OPERATIONS SECURITY

IKI-83408T

Proteksi dan Teknik Keamanan Sistem Informasi
Kelompok 127
Bab 6
USAHA KECIL DAN MENENGAH – Klinik Kesehatan Sehat Bahagia

Disusun oleh :

7204000446 - Argabudhy Sasrawiguna
7204000594 - Rio Ricardo
720400056x - Nugroho Gito Prasojo
7204000543 - Muhamad Rachmadi

UNIVERSITAS INDONESIA
MAGISTER TEKNOLOGI INFORMASI
FAKULTAS ILMU KOMPUTER
2005

DAFTAR ISI

I. PENDAHULUAN

1.1. Latar Belakang

Setiap hari pelanggan dan bisnis di seluruh dunia mendapatkan keuntungan dari penggunaan komputer, pelayanan dan transaksi melalui web dan itu semua dasarnya adalah *data center*. *Data center* membuat proses komputer, penyimpan data dan alat-alat jaringan melakukan tugas lebih cepat mudah dan akurat. Pertumbuhan dari internet telah membuat teknologi informasi merupakan bagian dari kehidupan kita, dan organisasi terus berusaha untuk meningkatkan *data center* mereka untuk memenuhi kebutuhan yang terus bertambah.

Salah satu aspek yang paling harus dijaga dari suatu *data center* dengan optimal adalah tren yang ada dalam dunia perbankan saat ini, secara konservatif diperkirakan bahwa 60% dari pelanggan sekarang membuat pembayaran tagihan secara otomatis. Bank tidak hanya harus meningkatkan kapasitas komputer untuk menghadapai transaksi, tetapi mereka juga harus mengkuti standar dari pemerintah dalam penggunaan teknologi informasi. Oleh karena itu dibutuhkan suatu pengukuran juga untuk menjamin kemanan informasi dan kelanjutan bisnis. Sekarang menjadi cukup umum menemukan pintu *data center* dikontrol tidak hanya dengan *badge readers*, tetapi juga *biometric scanners*. Dan *single robust data center* tidak lagi mencukupi, institusi finansial harus mempunyai *redundant coverage*, dimana mempunyai pengertian duplikasi "*back-up data center*" dibangun jauh dari *data center* yang utama. Banyak organisasi mengarahkan pelayanan *data center* kepada *third-party* untuk *disaster recovery* dan alih daya untuk beberapa proses bisnis.

Bila perusahaan ingin menjadi teratas dalam bisnis, berarti harus berada teratas dalam teknokogi informasi juga. Dengan pertambahan kuantitas data dari informasi yang dibuat, diproses , disimpan dan di-*deliver* setiap hari, profesional teknologi informasi mengetahui bahwa meng-*upgrade*

komputer "*piece-by-piece*" adalah bukan solusi untuk permintaan yang terus berkembang, jadi diambil cara bagaimana untuk mengabungkan semua komponen itu bersama beserta semua sistem, yaitu dengan menggunakan *data center*.

Untuk menjalankan *operations security* pada *data center* maka banyak hal yang harus diterapkan untuk menjamin keamanan dari *data center* antara lain adalah:

• *Access door*

Keluar masuk ke dalam ruangan data center harus melalui satu pintu saja. Pintu tersebut hanya dapat dibuka dengan menggunakan kartu akses maupun *biometric*. Setiap akses baik melalui kartu dan *finger biometric* akan dicatat baik masuk maupun keluar dari *data center*.

• *Fire protection*

Ruang *data center* dilindungi dengan sensor terhadap kebakaran serta mekanisme pemadamannya, dalam hal ini mekenisme pemadanam api tidak menggunakan air melainkan menggunakan suatu gas (NN100) yang berfungsi mengurangi oksigen, untuk itu perlu dukungan dari SOP agar bila ada alarm kebakaran maka semua personel harus keluar dari ruang *data center* secepatnya (dalam hal ini *best practice* adalah 5 menit) sebelum pengeluaran gas NN100 .

• *Single Entry Door*

Single entry door merupakan pintu masuk ke dalam *data center* yang dibuat sedemikian rupa sehingga hanya satu orang yang bisa lewat pada suatu saat. Hal ini diterapkan agar tidak ada orang yang memanfaatkan saat seseorang punya akses membuka pintu berkesempatan untuk masuk.

Bentuk *single entry door* ini adalah pintu yang berbentuk bulat, dengan mekanisme pintu berputar dengan dimensi yang hanya cukup satu orang.

• *Car Barrier*

Car barrier adalah pagar penghalang kendaraan masuk dalam kawasan gedung *data center*, sehingga dapat mengurangi dampak terhadap bencana dalam bentuk ledakan serta mengisolasikan perangkat yang belum teridentifikasi.

• *Finger Scan*

Finger scan merukan alat bantu dalam penggunaan *access door*, sehingga tingkat keamanan dari ruang server ataupun *data center* dapat lebih terjamin keamanannya, hanya orang-orang tertentu saja yang dapat masuk dan ini dapat meminimalisasi tingkat ancaman.

• *CCTV Camera*

Merupakan kamera yang dipasang di setiap sudut ruangan untuk melakukan *surveillance* dari setiap aktifitas yang ada di *data center* dan akan direkam sehingga setiap kegiatan dapat direkam. Bila terjadi sesuatu maka rekaman ini bisa menjadi suatu alat bantu investigasi yang cukup handal.

• *Uninterrupted Power Supply Control*

Merupakan bagian untuk menjadi keberlangsungan *power* bagi setiap perangkat, perangkat ini bertujuan untuk memberikan *power* saat *main power* mati serta meniadakan gangguan pada aliran dari *main power*.

• *Air Condition Control*

Pengontrolan terhadap suhu dan kelembaban dari ruang *data center*, dimana suhu yang biasa menjadi batasan adalah tidak boleh melebihi dari 20 derajat serta kelembaban dipertahankan pada 50 %.

• *Console Monitoring, remote KVM*

Merupakan suatu alat yang menggantikan fungsi dari *console* (*monitor*, *mouse* dan *keyboard*) sehingga aktiftas di *console* dalam ruang *data center* dapat dikurangi dan digantikan dengan ruangan khusus di luar *data center* (ruang operator) yang terdapat alat KVM untuk dapat mengakses *console*.

• *Segmentation Area restricted area, docking area, storage area, etc*.

Suatu penyusunan ruangan dengan memisahkan kawasan berdasarkan tingkat kekritisan dari perangkat. Biasanya dibedakan antara ruangan *data center* untuk *production*, *development*, ruang *assembling* (merakit mesin), ruangan penyimpanan media *backup*, serta ruangan khusus jaringan.

• *Restricted Lift and Elevator Access*

Melakuan setting pada *lift* dengan men-*disable* akses ruang *data center* secara umum. Jadi akses ke lantai *data center* tidak dapat langsung ditekan tombolnya. Harus ada kartu akses tertentu atau melalui tangga khusus.

• *Raise Floor and Ceiling Management*

Raise floor dibuat untuk menyalurkan udara AC di bawah mesin serta mengurangi medan statis. Sedangkan untuk *ceiling* sebaiknya tidak dibuat plafon/eternit agar tidak menimbulkan gangguan dari kebocoran, kotoran tikus, dan debu.

1.2. Tujuan

Tujuan dari penulisan makalah ini adalah sebagai berikut:

1. Melakukan kajian untuk *operations security* apa saja yang bisa diterapkan dalam suatu Usaha Kecil dan Menengah.

2. Melakukan kajian untuk hal yang tidak bisa diterapkan dan langkah apa yang harus dilakukan untuk dapat mengurangi resiko dan menjamin keamanan sistem.
3. Memberikan alternatif dari sisi teknologi maupun prosedur dalam pelaksanaan *operations security* dalam Usaha Kecil Dan Menengah kesehatan.

Usaha Kecil dan Menengah yang diambil berada dalam domain kesehatan. Usaha Kecil Dan Menengah ini bernama **Klinik Sehat Bahagia.** Klinik ini mulai menggunakan komputerisasi dalam bisnis prosesnya dan untuk mengoptimalkan kinerja dan peralatan Teknologi Informasi yang sudah dibeli maka mereka membutuhkan juga proteksi untuk sistem informasi yang sudah mereka bangun sehingga data-data yang ada cukup signifikan dijaga CIA-nya (*Confidential*, *Integrity* dan *Avaibility*) untuk dapat tetap menjalankan bisnis dengan baik dan menjaga investasi teknologi informasi yang sudah dilakukan agar menjadi optimal.

1.3. Profil Perusahaan

Klinik Sehat Bahagia adalah sebuah poliklinik yang memberikan berbagai layanan kesehatan. Klinik ini terdiri dari:

- Klinik Umum
- Klinik Ibu dan Anak
- Klinik Gigi
- Klinik Mata

Pelayanan kesehatan dilakukan di gedung berlantai dua dengan fasilitas layanan rawat jalan dan rawat inap, laboratorium darah dan ronsen, apotik, dan ruang bersalin. Gedung ini memiliki sepuluh kamar untuk layanan rawat inap kebidanan dan bersalin.

Tenaga medis yang tersedia terdiri dari enam orang dokter umum, empat orang dokter spesialis kebidanan, dua orang dokter gigi, dua orang dokter spesialis mata, enam orang bidan, dan tiga puluh orang perawat. Untuk

pelayanan administrasi dilayani oleh sepuluh orang tenaga administrasi. Pelayanan laboratorium dilayani oleh enam petugas laboratotium. Sedangkan pelayanan apotik dilayani oleh dua apoteker dan enam petugas apotek.

Penanganan teknologi informasi di Usaha Kecil Dan Menengah ini dilakukan oleh bagian teknologi dan sistem informasi yang terdiri dari para pengembang dan pengelola operasional teknologi informasi. Pelaksanaan pengembangan aplikasi baik yang dilakukan sendiri maupun yang dilaksanakan dengan rekanan teknologi informasi dikelola oleh satu kepala grup dengan empat staf yang masing-masing setiap orangnya melakukan analisis, desain, dan *coding*. Tim lainnya dalam hal ini sebagai pelaksana operasional teknologi informasi dipimpin satu kepala grup dan tiga staf yang mana kegiatannya melakukan kegiatan implementasi dan kegiatan operasional teknologi informasi.

Pelaksanaan kebijakan dan prosedur dari teknologi dan sistem informasi hanya berdasarkan keputusan-keputusan yang diambil oleh kepala bagian teknologi informasi dan kedua kepala grup. Kondisi teknologi informasi yang telah diimplementasi saat ini adalah menggunakan aplikasi yang bersifat terpusat dengan setiap user melakukan telnet dari *PC* masing-masing. Hubungan teknologi informasi dari Usaha Kecil Dan Menengah ini terhadap pihak luar hanya terjadi apabila ada konsolidasi dari pembayaran-pembayaran transaksi dari pihak bank.

1.4. Referensi

Sebagai acuan penulisan makalah ini, digunakan berbagai referensi seperti yang dimuat dalam daftar pustaka. Dari keseluruhan referensi yang ada, sebagian memuat hal-hal yang hampir sama dengan bahasa yang hampir seragam sehingga digunakan salah satu di antaranya saja.

II. *OPERATIONS SECURITY*

Dalam penggunaan teknologi infromasi di setiap institusi, terutama yang mengutamakan teknologi informasi dalam proses bisnisnya membutuhkan suatu operasional yang optimal untuk dapat mendukung bisnis yang berjalan. Perbedaan kebutuhan operasional bergantung pada kebutuhan bisnis yang ada. Operasional bisa berupa operasi yang berjalan 7x24 ataupun hanya dalam jam kerja saja dalam berbagai kebutuhannya tetaplah dibutuhkan suatu operasi yang optimal dapat bekerja mendukung bisnis.

Bila berbicara tentang operasional, maka banyak hal yang bisa dilibatkan mulai dari *hardware*, *software*, prosedur dan sumber daya manusianya sendiri untuk bisa melaksanakan operasional itu. Ketergantungan dari setiap komponen di atas sangatlah menentukan keberhasilan operasional yang dilakukan tetapi dengan keberhasilan operasional dengan teknologi yang canggih pun tanpa melibatkan faktor keamanan semuanya menjadi kurang berarti karena informasi atau data apapun yang dihasilkan dari teknologi tanpa adanya keamanan bisa menjadi bencana bila tidak memperhatikan *confidenciality*, *integrity* dan *avaibility* pada umumnya dan keamanan pada khususnya sehingga setiap informasi yang dimiliki benar-benar diperlakukan sebagai asset yang berharga bagi institusi.

Untuk menjamin keamanan operasional tidak hanya bicara teknologi pelindungnya, tetapi kebijakan yang jelas dalam melakukan kemanan operasional adalah sangat penting untuk dapat dijalankan dengan baik karena ancaman yang paling tinggi pada prakteknya adalah dari sumber daya internal sendiri. Hal ini adalah ancaman yang sebenarnya sangat mengancam dan sulit untuk diperkirakan, karena internal sumber daya sudah ada di dalam sistem itu sendiri. Dalam rangka meminimalisasi ancaman ini maka kebijakan untuk keamana operasional harus dibuat dengan sedetail mungkin memperkirakan hal-hal yang dapat menjadi

ancaman, dan melakukan prosedur – prosedur keamanan dengan konsekwen. Jadi tanpa kebijakan dan prosedur yang baik maka tidak hanya ancaman dari luar yang menakutkan tetapi juga lebih menakutkan ancaman dari dalam. Untuk itu setiap divisi teknoogi informasi harus punya kebijakan untuk *corporate user* dalam menggunakan sumber daya teknologi informasi yang dipunyai.

Pada kesempatan ini , penulisan akan membahas sisi operasional dari sudut pandang keamanan operasional tersebut, dan tidak membahas secara detail untuk kebijakan dan prosedur seperti yang dijelaskan dia atas. Operasional yang baik dengan teknologi yang canggih dan sumber daya yang handal tanpa adanya keamanan yang maksimal menjadi sesuatu yang tidak begitu berarti karena tanpa keamanan berarti hanya membuka pintu untuk bencana bagi informasi dan asset yang dimiliki. Sedangkan alat-alat security seperti firewall, proxy hanyalah alat bantu yang harus juga dikendalikan oleh manusia, sehingga ancaman dan kelemahan itu bisa terjadi baik dari ancaman luar, kelemahan teknologi, ataupu ancaman dari internal user. Dalam pembahasan ini akan dijelasakan setidaknya terdapat 3 hal besar yang harus dapat dipahami :

1.Control and Protection

Berisi pemahaman tentang pengaturan dan proteksi dalam kegiatan operasional untuk dapat mencapai tingkat keamanan operasional yang optimal ada bererapa hal yang harus diperhatikan diantaranya adalah *preventive control*, *corrective control detective control*, *deterrent control, application control*, *transaction control* dan *separation and rotation of duties* lebih menekankan kepada *confidenciality* (kerahasiaan) dan *integrity* atau keutuhan data. Semua hal di atas lebih memfokuskan juga pada prosedur pengawasan yang optimal dalam melakukan berbagai hal mulai dari pencegahan hingga rotasi tugas yang baik dan bila tidak dilakukan dengan benar akan menjadi ancaman dan membuka lebar pintu keamanan.

2.Monitoring and Auditing

Setelah dilakukan pengaturan dan proteksi yang baik maka tidak bisa hanya berhenti untuk bisa melakukan proteksi tetapi tetap diperlukan monitoring and auditing untuk bisa mengetahui dan menjamin sejauh mana keamanan yang sudah dicapai, faktor yang harus diperhatikan adalah *Change management*, *Escalation management*, *Record retention*, *Due dilligince*, dan *Logging monitoring*.

Dengan melakukan hal-hal diatas yang lebih bersifat prosedur maka pengawasan keamanan dapat lebih ditingkatkan.

3.Threat and Vulnerabilities

Berisi pemahaman tentang jenis ancaman dan kelemahan yang dapat mengancam operasional keamanan yang sudah dilakukan. Untuk *threat* dan *vulnerability* beberapa hal yang akan dibahas adalah *Accidental Loss*, *Inappropriate Activities*, *Illegal computer operations*, *Account maintenance*, *Data Scavenging Attacks*, *IPL/rebooting*, dan *Network highjacking*. Hal-hal ini tidak mencakup semua ancaman tetapi dapat mewakili berbagai macam ancaman dan kelemahan yang sering terjadi dan kurang menjadi perhatian dan seringkali menjadi ancaman yang tidak terduga dan dapat mengganngu operasional keamanan yang harus dilakukan.

2.1. *Control and Protection*

Tujuan dari kontrol dan proteksi dalam *operations security* adalah menjamin terlaksananya *Confidentiality, Intergity,* dan *Avaibility* yang dijelaskan seperti dibawah ini :

- ***Confidentiality***: dalam keamanan operasional melakukan kontrol terhadap kegiatan operasional yang berdampak pada informasi yang bersifat rahasia dan sensitif.
- ***Integrity***: dalam keamanan operasional melihat seberapa baik/bagus kontrol terhadap kegiatan operasional diterapkan secara langsung yang berdampak pada akurasi dan keaslian data.

- ***Availability***: dalam keamanan operasional melihat dampak yang terjadi pada kegiatan kontrol terhadap tingkat organisasi dengan melihat sifat *fault tolerance* dan kemampuan *recovery* dari suatu *disaster*.

2.1.1 *Preventive Control*

Preventive control dirancang untuk menekan tingkat kesalahan dan tingkat kerusakan dari kesalahan-kesalahan yang tidak disengaja yang masuk ke dalam sistem. Ini juga dilakukan untuk mencegah masuknya *intruder* (yang tidak berhak) baik dari dalam maupun dari luar untuk menggunakan sistem.

Metodologi untuk *preventive control* mesti memenuhi beberapa persyaratan. Tehnik-tehnik pencegahan tersebut haruslah:

1. Dapat mencegah berhasilnya upaya pelanggaran.
2. Dapat diimplementasikan.
3. Dapat dikelola.

Karena tujuan dari *preventive control* adalah untuk mencegah pelanggaran. Maka dari itu upaya ini merupakan persyaratan yang bersifat *mandatory*. Teknologi yang digunakan harus dapat melakukan pencegahan pelanggaran secara *real time*. Ada dua hal yang mesti diperhatikan, pertama, berbagai jenis pelanggaran yang mesti dapat dicegah baik itu dari jenis yang sudah diketahui maupun jenis yang baru. Kedua, upaya-upaya pelanggaran harus dihentikan sebelum berhasil. Selain itu, teknologi yang digunakan harus akurat. *False negative* (kegagalan untuk mencegah serangan) dan *false posiive* (menghentikan serangan padahal tidak ada serangan) tidak mesti terjadi atau paling tidak jarang terjadi.

Menghentikan serangan sebelum upaya tersebut berhasil memerlukan *machine-time response*. Sebaiknya tidak menggunakan orang untuk melakukan respon terhadap serangan karena tidak akan mampu untuk merespon setiap upaya secara cepat. Keterlibatan orang dalam hal ini

hanyalah untuk mengawasi dan melakukan *fine-tuning* terhadap respon otomatis untuk menjamin kesesuaian dengan kebijakan keamanan.
Penyediaan fasilitas ini haruslah tidak memiliki dampak pada kinerja, kehandalan, dan ketersediaan layanan yang harus dilindungi. Tehnik-tehnik yang dipilih atau dikembangkan harus dapat diimplementasikan tanpa berdampak pada penggunaan sistem atau layanan secara tepat.

Selain itu, proteksi harus mudah dikelola. Departemen teknologi informasi harus dapat mengintegrasikan manajemen *preventive control* ke dalam jaringan standar dan tugas-tugas administratif sistem. Administrasi keamanan merupakan tugas yang tidak dapat diprediksi. Inilah salah satu alasan bahwa sistem keamanan harus mutakhir.

Contoh: Penomoran form/server, melakukan validasi data dan prosedur agar tidak terjadi dupllikasi data.

Tehnik-tehnik pencegahan dapat dilakukan baik dari sisi manusia maupun dari sisi komponen teknologi. Ada tiga aspek utama dari sisi manusia: otorisasi, pembuatan kebijakan, dan manajemen. Otorisasi menentukan siapa yang diijinkan untuk menggunakan suatu sumberdaya dan juga kondisi penggunaan yang diijinkan. Pembuatan kebijakan keamanan juga merupakan tugas manusia. Kebijakan keamanan harus mengatur aktivitas apa yang diijinkan dan yang tidak diijinkan.Yang terakhir dari sisi manusia adalah manajemen rutin terhadap komponen teknologi yang digunakan.

Ada tiga komponen teknologi yang digunakan untuk *preventive control*: otentikasi, kontrol perilaku, dan kontrol akses. Tiap-tiap komponen ini mengimplementasi satu jenis kontrol terhadap perilaku sistem. Otentikasi mengontrol akses terhadap sistem sehingga hanya orang-orang yang berhak yang bisa masuk. Kontrol perilaku mengatur apa yang boleh dilakukan pengguna yang berwenang dan otentik pada suatu sistem setelah mereka melakukan *log in*. Kontrol perilaku membatasi eksekusi dan perlaku penggunaan sistem sehingga tetap berada dalam perilaku

yang disetujui seperti yang ditetapkan dalam kebijakan keamanan. Kontrol akses membatasi penggunaan data oleh para pengguna yang otentik dari suatu sistem sesuai dengan kebijakan keamanan.

Dengan bekerja bersama-sama, ketiga aspek teknologi dari *preventive control* ini juga dapat mengontrol dan membatasi aktivitas sistem. Sebagai contoh, suberdaya (*file*) yang digunakan dalam proses otentikasi harus dilindungi. Kendali akses menyediakan proteksi ini. Proses aktual dari otentikasi itu sendiri dilindungi oleh kendali perilaku untuk menjamin bahwa proses otentikasi dieksekusi secara tepat. Otentikasi, pada gilirannya, mengontrol siapa yang dapat memperbaharui dan mengubah sistem kendali akses dan kendali perilaku.

2.1.2 *Corrective Control*

Corrective control memulihkan keadaan yang diakibatkan oleh aktivitas yang tidak berwenang atau mengembalikan kondisi ke keadaan semula sebelum pelanggaran terjadi. Tindakan ini juga digunakan untuk membantu mengurangi dampak yang terjadi dari waktu kejadian kesalahan sampai dengan data prosedur perbaikannya. Kegiatan ini dapat digunakan untuk melakukan pemulihan setelah terjadinya kerusakan.

Contoh : *Restore data backup*, jika terjadi gangguan sistem yang menyebabkan *state* dari database menjadi tidak stabil, maka proses restore dapat dilakukan untuk mengembalikan state ke kondisi terakhir.

2.1.3 *Detective Control*

Detective control digunakan untuk mendeteksi suatu kesalahan pada saat ketika akan terjadi. *Detective control* dapat menggunakan fakta-fakta yang sudah terjadi untuk melakukan pelacakan terhadap transaksi yang tidak berhak yang dapat digunakan sebagai alat penahan. Kegiatan ini bertujuan pula untuk menekan dampak dari kesalahan karena dapat mengindetifikasikan suatu kesalahan dengan cepat.

Contoh: *Audit trail*, jika terjadi sebuah kejahatan melalui sistem, maka proses investigasi dapat dilakukan melalui penelusuran sistem log. Temuan yang didapat dapat digunakan sebagai barang bukti untuk diproses lebih lanjut.

Secara administratif, *detective control* digunakan untuk menentukan seberapa baik kebijakan keamaan dan prosedur-prosedur yang disusun untuk mendeteksi *fraud*, dan untuk menghindari mempekerjakan orang-orang yang melakukan resiko keamanan yang tidak bisa diterima. Kontrol jenis ini meliputi:

- *Review* dan audit keamanan
- Evaluasi kinerja
- *Required vacation*
- Investigasi latar belakang

Review dan audit dapat mengidentifikasi hal-hal dimana kebijakan dan prosedur tidak diikuti secara memuaskan. Keterlibatan manajemen dalam melakukan koreksi dapat menjadi faktor yang signifikan dalam memperoleh dukungan pengguna untuk program keamanan komputer.

Melakukan evaluasi kinerja secara berkala merupakan suatu elemen penting dalam merangsang kinerja kualitas. Di samping itu, evaluasi ini juga merupakan forum yang efektif untuk menegakkan dukungan manajemen dalam prinsip-prinsip keamanan.

Karyawan yang memiliki tekanan lebih memungkinkan untuk membuat kesalahan ketika melakukan pekerjaannya. Liburan membantu karyawan dalam hal kesehatannya untuk memlepaskan tekanan akibat bekerja dalam periode yang lama. Selain itu, jika karyawan dalam posisi kritis dan sensitif dipaksa untuk cuti, kesempatan bagi seorang karyawan untuk mengatur skema *fraudulent* yang membutuhkan kehadiran akan menjadi lebih kecil (misalnya untuk menjaga kelangsungan dan kerahasiaan *fraud*).

Investigasi latar belakang bisa mengungkap kinerja masa lalu yang mengindikasikan resiko potensial pada kinerja masa depan. Investigasi ini mesti dilakukan pada semua karyawan yang dipertimbangkan untuk dipromosikan atau ditransfer ke posisi kepercayaan. Investigasi mesti dilakukan sebelum karyawan tersebut benar-benar ditempatkan dalam posisi sensitif. Pelamar kerja yang dipertimbangkan untuk posisi sensitif mesti juga diinvestigasi untuk masalah-masalah potensial.

2.1.4 *Deterrent Control*

Deterrent control digunakan untuk merujuk kepada suatu kepatuhan (*compliance*) dengan peraturan-peraturan eksternal maupun regulasi-regulasi yang ada.

Contoh: penerapan standar *business practice* yang berlaku secara internasional, yaitu penerapan SWIFT (*Society for the Worldwide Interbank Financial Telecommunication*) pada dunia perbankan, dimana semua bank koresponden SWIFT harus menerapkan standar yang telah ada untuk menjamin *interoperability* antar bank.

2.1.5 *Application Control*

Application control adalah pemindaian secara terus menerus terhadap sistem operasi dan aplikasi untuk mendeteksi perilaku tidak normal. Perilaku tidak normal ini berkaitan dengan penyalahgunaan dari

karyawan, penyusup dari luar, virus, dan *worm*. Sebagian besar kontrol ini dilakukan dengan memonitor *software* yang melakukan *call* ke kernel sistem operasi dari *host computer* dan memungkinkannya untuk "melihat" serangan ketika serangan tersebut terjadi pada *host computer*. Jika masalah terdeteksi maka dengan segera dilakukan tindakan-tindakan untuk mengatasinya sebelum kerusakan terjadi, biasanya dengan menolak atau mematikan aktifitas atau aplikasi tersebut. Misalnya, jika masalah terdeteksi maka akan dilakukan pemutusan trafik terhadap alamat-alamat IP tertentu dalam jaringan, atau memblok akses terhadap aplikasi oleh seorang pengguna atau sekelompok pengguna.

Application control tidak menggantikan kebutuhan akan antivirus, *firewall*, dan *security tools* lainnya melainkan menambahkan lapisan baru dari proteksi terhadap keamanan perusahaan. Organisasi masih memerlukan tools yang ada untuk mengotorisasi pengguna dan data serta untuk mengontrol akses jaringan dan *workstation*.

2.1.6 *Transaction Control*

Transaction control digunakan dalam melakukan kegiatan kontrol dalam setiap tahap transaksi yang dimulai dari insiasi, dokumentasi, *testing* dan manajemen perubahan. Ada beberapa tipe dari *transaction control*, yaitu:

i. Input control

Digunakan untuk memastikan kegiatan transaksi berjalan sesuai dengan aturannya. *Transaction* di sini mempunyai pemahaman setiap kegiatan atau aktivitas yang dilakukan dalam operasional

Contoh: untuk mencatat kegiatan *tasklist* dari urutan kerja operasional maka setiap kegiatan harus diberikan hari tanggal dan tempat tempat aktivitas itu dilakukan.

ii. Processing control

Digunakan untuk menjamin suatu transaksi adalah valid dan akurat termasuk di dalamnya perbaikan pada kesalahan pemasukan data. Dalam kegiatan *operation security* ada kalanya berkaitan dengan

aplikasi. Input-input yang dilaksanakan dalam aplikasi ini secara *embeded* oleh sistem harus divalidasi.

Contoh: dalam proses akhir hari dalam perbankan diperlukan input tanggal transaksi hari itu agar tidak terjadi kesalahan maka sistem harus memeriksa tanggal masukan tersebut. Apabila tanggal tidak sesuai maka sistem harus memberikan tampilan peringatan.

iii. Output control

Digunakan untuk melindungi *confidentiality* dari suatu *output* dan memastikan integritas dari proses *input* sampai dengan proses *output*. Kegiatan ini menjamin bahwa hasil yang dikeluarkan sesuai dengan yang proses yang dilakukan, dan ini harus dapat diawasi untuk menjamin kualitas output yang baik

iv. Change control

Digunakan untuk menjaga integritas data selama proses perubahan, sehingga kehilangan data dapat diminimalisasi dan tidak menimbulkan kerugiaan. *Change control* ini harus dapat dibakukan dalam proses dan prosedur agar setiap saat terjadi perubahan ada pengawasan yang baku sehingga kesalahan dapat dihindari dalam melakukan proses ini.

v. Test control

Digunakan dalam kegiatan *testing* di sistem untuk mencegah adanya program-program/*code-code* yang tidak seharusnya berjalan dalam sistem. Kegiatan ini dilakukan dalam rangkaian meminimalisasi *error*, karena setiap software tidak mungkin bisa dihilanggakan kesalahannya. Suatu saat pasti akan terjadi kesalahan, dan testing ini untuk menjamin pengurangan kesalahan-kesalahan yang akan terjadi

Contoh: menghitung jumlah data dan melakukan *time-stamp*.

2.1.7 *Separation and Rotation of Duties*

Separation and rotation of duties merupakan kegiatan yang membedakan suatu tugas dengan pemisahan orang sehingga diharapkan tidak ada orang yang menguasai sistem secara keseluruhan. Kegiatan ini berhubungan dengan konsep *least privilege*. Sedangkan rotasi dilakukan

untuk meminimalkan terjadinya KKN dalam pelaksanaan kegiatan operasional.

Contoh: pemisahan antara fungsi system administrator dengan *database administrator* dan *security administrator*. Pemisahan antara fungsi melakukan *backup* dengan fungsi yang melakukan penempatan media *backup*.

2.2. Monitoring and Auditing

2.2.1 *Change Management*

Sebuah proses untuk mengelola perubahan proses bisnis atau *policy* organisasi yang memberikan dampak langsung kepada Sistem Informasi dimana terdapat kebutuhan untuk melakukan perubahan pada sistem yang sudah ada. Untuk melakukan manajemen perubahan maka dibentuk suatu tim dari perwakilan pengguna, *business line* manager dan *Infromation Technology admin* untuk mengotorisasi tiap perubahan. Harus dibuat suatu kebijakan yang akan digunakan untuk mengidentifikasi pengguna yang mana yang dapat mengotorisasi perubahan dan pengguna yang mana yang dapat membuat perubahan. Sebagai bagian dari proses dokumentasi, *Information Technology management* harus mengevaluasi permintaan, menentukan sumberdaya yang dibutuhkan, mengatur prioritas dan menyediakan perkiraan biaya kepada manajemen. Segera setelah manajemen menyetujui biaya tersebut dan resiko yang berkenaan dengan perubahan tersebut, *Information Technology management* mesti menugaskan staf yang sesuai dan jadwal perubahan.

Otorisasi perubahan mesti didokumentasikan pada formulir permintaan standar yang merinci perubahan-perubahan, menyediakan justifikasi yang sesuai dan membutuhkan persetujuan manajemen. Formulir ini mesti disetujui oleh *IT management* dan disimpan sebagai bukti bahwa perubahan tersebut sudah diotorisasi.

2.2.2 *Escalation Management*

Sebuah tahapan yang dibutuhkan untuk menangani sebuah keputusan/masalah secara berjenjang sesuai dengan kompleksitas dari keputusan/masalah yang dihadapi. Eskalasi dilakukan mulai dari struktur organisasi yang paling rendah, untuk kemudian dibawa ke struktur yang lebih tinggi. Jika masalah belum dapat ditangani, ataupun jika dibutuhkan sebuah proses otorisasi dari orang yang mempunyai wewenang lebih tinggi. Manajemen eskalasi merupakan proses pemantauan situasi, menilai kemampuan organisasi untuk mengendalikan situasi. Dalam hal ini, manajemen eskalasi merupakan tujuan inti dari *emergency response* dalam suatu organisasi.

Setiap insiden adalah unik. Setiap insiden baru membutuhkan dibentuknya suatu *emengency response organization* yang mampu untuk mengendalikan insiden. Dalam prakteknya, misalnya, mengirim orang yang tepat dalam jumlah yang cukup ke lokasi insiden, membuat rencana yang tepat untuk mengatasi situasi darurat, memberi informasi kepada orang yang tepat, dan membuat gambaran mutakhir dari perkembangan situasi. Untuk dapat menangani keadaan darurat secara efisien, dibutuhkan suatu rencana yang tepat dan organisasi yang berkemampuan menanganinya. Eskalasi adalah apa yang terjadi ketika rencana tidak sesuai dengan status aktual dari insiden. Eskalasi terjadi jika organisasi tidak lagi mampu untuk mengendalikan situasi sehingga perlu melakukan perubahan untuk mendapatkan kembali kendali tersebut.

2.2.3 *Record Retention*

Record retention adalah suatu catatan yang berupa daftar yang berisi informasi tentang berapa lama suatu dokumen dipertahankan. Beberapa dokumen dipertahankan untuk waktu tertentu karena alasan hukum, sementara yang lainnya berdasarkan pertimbangan-pertimbangan praktis. Mekanisme penyimpanan informasi historikal untuk sebuah periode waktu

yang diinstruksikan atau dianjurkan oleh negara atau hukum yang berlaku.

Informasi tersebut harus tetap disimpan untuk kebutuhan audit, ataupun untuk penelusuran informasi tentang suatu kejadian yang terjadi di masa lalu. Informasi yang tetap disimpan bisa berbentuk berkas fisik ataupun dalam bentuk arsip digital.

2.2.4 *Due Dilligince*

Memastikan langkah-langkah tertentu sudah dilakukan untuk melakukan operasional dengan baik. Proses investigasi dilakukan oleh pihak yang tidak berkepentingan/netral atas nama pihak yang akan melakukan transaksi bisnis (dalam proses pembelian perusahaan, *merger*, peminjaman uang atau pembelian saham) untuk keperluan penyediaan informasi yang akan digunakan untuk mengevaluasi keuntungan dan resiko yang terkait.

2.2.5 *Logging Monitoring*

Sistem yang baik menggunakan suatu cara untuk melakukan pencatatan terhadap aktifitas baik dalam sistem maupun *checklist* operasional. Pencatatan ini berlangsung secara terus menerus dan tersimpan dalam sistem. Catatan tersebut dipantau secara berkala dan dilakukan verifikasi guna memastikan tidak adanya aktifitas abnormal.

Pemantauan ini dilakukan secara berkala untuk memastikan tidak ada aktivitas yang bersifat abnormal. Jika ternyata ditemukan aktivitas yang abnormal maka akan ditindaklanjuti sesuai dengan prosedur yang berlaku.

Sebuah proses pemantauan catatan/log yang dimiliki oleh sebuah sistem/*hardware* untuk mengevaluasi kinerja atau investigasi sebuah

insiden. Tindakan lebih lanjut akan dilakukan setelah kesimpulan didapat dari evaluasi yang telah dilakukan sebelumnya.

Dengan adanya *logging monitoring* akan akan mempermudah kerja administrator untuk dapat melakukan langkah-langkah solusi yang signifikan dalam menjamin operasional untuk dapat berjalan dengan optimal sesuai dengan yang diharapkan.

2.3. *Thread and Vulnerabilties*

2.3.1 *Accidental Loss*

Accidental threats terkait dengan kesalahan dan penghilangan, kesalahan, dan penghilangan yang dilakukan oleh karyawan atau orang dalam adalah penyebab utama dari masalah keamanan informasi. Kesalahan seringkali menjadi ancaman (contoh: kesalahan *programming* dapat membuat sistem *crash*) atau dapat membuat kelemahan (contoh: layar komputer yang ditinggal dapat dieksploitasi oleh pengguna yang tidak berwenang).

Ancaman yang terutama pada umumnya adalah kecellakaan karena meningkatkan kelemahan melalui konfigurasi yang tidak benar atau pengaturan keamanan yang tidak dibaharui atau penggunaan *software* seperti sistem operasi dan *database* tanpa memperbaharui *patches*. Beberapa ancaman mengakibatkan sabotase tetapi kebanyakan adalah kecelakaan dan penghilangan.

Ancaman-ancaman ini menghasilkan:

- Keputusan yang dibuat menjadi tidak benar;
- Gangguan kepada fungsi bisnis;
- Hilangnya kepercayaan publik;
- Kehilangan finansial;
- Kewajiban hukum dan *breakdown of duty of care*;
- Penambahan biaya yang terjadi.

Beberapa hal yang termasuk *accidental threat* adalah sebagai berikut:

- Kegagalan layanan komunikasi.
- Kegagalan operasi yang dialihdayakan.
- Kehilangan atau ketidakhadiran personil kunci.
- *Misrouting/re-routing* pesan-pesan.
- Kesalahan staf operasi atau pengguna.
- Kesalahan *software* atau pemrograman.
- Kegagalan teknis.
- Kegagalan transmisi.

Kegagalan layanan komunikasi dapat menyebabkan hilangnya ketersediaan informasi melalui layanan ini. Jika layanan komunikasi tidak tersedia, organisasi tidak bisa melakukan komunikasi antar situs, mengirim pesan ke pihak luar melalui *e-mail*, mengakses informasi yang tersimpan pada media penyimpan yang berada di jaringan luar atau memroses informasi menggunakan *software* aplikasi yang terletak pada jaringan tersebut.

Kegagalan komunikasi dapat disebabkan kerusakan yang tidak disengaja pada pengabelan jaringan, kerusakan perangkat jaringan seperti *router* atau server, kegagalan *software*, atau kehilangan layanan seperti telekomunikasi atau daya listrik.

Contoh-contoh *vulnerability*-nya:

- Kekurangan redudansi dan *back-up*.
- Manajemen jaringan yang tidak memadai.
- Kurangnya perencanaan dan implementasi pengabelan komunikasi.
- Kurangnya penanganan insiden.

Pengalihdayaan (*outsourcing*) operasi menimbulkan ancaman lain terhadap organisasi. Kontrak alih daya harus mencakup kebutuhan dan

tanggung jawab keamanan. Kegagalan operasi alih daya dapat menimbulkan kehilangan *availability*, *confidentiality* dan *integrity* dari informasi.

Contoh-contoh *vulnerability*-nya:

- Kewajiban yang tidak jelas dalam perjanjian alih daya.
- Tidak ada rencana atau prosedur *Business Continuity* untuk pemulihan informasi dan asset informasi.
- Sistem *back-up* yang tidak tersedia.

Personil tertentu bisa jadi kritis terhadap penyediaan efektif layanan. Kehilangan atau ketidakhadiran dari personil seperti itu dapat menyebabkan kehilangan *availability*, *confidentiality* dan *integrity* dari informasi.

Kehilangan atau ketidakhadiran personil kunci dapat disebabkan oleh beberapa faktor, misalnya, kejadian alam, masalah transportasi, sakit, stress, dan lain-lain.

Contoh-contoh *vulnerability*-nya:

- Tidak ada cadangan personil kunci.
- Prosedur yang tidak didokumentasikan.
- Kurangnya perencanaan yang berkelanjutan.

Pengarahan atau *re-routing* pesan-pesan kepada orang yang salah dapat menimblkan kehilangan *confidenciality* atau kerahasiaan jika pesan-pesan ini tidak diproteksi, dan kehilangan *availability* atau ketersediaan bagi orang yang dituju. *Misrouting* maupun *re-routing* pesan-pesan dapat menyebabkan kehilangan *integrity* dari pesan-pesan tersebut dengan memungkinkan perubahan yang tidak berwenang yang dilakukan sebelum penyampaian ke tujuan aslinya. *Misrouting* yang tidak disengaja biasanya disebabkan oleh kesalahan pengguna.

Contoh-contoh *vulnerability*-nya:

- Kurangnya pelatihan pengguna.
- Data sensitif tidak dienkripsi.
- Kurangnya bukti penerimaan pesan.

Kesalahan tindakan oleh operator dapat menyebabkan ancaman terhadap *integrity*, *availability*, *confidentiality* dan *reliability* data. Berikut adalah contoh-contohnya:

- Kesalahan *set-up* pada fitur keamanan dapat menyebabkan kehilangan *integrity*, *availability*, *confidentiality* dan *reliability* data.
- Mematikan komputer ketika pesan kesalahan muncul sebagai ganti dari menutup semua aplikasi yang sedang berjalan.
- Tidak sengaja menimpatulis atau menghapus berkas-berkas.
- *Back-up* yang tidak memadai.
- Pengolahan data dengan versi yang salah.

Contoh-contoh *vulnerability*-nya:

- Kurangnya kesadaran pengguna.
- Pelatihan keamanan yang tidak mencukupi.
- Kurangnya dokumentasi.
- Kurangnya kendali perubahan konfigurasi yang efisien.
- Antarmuka pengguna yang rumit.

Jika kesalahan-kesalahan dibuat selama pengembangan, pemeliharaan atau proses instalasi perangkat lunak, *integrity*, *reliability*, *confidentiality* dan *availability* informasi yang diolah dapat terancam.

Commercial off-the-shelf software tidak ada jaminan merupakan *software* yang tanpa kesalahan. Microsoft telah merilis perangkat lunak yang membuat celah pada sistem terhadap ancaman keamanan. Misalnya, Hotmail memiliki *bug* yang memungkinkan seseorang untuk menggunakan *account* dari para pelanggannya dengan atau tanpa *password*. Perangkat lunak Microsoft Outlook dan Outlook Expresss

mempunyai *bug* yang memungkinkan *malicious code* untuk dijalankan pada komputer tanpa sepengetahuan pengguna dan menyebabkan Outlook dan Outlook Expresss gagal, atau memungkinkan *hacker* untuk menggunakan hak akses pengguna untuk memformat ulang disk, mengubah data atau berkomunikasi dengan situs-situs eksternal.

Contoh-contoh *vulnerability*-nya:

- Prosedur siklus hidup pengambangan sistem yang tidak memadai.
- Spesifikasi yang tidak jelas atau tidak lengkap.
- Kurang efisien dan efektifnya konfigurasi kendali perubahan.
- Staf yang tidak ahli.

Kegagalan dapat terjadi pada perangti perangkat keras atau jaringan. Hal ini bisa disebabkan:

- Kegagalan manufaktur peralatan tersebut.
- Perubahan temperatur atau kelembaban.
- Kesalahan penanganan peralatan ketika melakukan relokasi.
- Tanpa sengaja menjatuhkan atau membenturkan peralatan seperti pelatan komputer dekstop atau *notebook*.
- Kegagalan pendingin ruangan.
- Kehilangan layanan esensial seperti telekomunikasi atau listrik.

Contoh-contoh *vulnerability*-nya:

- Kurangnya proteksi lingkungan.
- Kurangnya kesadaran pengguna.
- Pemeliharaan yang tidak tepat atau tidak sesuai terhadap fasilitas-fasilitas teknis.
- Kurangnya fasilitas atau proses *back-up*.
- Kurangnya kapasitas jaringan melalui perencanaan yang tidak tepat atau pemeliharaan.
- Kegagalan dalam proses manajemen perubahan.
- Tidak adanya rencana atau prosedur *Business Continuity*.

Kegagalan transmisi dapat merusak *integrity* dan *reliability* data, dan dapat menimbulkan hilangnya *availability*. Hal ini terjadi karena kegagalan salah satu dari komponen jaringan yang digunakan untuk transmisi data yang seperti itu.

Contoh-contoh *vulnerability*-nya:

- Pengabelan yang tidak tepat atau tidak sesuai.
- Kurangnya fasilitas atau proses *backup*.
- Tidak adanya rencana atau prosedur *Business Continuity*.

2.3.2 *Inappropriate Activities*

Inappropriate activity adalah aktivitas dalam pemakaian komputer yang sekedar penyalahgunaan biasa sampai yang termasuk tindak kriminal. Penggunaan yang tidak sesuai mencakup aktivitas yang luas. Sebagai contoh adalah pada sisi yang satu karyawan melakukan belanja *online* pada jam kerja, dan pada sisi lainnya, bisa terjadi aktivitas kriminal seperti menjual rahasia perusahaan.

Satu dari yang paling utama bentuk dari penggunaan yang tidak sesuai adalah melihat, men-*download*, atau mendistribusikan bahan pornografi. Sejumlah peristiwa sudah membuktikan dapat mempermalukan perusahaan tetapi ini merupakan suatu resiko untuk perusahaan manapun, tanpa tergantung dengan ukuran perusahaannya. Penggunaan yang tidak sesuai tidak hanya memalukan, tetapi mempunyai akibat di antaranya:

- Hilangnya produktivitas.
- Berkurang atau hilangnya *bandwidth* jaringan.
- Meningkatnya resiko terinfeksi virus dan *malicious code* lainnya.
- Meningkatnya resiko dari kewajiban dan tindakan hukum.

Untuk meminimalkan resiko dari penggunaan yang tidak sesuai, cukup mendasar untuk menyediakan klarifikasi dari apa yang bisa dan tidak bisa diterima dalam suatu organisasi.

Apa yang dianggap/disebut penggunaan tidak sesuai ada bermacam-macam dari satu organisasi ke yang lainnya, Kuncinya adalah untuk meyakinkan kebijakan yang jelas yang dibuat oleh perusahaan, dan semua orang dapat memperhatikannya.

Ada beberapa hal yang bisa dianggap sebagai aktivitas yang tidak semestinya diantaranya adalah penggunaan e-mail. Banyak organisasi yang mengijinkan stafnya untuk menggunakan sistem *e-mail* untuk kebutuhan pribadi yang wajar. Yang bisa dijadikan ukuran wajar adalah apa yang dianggap wajar dalam ukuran umum. Yang dianggap kurang wajar misalnya adalah hal-hal berikut:

- Karyawan menerima guyonan melalui *e-mail* eksternal dari temannya.
- Karyawan mem-*forward* ‘guyonan’ tersebut ke rekan-rekannya melalui *e-mail* internal.
- Karyawan itu mem-*forward* ‘guyonan’ tersebut ke *distribution list* internal.
- Karyawan lain mem-*forward* ‘guyonan’ tersebut ke rekannya secara eksternal.

Masalah lain yang termasuk aktivitas yang tidak semestinya adalah penyingkapan dengan sengaja terhadap informasi sensitif. Skenario berikut adalah contoh serius penyalahgunaan yang disengaja terhadap *e-mail*:

- Mengirimkan data sensitif keluar dari organisasi.
- Membocorkan atau menggunakan daftar pelanggan untuk kepentingan pribadi.
- Penyingkapan daftar harga.

Contoh-contoh ini tidak terbatas pada *e-mail*. Seseorang dapat membawa salinan cetak dari daftar harga, misalnya. Namun *e-mail* tentunya membuat hal tersebut jadi lebih mudah, secara potensial kurang dilacak, dan memungkinkan untuk didistribusikan dalam jumlah besar secara cepat.

Selanjutnya adalah penyalahgunaan akibat kurang hati-hati. Berikut adalah tindakan yang kurang hati-hati:

- Mengirim dokumen perusahaan ke *e-mail accoun*t rumah untuk dikerjakan di rumah.
- Mengirim kembali dokumen tersebut ke kantor dari rumah.
- Mengirim berkas berukuran besar.
- Melakukan CC yang berlebihan.

Dua hal yang pertama dapat mengekspos informasi perusahaan ke dalam resiko yang tidak mesti terjadi di tempat kerja. Anggota keluarga mungkin dapat melihat informasi rahasia karena sebagian rumah memiliki perangkat fisik yang digunakan bersama-sama. Dua hal yang terakhir merupakan kesalahan sederhana yang dapat membuat *e-mail* menjadi kurang efisien.

2.3.3 *Illegal Computer Operations*

Aktifitas komputer yang diangap sebagai kesengajaan dan ketidaksahan aktivitas komputer untuk keuntungan keuangan pribadi dan untuk penghancuran

- *Eavesdropping*
- *Fraud*
- *Theft*
- *Sabotage*
- *External Attack*

Eavesdropping adalah tindakan seseorang dalam menangkap atau mendengarkan percakapan secara diam-diam. Tindakan ini dilakukan terhadap pesan-pesan *email*, pesan instan, dan metode komunikasi lainnya yang dianggap pribadi. Pesan-pesan dapat diproteksi terhadap *eavesdropping* dengan menerapkan layanan keamanan *confidentiality* atau *privacy*. Layanan keamanan ini biasanya diimplementasikan dengan enkripsi.

Fraud adalah semua jenis kejahatan dimana seseorang dengan cara yang salah memperoleh dan menggunakan data pribadi orang lain dengan cara tertentu yang melibatkan penipuan khususnya untuk memperoleh keuntungan ekonomis.

Contoh jenis-jenis *fraud* adalah transaksi palsu, manipulasi data, dan penggantian integritas data lainnya dengan tujuan keuntungan.

Fraud biasanya juga melibatkan pencurian identitas. Dengan identitas curian tersebut, si pencuri dapat menggunakannya untuk melakukan transaksi *online* menggunakan kartu kredit seseorang, misalnya. Bentuk lain dari penggunaan identitas curian adalah dengan tujuan untuk memasuki suatu sistem. Jika si pelaku telah memasuki sistem tersebut maka dengan mudah dia dapat memanipulasi data dalam sistem tersebut bahkan juga dapat menghancurkan data secara keseluruhan.

Theft adalah semua jenis pencurian informasi atau data serta pencurian *hardware* dan *software* secara fisik. Jika pencurian secara fisik bisa lebih mudah dihindari dengan melakukan pengamanan fisik terhadap berbagai sumberdaya fisik dan mudah dilihat dengan mata, tidak demikian dengan yang pencurian informasi atau data. Pencurian informasi atau data salah satunya bisa dimulai dengan pencurian identitas. Dengan identitas curian, si pelaku bisa mencuri data dari sistem yang dimasukinya dan menjualnya kepada pihak lain untuk memperoleh keuntungan ekonomis.

Untuk menghindari pencurian informasi atau data perlu diterapkan suatu kebijakan keamanan pada sistem maupun pada personil yang berinteraksi dengan sistem tersebut.

Contoh jenis-jenis *theft* adalah pencurian informasi atau menjual rahasia untuk memperoleh keuntungan atau penyingkapan yang tidak berwenang, dan pencurian fisik *hardware* dan *software*.

Sabotage adalah merugikan dengan sengaja, *defacement*, pengrusakan atau penggantian pada berkas elektronik, data, halaman web, program, dan lain-lain.

Contoh jenis-jenis *sabotage* adalah *Denial of Service* (*DoS*), *production delays*, dan sabotase integritas data.

Ada banyak jenis *Denial of Service*. Berikut adalah gambaran tentang *Distributed Denial of Service*. *Denial of Service* adalah gangguan atau degradasi koneksi internet atau layanan *e-mail* yang mengakibatkan interupsi aliran informasi normal. *Denial of Service* biasanya disebabkan oleh serangan *ping*, *port scanning*, jumlah data masuk yang berlebihan, dan sebagainya.

Untuk menfasilitasi *Denial of Service*, para penyerang perlu memiliki beberapa ratus sampai beberapa ribu *host* yang bisa digunakan. Proses untuk menggunakan *host* dan menginstal *tool* yang diperlukan dilakukan secara otomatis. Prosesnya bisa dibagi ke dalam langkah-langkah berikut:

1. Mulai fase pemindaian dimana sejumlah besar *host* diperiksa celah keamanan yang mudah diserang.
2. Berkompromi dengan *host* tersebut untuk memperoleh akses.
3. Menginstal *tool* yang dibutuhkan pada setiap *host*.
4. Menggunakan *host* tersebut untuk melakukan pemindaian lebih lanjut.

Karena proses tersebut dilakukan secara otomatis, penyerang dapat berkompromi dan menginstal *tool* yang dibutuhkan pada *host* yang dituju dalam hitungan detik. Dengan kata lain, dalam satu jam, beberapa ribu *host* dapat dikompromikan. *Host* tersebut yang akan digunakan sebagai sumber serangan kepada target yang dituju dengan menggunakan *tool* yang telah terinstal di dalamnya.

2.3.4 *Maintenance Account*

Biasanya dalam sistem ada *account* untuk *maintenance* seperti *administrator* atau *root*, seringkali pengguna sistem lupa untuk mengubah *account* ini dari *default* yang ada pertama kali, sehingga dapat mudah sekali ditebak oleh user yang tidak terotorisasi atau pun orang luar sangat memungkinkan sekali masuk dalam sistem.

2.3.5 *Data Scavenging Attacks*

Data scavenging adalah teknik penambahan data infromasi dari bit data yang ditemukan. Dua tipe *data scavening attacks* adalah:

- *Keyboad attack*: suatu tindakan untuk mengekstrak informasi dari media penyimpan dengan cara mengeksekusi *software utilities*, *keystroke*, atau sumber daya sistem lainnya yang dieksekusi dari *keyboard*. Misalnya, *utility* pemulih *disk* dan *file* dan prosedur *memory scavenging* dapat digunakan untuk melakukan *keyboard attack*.
- *Laboratory attack*: menggunakan peralatan pemulih sinyal di lingkungan laboratorium untuk memulihkan informasi yang tersimpan dari media penyimpan data.

2.3.6 *IPL/Rebooting*

Permulaan setiap sistem selalu dapat memberikan kelemahan, pada saat IPL (*Initial Program Load*), seorang operator dapat saja menjalankan program, data yang tidak terotorisasi, bahkan mereset sistem. Operator memiliki kemampuan untuk masuk ke sistem dengan modus *single user*

tanpa fitur keamaan penuh. Dalam kondisi ini operator dapat memuat program-program atau yang tidak semestinya, mereset password, mengganti nama berbagai sumber daya, atau mereset jam dan tanggal sistem. Operator juga dapat menetapkan ulang *data port* atau jalur komunikasi untuk mengirim informasi ke luar *data center*.

Dalam LAN, administrator sistem dapat memulai *boot sequence* dari *tape*, *CD-ROM*, atau *floppy disk*. Dengan demikian bisa melewati keamanan sistem operasi pada *hard drive*.

Dengan ancaman ini harus dilakukan pembagian tugas bagi administrator ataupun dengan *split knowledge* sehingga ancaman seperti ini dapat dikurangi,karena pada dasarnya adalah human error yang harus dapat diatasi bisa dengan prosedur ataupun sistem

2.3.7 *Network Address Hijacking*

Intruder selalu saja dapat merubah *route* dari *traffic data* dari server, jaringan ke *personal machine*, baik dengan modifikasi alamat perangkat ataupun *network address"hijacking"*, dengan melakukan ini *intruder* dapat saja melakukan analisis data ataupun modifikasi atau mencuri *password* dari server.

Salah satu cara yang dilakukan oleh *intruder* adalah dengan menggunakan *tool* yang disebut "tap" untuk mengambil alih sesi *login* yang sedang berlangsung pada sistem. *Tool* ini memungkinkan intruder untuk menggunakan akses *root* untuk memperoleh kendali ke sesi manapun yang sedang aktif pada sistem, mengeksekusi perintah-perintah seolah-oleh perintah-perintah tersebut dilakukan oleh pemilik sesi tersebut. Jika pengguna sesi sebelumnya telah melakukan *telnet* atau *remote login* ke sistem lain maka *intruder* bisa juga memperoleh akses ke *remote system*, melewati otentikasi normalnya dibutuhkan untuk mengaksesnya.

Deteksi terhadap pembajakan ini bisa dilakukan. Pemilik sesi yang dibajak bisa mengetahui aktivitas yang tidak biasa tersebut, termasuk tampilan perintah yang diketik oleh *intruder*. Para pengguna mestinya menyadari kemungkinan ini dan mendorong mereka untuk melaporkan aktivitas yang mencurigakan. Untuk mencegah terjadinya pembajakan ini, pertahanan utamanya adalah dengan cara menggunakan akses *root* secara hati-hati terhadap sistem, menginstal *security patch*, dan menggunakan *firewall* untuk mengontrol jaringan.

III. KAJIAN USAHA KECIL DAN MENENGAH KLINIK SEHAT BAHAGIA

3.1. *Best Practice* dalam *Operasions Security* pada *Banking Industry*

Sebagai bahan perbandingan, berikut akan dibahas secara ringkas *best practice* yang digunakan dalam perbankan. Industri perbankan dipilih sebagai perbandingan karena industri ini bersifat mission critical dan memiliki dampak yang luas jika prosedur pengamanan tidak diberlakukan secara baik dan benar.

- *Preventive Control*

  Tindakan pencegahan yang dilakukan adalah dengan penggunaan *access control* dan *single entry door*. Pengendalian akses terhadap sumber daya dilakukan agar tidak terjadi akses yang tidak diinginkan terhadap sumberdaya organisasi. Selain itu, untuk memudahkan pengawasan, dibuat sistem satu pintu masuk. Dengan demikian pencegahan bisa dilakukan dengan lebih mudah.

  Pengawasan satu pintu masuk akan dikombinasikan dengan adanya mekanisme pengenalan pengguna dengan digunakannya access card, ataupun finger recognition. Tanpa adanya teknologi pengenalan pengguna yang baik, maka preventive control dapat berjalan dengan optimal

- *Corrective control*

  Tindakan korektif dilaksanakan dengan melakukan kegiatan *upgrade* dan *patching*. Kegiatan ini dimaksudkan untuk memperbaharui sistem dengan versi yang lebih baru atau dengan menambal celah-celah keamanan yang memungkinkan untuk dimanfaatkan oleh pihak tertentu.

  Contoh tindakan korektif lain adalah jika adanya korupsi data yang diakibatkan bugs dari aplikasi, maka proses perbaikan dapat dilakukan dengan melakukan restore, atau koreksi data melalui utility kecil.

Satu hal yang harus dilakukan jika hal ini terjadi, maka koreksi yang dilakukan harus pada aplikasi, dengan merelease versi yang lebih baru, dan perbaikan data.

- *Detective control*

  Tindakan detektif yang dilakukan adalah dengan pemasangan *intrusion detection system* dan *audit trail*. Dengan sistem pendeteksi ini, segala usaha untuk menyusup ke dalam sistem dapat diketahui. Intrusion Detection System (IDS) yang berguna untuk mengenali pola-pola serangan yang berpotensi menghancurkan internal network sebuah organisasi. IDS bersifat preventif, dengan berusaha untuk mengantisipasi serangan lebih awal dan dapat menekan angka kerugian yang lebih besar terhadap operasional organisasi. Untuk mengantisipasi adanya pola serangan di masa depan yang belum diidentifikasi saat ini, maka IDS haruslah di upgrade versinya secara periodik agar pola serangan yang baru dapat dikenali dan dicegah.

- *Accidental Loss*

  Penerapan prosedur Business Continuity Plan sebagai rencana untuk tetap melakukan bisnis di tengah terjadi kehilangan, adalah sesuatu yang patut dilakukan untuk dapat mengatasi accidental loss yang tidak bisa diperkirakan darimana sumbernya dan Disaster Recovery Centre sebagai backup plan untuk dapat mengembalikan data juga merupakan kegiatan yang sebaiknya harus dipunyai dan dilakukan test untuk setiap beberapa waktu , sehingga bila benar-benar terjadi bencana, sudah dapat mengatasinya karena sudah terbiasa dengan prosedur yang selalu dilatih untuk diterapkan

- *Inappropriate Activities*

Untuk mencegah penggunaan komputer yang tidak semestinya dalam jaringan suatu organisasi dilakukan pemasangan *content filtering*. Dengan demikian, para pengguna tidak dapat mengakses informasi, khususnya melalui internet, secara bebas.

Hal lain yang dapat dilakukan adalah adanya pembagian wilayah network secara logical, dimana pada network tertentu yang memiliki informasi sensitive akan diproteksi lebih tinggi disbanding wilayah network lain.

Pada implementasinya adalah wilayah network production akan berada disebuah VPN environment yang tidak dapat diakses oleh wilayah network lain, meskipun mereka secara fisik berada pada jaringan yang sama. Dengan adanya penerapan ini, maka hanya pihak tertentu yang memiliki akses ke VPN yang dapat mengakses resource yang terdapat dalam wilayah yang dilindungi tersebut.

- *Illegal Computer Operations*

  Dalam upaya untuk membatasi operasi illegal maka dilakukan pemasangan *firewall* dan *audit log analysis*, sehingga dapat diketahui setiap kegiatan akses user, untuk itu administrator harus peka dalam melakukan analisa, karena seringkali alat- alat Bantu seperti firewall itu hanya melakukan logika yang diinstall pada alat itu, tetapi seringkali *illegal computer operations* dapat dilakukan tanpa dimengerti firewall untuk dicegahnya.

- *Maintenance Account*

  Melakukan prosedur pembagian *password* untuk super user suatu sistem. Disini diterapkan sebuah konsep yang bernama separation of concern, yaitu adanya sebuah pemisahan concern (dalam hal sekuriti concern adalah privilege yang dimiliki oleh seorang user) secara fisik dan didistribusikan ke beberapa orang yang berkompeten.

  Hal ini akan mencegah adanya excessive power (kekuasaan yang berlebihan) yang dimiliki oleh satu orang. Dengan adanya

pemisahan privilege ke beberapa orang, akan dapat dijamin bahwa masing-masing pihak akan saling mengontrol satu sama lain.

Kalaupun ada penyelewengan tanggung jawab, haruslah dilakukan secara kolektif, dimana penyelewengan dilakukan bersama-sama dengan orang lain yang memiliki wewenang pada area lain.

3.2. Implementasi *Operations Security* pada Usaha Kecil dan Menengah Klinik Sehat Bahagia

3.2.1 *Control and Protection*

- *Preventive Control*

  Penerapan *preventive control* pada Klinik Sehat Bahagia adalah dengan membuat kebijakan keamanan yang mengatur otorisasi penggunaan sumberdaya baik secara fisik maupun logis. Otorisasi ini juga mencakup pengaturan kondisi penggunaan sumberdaya melalui pengaturan batasan wewenang dan aktivitas apa saja yang boleh dilakukan. Di samping itu, digunakan juga teknologi yang dapat melakukan pencegahan pelanggaran secara *real time*.

- *Corrective Control*

  Sebagai sarana untuk memulihkan keadaan akibat aktivitas yang tidak berwenang atau akibat kesalahan operasi, disiapkan suatu prosedur *backup* dan *restore* untuk data-data yang penting. Dengan demikian jika masalah terjadi bisa dikembalikan ke kondisi sebelum terjadinya masalah tersebut.

- *Detective Control*

  Penggunaan *audit trail* diterapkan untuk melacak penyimpangan terhadap sistem. Jika masalah terjadi, investigasi dapat dilakukan melalui penelusuran sistem log. Dari sistem log tersebut dapat ditemukan bukti yang bisa digunakan untuk proses lebih lanjut.

- *Application Control*

Untuk mendeteksi perilaku yang tidak normal dari sistem operasi dan aplikasi maka dipasang suatu *tool* untuk kebutuhan ini. *Tool* ini digunakan untuk mendeteksi penyalahgunaan dari karyawan, penyusup dari luar, virus, dan *worm*. *Tool* yang digunakan tidak menggantikan fungsi *firewall*, dan antivirus.

- *Transaction Control*

  Sebagai kontrol terhadap transaksi, dibuat suatu kebijakan untuk mengatur transaksi mulai dari inisiasi, dokumentasi, *testing*, dan manajemen perubahan.

- *Separation and Rotation of Duties*

  Pengendalian sistem agar tidak terjadi penguasaan sistem secara keseluruhan adalah dengan membuat kebijakan yang mengatur pemisahan tugas dan rotasi. Kebijakan ini menggunakan konsep *least priviledege*.

3.2.2 *Monitoring and Auditing*

- *Change Management*

  Penerapan *change management* pada klinik ini adalah dengan membuat suatu kebijakan yang mengaturnya. Dalam kebijakan tersebut diatur suatu prosedur untuk mengidentifikasi pengguna yang mana yang dapat mengotorisasi perubahan dan pengguna yang dapat melakukan perubahan.

  Dengan adanya implementasi *Change management* akan memberikan jaminan dari stabilitas sistem yang sedang berjalan, dimana setiap perubahan haruslah melalui kegiatan protokoler yang harus dipatuhi oleh semua pihak yang terkait. Dengan adanya protokoler tersebut, sistem tidak dapat diubah secara seenaknya, dimana perubahan yang dilakukan kemungkinan dapat membuat ketidak stabilan sistem yang dapat mengganggu operasional organisasi.

- *Record Retention*

  Catatan yang berupa daftar yang berisi informasi tentang berapa lama suatu dokumen dipertahankan dibuat dalam suatu daftar yang disebut *record retention*. Pengaturan mengenai berapa lama untuk masing-masing dokumen tersebut dipertahankan diatur dalam kebijakan. Record retention sebuah informasi biasanya diatur oleh badan regulasi dari masing-masing industri. Dimana informasi yang disimpan dapat digunakan lagi untuk penelusuran permasalahan yang telah terjadi dimasa lalu.

- *Logging Monitoring*

  Manajemen membuat suatu kebijakan yang berguna untuk melakukan pemantauan *log* yang dihasilkan oleh sistem. Pemantauan ini dilakukan secara berkala untuk memastikan tidak ada aktivitas yang bersifat abnormal. Jika ternyata ditemukan aktivitas yang abnormal maka akan ditindaklanjuti sesuai dengan prosedur yang berlaku.

  Log yang dihasilkan oleh alat alat network, atau pun aplikasi haruslah dianalisa untuk mengenali pola dari aktivitas sistem yang terjadi. Hasil analisa ini dapat digunakan untuk mengetahui adanya pola-pola penipuan, atau manipulasi yang dilakukan oleh pihak internal organisasi yang berpotensi memberikan kerugian secara financial, atau non financial. Pada beberapa industri log adalah salah satu informasi krusial yang masuk dalam item checklist backup harian, mengingat tingginya nilai informasi yang terkandung dalam log tersebut.

3.2.3 *Thread and Vulnerabilties*

- *Accidental Loss*

  Untuk mengantisipasi terjadinya *accidental loss*, dibuat suatu kebijakan untuk penanganan insiden, prosedur manajemen jaringan, penggunaan redudansi pada server, dan prosedur

back-up dan *restore*. Di samping itu juga dibuat suatu prosedur yang mengatur masalah alih daya (*out source*) untuk menghidari ketidajelasan kewajiban pihak luar yang dikontrak jika terjadi ketidaksesuaian dengan produk atau layanan yang dikerjakannya. Masalah lain yang tidak kalah pentingnya adalah penerapan enkripsi untuk data-data sensitif dan melakukan pelatihan secara berkala bagi pengguna sistem.

- *Inappropriate Activities*

  Untuk kebutuhan ini, dibuat suatu kebijakan yang mengatur batasan-batasan penggunaan sumberdaya, baik fisik maupun non-fisik. Pengaturan ini meliputi pembatasan penggunaan *e-mail account* dari sisi bagaimana dan untuk tujuan apa saja *account* tersebut digunakan. Selain itu, diatur juga masalah transmisi data apa saja yang boleh dilakukan ke luar organisasi. Untuk menghindari para pengguna dari pengaksesan situs-situs yang tidak diinginkan, dipasang *content filtering* yang menyaring situs mana yang bisa diakses.

  Pengaturan lain yang dapat dilakukan adalah adanya pengamanan berjenjang dimana masing-masing jenjang hanya mampu mengakses wewenang tertentu saja. Dengan adanya pengamanan ini, maka aktivitas dari pengguna sistem akan terkontrol dan aktivitas lain diluar wewenang yang dapat memberikan kerugian bagi organisasi dapat dicegah secara preventif.

- *Illegal Computer Operations*

  Masalah ini mungkin bisa dikatakan masalah yang paling serius yang dapat mengancam keamanan sistem. Untuk itu dibuat suatu kebijakan yang menyeluruh dan ditinjau secara berkala untuk menjamin kesesuaian dengan perkembangan yang berlaku. Kebijakan ini mencakup masalah penggunaan *tool* (misalnya *intrussion detection system*) yang bisa digunakan dalam sistem

untuk menangkal dan mengurangi dampak dari serangan. Selain itu, dilakukan pelatihan secara berkala untuk membangun kesadaran akan pentingnya keamanan sistem.

- *Maintenance Account*

  Masalah ini sebetulnya merupakan masalah sederhana namun dapat berdampak serius terhadap keamanan sistem. Untuk mengatasinya dibuat suatu *account register* dan informasi *account* dibagikan kepada masing-masing pengguna. Selain itu para pengguna juga digalakkan untuk melakukan perubahan *password* secara berkala dan merahasiakannya kepada pengguna lain.

  Adapun password yang digunakan juga harus memiliki minimal jumlah karakter, kombinasi huruf ataupun angka yang dapat mempersulit password abuse terhadap sebuah account.

- *Data Scavenging Attacks*

  Masalah ini lebih cenderung diakibatkan oleh orang dalam organisasi. Untuk itu dibuat suatu kebijakan yang mengatur bahwa *data center* ditempatkan pada ruangan tersendiri dengan satu pintu masuk dan diamankan secara fisik dengan menggunakan kunci ruangan. Kunci tersebut digandakan untuk masing-masing pengguna yang diijinkan untuk memasuki ruangan tersebut. Di dalam ruangan ditempatkan suatu catatan yang harus diisi setiap orang yang memasuki ruangan. Informasi yang dicatatkan adalah nama dan waktu masuk dan keluar ruangan. Untuk mengatasi serangan dari luar ruangan, digunakan *tool* yang ditujukan untuk mendeteksi tindakan penyimpangan terhadap sistem. Selain itu dibuat juga prosedur penghapusan berkas elektronik dengan suatu metode yang dapat menjamin bahwa data yang dihapus tidak bisa dipulihkan kembali agar tidak bisa dilacak oleh orang-orang yang tidak berkepentingan.

- IPL/rebooting

  Permulaan setiap sistem selalu dapat memberikan kelemahan, pada saat IPL (*Initial Program Load*), seorang operator dapat saja menjalankan program, data yang tidak terotorisasi, bahkan mereset sistem. Operator memiliki kemampuan untuk masuk ke sistem dengan modus *single user* tanpa fitur keamaan penuh. Dalam kondisi ini operator dapat memuat program-program atau yang tidak semestinya, mereset password, mengganti nama berbagai sumber daya, atau mereset jam dan tanggal sistem. Operator juga dapat menetapkan ulang *data port* atau jalur komunikasi untuk mengirim informasi ke luar *data center*.

  Kebijakan yang dibuat untuk mengantisipasi masalah ini sudah tercakup dalam kebijakan mengenai *data scavenging*.

- *Network Highjacking*

  Kebijakan yang dibuat sehubungan dengan masalah ini adalah melakukan pelatihan secara berkala tentang ancaman-ancaman yang mungkin terjadi. Selain itu dilakukan *security patch* terhadap sistem secara berkala, serta menggunakan *firewall* untuk mengontrol jaringan.

3.3. Beberapa Penerapan *Security* dalam *Data Center*

- *Access door*

  Keluar masuk ke dalam ruangan data center harus melalui satu pintu saja. Pintu tersebut hanya dapat dibuka dengan menggunakan kartu akses maupun biometric. Setiap akses baik melalui kartu dan finger biometric akak dicatat baik masuk maupun keluar dari data center. Pengaturan access door ini dapat diterapkan dengan memadukan dalam SOP, seperti misalnya pintu masuk dari depan sebagai akses utama, sedangkan pintu masuk dari belakang hanya digunakan apabila

ada nya kegiatan pemasukan barang maupun evakuasi jika terjadi sesuatu hal (mungkin kebakaran ataupun gempa bumi).

Access door dalam implementasinya selalu dikaitkan dengan teknologi lainnya seperti untuk identifikasi dapat digabungkan dengan finger scan biometric dan untuk limitasi dapat digabungkan dengan single entry door.

Penerapan ini dalam UKM dapat diimplementasikan pada pembatasan masuk (pintu depan dan pintu belakang) dan sebagai pengganti kartu akses (karena biasanya relative mahal bagi UKM), dapat digantikan dengan pemberian anak kunci kepada beberapa personel yang dalam pemberian anak kunci tersebut di syah kan dengan berita acara serah terima. Dalam berita acara serah terima tersebut dimasukan pemberian kewenanngan dan tanggung jawab terhadap akasesnya.

• *Fire protection*

Ruang data center dilindungi dengan sensor terhadap kebakaran serta mekanisme pemadamannya, dalam hal ini mekenisme pemadanam api tidak menggunakan air melainkan menggunakan suatu gas (NN100) yang berfungsi mengurangi oksigen, untuk itu perlu dukungan dari SOP agar bila ada alarm kebakaran maka semua personel harus keluar dari ruang data center secepatnya (dalam hal ini best practice adalah 5 menit) sebelum pengeluaran gas NN100 . Sensor kebakaran dapat digabungkan dengan alat komunikasi seperti *link* ke sistem *pager*, *email* maupun *handphone* dengan SMS nya. Biasanya sensor kebarakan dapat berupa sensr tehadap asap ataupun perubahan panas, sensor tersebut dipasang baik di bawah *raise floor* untuk mendeteksi terjadinya hubungan singkat dari kabel *power*, ada juga sensor yang di letakan di atas. Dalam implementasinya biasanya dihubungkan juga ke sistem *access door*, dimana bila terjadi alarm kebakaran maka sistem *access door* secara otomatis akan membuka semua pintu., sehingga bila ada personel yang sedang berada dalam *data center* dapat dengan segera secara langsung

keluar ruangan sehingga terhindar dari sistem penyemprotan kebakaran.

Penerapan ini dalam UKM akan sangat mahal, sebaiknya dalam UKM implementasi dari *fire protection* adalah dengan membeli pemadam kebakaran yang biasa ditenteng dengan tangan, namun dibedakan dari isi tabung pemadam kebakraan. Isi tabung pemadam kebakaran biasanya dibagi atas 3 tipe yaitu air, busa dan bubuk. Untuk UKM dalam meminimalkan resiko akibat kebakaran di ruang *data center*-nya atau ruang komputernya ada baiknya menggunakan alat pemadam kebakaran yang menggunakan campuran gas dan bubuk dalam bentuk tabung yang mudah dibawa bawa.

- *Single Entry Door*

  Single entry door merupakan pintu masuk kedalam *data center* yang dibuat sedemikian rupa sehingga hanya satu orang yang bisa lewat pada suatu saat. Hal ini di terapkan agar tidak ada orang yang memanfaatkan saat seseorang punya akses membuka pintu dia bisa masuk.

  Bentuk *single entry door* ini adalah pintu yang berbentuk bulat, dengan mekanisme pintu berputar dan dimensi hanya cukup satu orang. Model pintu ini serupa dengan model bila kita akan masuk ke “Dunia Fantasi” dimana ada alat yang berputar dan hanya satu orang yang bisa lewat, setelah satu personel yang lewat maka alat itu akan berhenti bergerak dan menunggu *trigger* dari personel selanjutnya.

  Memang harga dari *single entry door* ini sangat mahal, sehingga penerapan di UKM mungkin tidak pernah diterapkan, namun dalam hal ini UKM masih dapat menggunakan prinsip *single entry door* ini dengan menerapkannya dalam suatu SOP serta menambah personel satpam yang setiap saat selalu berada dan menjaga pintu masuk. Satpam tersebut ditugaskan untuk

memastikan setiap personel yang masuk wajib untuk mengisi buku registrasi masuk dan keluar serta menolak bila ada personel yang tidak berhak masuk (tidak memiliki tanda otorisasi).

• *Car Barrier*

Car barrier adalah pagar penghalang kendaraan masuk dalam area gedung *data center* sehingga dapat mengurangi dampak terhadap bencana dalam bentuk ledakan serta mengisolasikan perangkat yang belum teridentifikasi. Penerapan *car barrier* biasanya saat ini biasanya dilakukan oleh beberapa pemilik gedung yang tujuan bukan hanya untuk bagunan data center namun untuk keseluruhan area.

Untuk UKM bila berada atau menyewa ruangan dalam gedung yang pemilik gedungnya sudah menerapkan *car barrier* maka UKM tersebut secara tidak langsung sudah menerapkan *car barrier*. Namun untuk UKM yang memiliki gedung sendiri biasanya hal ini tidak pernah dilaksanakan.

• *Finger Scan*

Finger scan merukan alat bantu dalam penggunaan *access door*, sehingga tingkat keamanan dari ruang server ataupun *data center* dapat lebih terjamin keamanannya, hanya orang-orang tertentu saja yang dapat masuk dan ini dapat meminimalisasi tingkat ancaman.

Dalam penerapannya di UKM biasnya sangat jarang karena relatif mahalnya peralatannya. Hal ini biasanya berhubungan dengan penerapan *access door*, dimana fungsi ini diganti dengan anak kunci.

• *CCTV Camera*

Merupakan kamera yang di pasang di setiap sudut ruangan untuk melakukan *surveillance* dari setiap aktifitas yang ada di *data center* akan direkam sehingga setiap kegiatan dapat direkam dan bila terjadi sesuatu menjadi suatu alat bantu investigasi yang cukup handal.

Dalam penerapan di UKM biasanya hal ini digantikan dengan pemanfaatan dari satpam, dimana dalam SOP ditambahkan prosedur buat satpam untuk selalu melakukan pengawasan ruangan, agar pengawasan ruangan ini berjalan dengan efektif maka satpam biasanya dibekali dengan *secure box* yang harus diputar setiap saat dengan menggunakan kunci tertentu, kunci tertentu tersebut biasanya diletakan secara permanent dibeberapa area yang harus di kunjungi oleh satpam.

• *Uninterrupted Power Supply Control*

Merupakan bagian untuk menjadi keberlangsungan *power* bagi setiap perangkat, perangkat ini bertujuan untuk memberikan *power* saat *main power* mati serta meniadakan gangguan pada aliran dari main power. UPS ini dapat berupa UPS besar yang mengontrol seluruh alat ataupun UPS ini dapat yang berbentuk modular yang di pasang di setiap alat.

Dalam penerapan di UKM hal ini sudah menjadi umum, dimana setiap alat biasanya di berikan UPS sederhana (*Stavolt*).

• Air Condition Control

Pengontrolan terhadap suhu dan kelembaban dari ruang data center, dimana suhu yang biasa menjadi batasan adalah tidak boleh melebihi dari 20 derajat serta kelembaban di pertahankan pada batas 50 %.

Penerapan dalam UKM sangat jarang, biasanya mengandalkan kemanpuan dari AC biasa yang hanya pengatur suhu saja, sering terjadi kelemahan di dalam penerapan pada UKM yaitu di tandai dengan adanya embun di kaca-kaca ruang *data center* atau ruang komputer.

- *Console Monitoring*, *remote KVM*

  Merupakan suatu alat yang menggantikan fungsi dari *console* (*Monitor*, *mouse* dan *keyboard*) sehingga aktiftas di *console* dalam ruang *data center* dapat di kurangi dan digantikan dengan ruangan khusus diluar *data center* (ruang operator) yang terdapat alat KVM untuk dapat mengakses *console*.

  Hal ini tidak pernah di lakukan di UKM mengingat ruangan *data center* atau ruang computer yang sangat terbatas, sehingga pekerjaan *console* sering dilakukandi ruang *data center*. Hal ini dapat diminimalkan resikonya dengan penerapan *control accsess door* yang diperkuat dengan integritas satpamnya.

- *Segmentation Area*, *restricted area*, *docking area*, *storage area*, *etc*.

  Suatu penyusunan ruangan dengan memisahkan area berdasarkan tingkat kekritisan dari perangkat, biasanya dibedakan antara ruangan *data center* untuk *production*, *development*, ruang *assembling* (merakit mesin) , ruangan penyimpanan media *backup*, ruangan khusus jaringan.

  Biasanya untuk UKM pemisahan segmentasi ini tidak pernah di lakukan, untuk meminimalkan resiko ada baiknya semua kegiatan instalasi, tes dan sebagainya (diluar kegiatan *production*) dilakukan di luar ruang *data center* atau ruang komputer.

• *Restricted Lift and Elevator Access*

Melakuan *setting* pada *lift* dengan men-*disable* akses ruang *data center* secara umum, jadi akses ke lantai *data center* tidak dapat langsung ditekan tombolnya. Harus ada kartu akses tertentu atau melalui tangga khusus.

Hal ini tidak ada dalam penerapan UKM, untuk meminimalkan resiko dapat menerapkan *access door* yang di perkuat dengan satpam.

• *Raise Floor and Ceiling Management*

Raise floor dibuat untuk menyalurkan udara AC di bawah mesin serta mengurangi medan statis. Sedangkan untuk *ceiling* sebaiknya tidak dibuat plafon/eternit agar tidak menimbulkan gangguan dari kebocoran, kotoran tikus, dan debu.

Dalam penerapan di UKM dapat di laksanakan dengan menaikan lantai dengan raise floor. Biasanya kendala adalah faktor biaya.

3.4. Kesimpulan

Dari pembahasan yang dilakukan terhadap Usaha Kecil dan Menengah Klinik Sehat Bahagia, dapat disimpulkan bahwa:

1. Tidak semua aspek *operation security* dapat diimplementasikan karena berbagai keterbatasan dan skala bisnis yang ada.
2. Pembuatan dan penerapan kebijakan keamanan sistem dilakukan sesuai dengan kondisi yang ada maupun kebutuhan organisasi.
3. Penekanan dilakukan pada pembuatan dan penerapan SOP (*Standard Operation Procedure*) dan pelatihan personil yang menggunakan sistem untuk membangun kesadaran akan pentingnya masalah keamanan sistem.

Lampiran

Operasional Prosedur Masuk Data Center

1. RUANG DATA CENTER MERUPAKAN RUANG YANG BERSIFAT RESTRICTIED AREA.

2. SEMUA PERSONEL YANG AKAN MASUK RUANG DATA CENTER HARAP MELAPOR KEPADA PETUGAS JAGA SECURITY.

3. SETIAP PERSONEL DILLUAR PERSONEL INTERNAL DATA CENTER OPERATION YANG MASUK DAN KELUAR RUANG DATA CENTER WAJIB DILAKUKAN PEMERIKSAAN FISIK OLEH PETUGAS JAGA SECURITY

4. LEPASKAN SEPATU ATAU SANDAL ANDA DI LUAR RUANG DATA CENTER TEPATNYA DI LOBBY DEPAN RUANG DATA CENTER.

5. MASUK KE DALAM DATA CENTER HARUS MEMAKAI SANDAL YANG TELAH DISEDIAKAN, DAN SETELAH SELESAI HARUS DIKEMBALIKAN PADA TEMPATNYA SESUAI DENGAN NOMOR SEMULA.

6. DILARANG MEMBAWA TAS KEDALAM RUANG DATA CENTER, TAS HARUS DISIMPAN DALAM LOCKER YANG TELAH DISEDIAKAN DAN KUNCI HARAP DIBAWA, DAN SETELAH SELESAI HARUS DIKEMBALIKAN PADA TEMPATNYA SESUAI DENGAN NOMOR SEMULA.

7. SETIAP PERSONEL DAN TAMU YANG MASUK DAN KELUAR RUANG DATA CENTER WAJIB MENGISI REGISTER MASUK, DAN MENGISI DENGAN LENGKAP DAN BENAR.

8. DILARANG MASUK KE RUANG DATA CENTER BAGI YANG TIDAK MEMILIKI SECURITY ID CARD, SECURITY ID CARD DIBERIKAN OLEH BAGIAN DATA CENTER OPERATION.

9. DILARANG MENGELUARKAN DAN ATAU MEMASUKKAN BARANG APAPUN KE RUANG DATA CENTER TANPA IJIN DAN SEPENGETAHUAN BAGIAN DATA CENTER OPERATION. TERMASUK DIDALAMNYA ALAT KOMUNIKASI SEPERTI TELEPON SELULAR (GSM/CDMA), HANDY TALKY DAN SEBAGAINYA.

10. PASTIKAN PINTU TELAH TERTUTUP RAPAT SAAT MASUK/KELUAR RUANG DATA CENTER.

11. DILARANG MEROKOK DI SELURUH LANTAI DAN AREA DATA CENTER.

12. DILARANG MEMBAWA MAKANAN/MINUMAN KEDALAM RUANG DATA CENTER .

13. DILARANG MAKAN DAN MINUM DI SELURUH LANTAN DAN AREA DATA CENTER

14. DILARANG MENGADAKAN RAPAT / PERTEMUAN DI LOBBY DEPAN RUANG SERVER. RAPAT / PERTEMUAN HARUS DILAKSANAKAN DI RUANG RAPAT YANG SUDAH TERSEDIA.

15. MENJAGA KEBERSIHAN RUANG DATA CENTER.

16. SEMUA KEGIATAN DI RUANG DATA CENTER DI MONITOR OLEH CCTV SURVEILLANCE CAMERA.

17. KEGIATAN VENDOR DI LUAR AKTIFITAS RUTIN WAJIB MENYERAHKAN SURAT PENUNJUKAN PEKERJAAN.

W A R N I N G

RESTRICTED AREA
AUTHORIZE PERSONAL
ONLY
DO NOT ENTER !!

A T T E N T I O N

ALL PERSONAL MUST FILL REGISTRATION BOOK, FILL COMPLETELY AND SIGN !!

REGISTRASI AKSES DATA CENTER

Nomor Locker	Nomor Sandal	Nama Lengkap	Nomor Identitas KTP/NIP/PIN	Unit Kerja Perusahaan/Divisi/Bagian	Keperluan	Waktu			Tanda - Tangan		
						Tanggal	Jam Masuk	Jam Keluar	Masuk	Keluar	Security

Daftar Pustaka

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

"Bringing Manageability to the Data Center", http**:*//*www.panduit.com/products/WhitePapers/102084.pdf diakses 20 Oktober 2005.

"Secure Network Design", http://www.hill.com/archive/pub/papers/papers.asp?yr=2003&mn=10, diakses 25 Oktober 2005.

"Five Technologies to Help Ensure Data Security What a Small Business Must Know", http://oe.quickbooks.com/misc/-datasecurity.pdf, diakses 27 Oktober 2005.

Government of Punjab. Department of Information Systems and Administrative Reforms, "*Information Technology (IT) Security Guidelines*", http://www.doitpunjab.gov.in/IT/securityguide.pdf, diakses 16 Oktober 2005.

"*AIMD-96-85R Security Weaknesses at IRS' Cyberfile Data Center*", http://www.steptoe.com/publications/PI1684.pdf, diakses 16 Oktober 2005.

"*RemoteStor Security White Paper*", http://www.msiservice.com/uploads/1103657752.pdf, diakses 16 Oktober 2005.

"*Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*", http://www.cert.org/archive/pdf/bankfin040820.pdf, diakses 16 Oktober 2005.

"*CERT-In Guideline CISG-2003-01*", http://www.cert-in.org.in/knowledge base/guidelines/cisg-2003-01.pdf, diakses 16 Oktober 2005.

"*eSign Security Policy*", http://www.verisign.com.au/repository/security/eSign_security_policy_V1.4.pdf, diakses 16 Oktober 2005.

Powanda, Jane. "*Writing an Operational Security Plan*", http://www.itsc.state.md.us/security/PDF/FISSEA.pdf, diakses 16 Oktober 2005.

"*Security case study: Cardinal Health*", http://www.itworld.com/Man/3886/CIOwatch/pfindex.html, diakes 27 Oktober 2005.

"*Computer Security Threat*", http://www.caci.com/business/ia/threats.html, diakses 28 Oktober 2005.

"*IT Security - Inappropriate Usage*", http://www.investni.com/index/develop/ebusiness/ebusiness_it_security/ebusiness_it_security_inappropriate_usage.htm, diakses 28 Oktober 2005.

"*Information Security Guideline for NSW Government - Part 2 Examples of Threats and Vulnerabilities*", http://www.oit.nsw.gov.au/Guidelines/4.3.17.g.security.asp#A50, diakses 25 Oktober 2005.

"*Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks*", http://www.cisco.com/warp/public/707/newsflash.html, diakses 5 Desember 2005.

"*Internet Address Spoofing and Hijacked Session Attacks*", http://www.ciac.org/ciac/bulletins/f-08.shtml, diakses 5 Desember 2005.