengah. Akhirnya upaya aktif untuk melakukan kegiatan keamanan komputer dapat dilakukan usaha kecil dan menengah.

Dengan memahami kesadaran, manajer usaha kecil dan menengah mencoba mengklasifikasikan tingkat keamanan komputer usaha kecil dan menengah dengan menanyakan makna pentingnya data bagi proses bisnis usaha kecil dan menengah. Sedangkan resiko keamanan komputer usaha kecil dan menengah dapat diketahui dengan apakah mudah memperoleh kembali data bila data tersebut mendadak hilang atau rusak.

Akhirnya beberapa tindakan aktif dapat dilakukan dengan dasar pemahaman pentingnya keamanan komputer usaha kecil dan menengah, antara lain membuat cadangan data atau melakukan instalasi perangkat lunak antivirus.

5.2. Saran

5.2.1. Pelatihan keamanan sistem informasi pada UKM

Untuk terus memahami perkembangan keamanan komputer tentu manajer dan administrator usaha kecil dan menengah harus terus mengembangkan pengetahuan mereka. Secara umum upaya mengembangkan pengetahuan dan keterampilan keamanan komputer dapat diperoleh:

- Secara informal, misalnya membaca majalah yang berkaitan dengan keamanan komputer atau mengikuti forum-forum di internet atau komunitas yang memperhatikan masalah-masalah keamanan komputer.
- Secara formal, misalnya dalam pelatihan kerja karyawan baru, konsultasi keamanan komputer pada pakarnya, mengikuti pelatihan yang diadakan instansi yang berkaitan maupun berbagai kegiatan lainnya

Daftar Pustaka

Gregg, M. and David Kim, "Inside Network Security Assessment: Guarding your IT Infrastructure", Sams, 2005.

Krutz, R.L and Russel D. Vines, "The CISSP® Prep Guide: Gold Edition", John Wiley Publishing, Inc., 2003.

Shea, B., "Have You Locked the Castle Gate?: Home and Small Business Computer Security", Pearson, 2002.

Turban, E., D. King, J. Lee, D. Viehland, "Electronic Commerce 2004, A Managerial Perspective", Pearson Prentice Hall New Jersey, 2004.

Young, S. and Dave Aitel, "The Hacker's Handbook", Auerbach Publications, 2004.