Government Computer Security Incident Response Team

BADAN PENGKAJIAN DAN PENERAPAN TEKNOLOGI

PANDUAN PENANGANAN INSIDEN

INFRASTRUKTUR

Diadopsi dari : SOP Incident Handling Infrastructure
Kementrian Komunikasi dan Informastika Republik Indonesia

BUKU PETUNJUK PELAKSANAAN

BPPT CSIRT
2014

DAFTAR ISI

BAGIAN 1 : PENDAHULUAN

Penanganan Insiden Keamanan Infrastruktur adalah bagian dalam menangani keamanan informasi. Sebab dari keadaan infrastruktur, seluruh komponen resource teknologi informasi yang ada dan diaplikasikan dalam suatu organisasi akan mempengaruhi keamanan informasi yang ada padanya.

1.1 TUJUAN

Panduan ini dimaksudkan untuk unit-unit di lingkungan BPPT memahami tentang penanganan suatu insiden yang terjadi pada infrastruktur fisik teknologi informasi. Infrastruktur fisik teknologi informasi terdiri dari semua komponen, baik komponen utama maupun komponen penunjang yang secara kasat mata terlihat fisiknya. Penanganan insiden yang tepat dan cepat akan sangat bermanfaat untuk mencegah terhambatnya layanan kerja di lingkungan BPPT.

Ketersediaan dari infrastruktur fisik tersebut harus selalu siap digunakan. Penanganan suatu insiden ditujukan utuk mencapai hal-hal sebagai berikut,

a. Mengumpulkan informasi sebanyak mungkin tentang sifat insiden
b. Menghalangi atau mencegah eskalasi kerusakan yang disebabkan oleh insiden tersebut
c. Memperbaiki kerusakan yang disebabkan oleh insiden tersebut
d. Mengumpulkan bukti insiden yang sesuai
e. Memulihkan layanan sesegera mungkin
f. Mengambil langkah-langkah proaktif untuk mengurangi insiden masa depan.

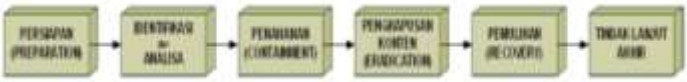
1.2 RUANG LINGKUP

Ruang lingkup pelaksanaan panduan ini adalah melingkupi seluruh komponen infrastruktur Teknologi Informasi. Untuk melakukan suatu pengawasan analisis dan penyelesaian problem yang bisa mempengaruhi keamanan informasi. Hal ini ditujukan untuk profesional TI dan manajer dalam organisasi di BPPT. Para penerima produk ini lebih lanjut dapat mendistribusikannya kepada para pemangku kepentingan teknis dalam organisasi mereka. Insiden keamanan pada infrastruktur bisa bermacam-macam, prosedur penanganan.

BAGIAN 2 :

PROSEDUR PENANGANAN INSIDEN KEAMANAN INFRASTRUKTUR

Agar tujuan diatas dapat terlaksana dengan baik, maka perlu ditentukan tahapan untuk melakukan penganan terhadap insiden yang terjadi. Tahapan tersebut digambarkan sebagai berikut:



Gambar 2.

Tahapan Penanganan Insiden Keamanan Infrastruktur

2.1 Tahap Preparation (Persiapan)

Pada tahap ini dilakukan persiapan untuk melakukan penanganan terhadap insiden pada infrastruktur fisik teknologi informasi.

- **Persiapan personil**

Meskipun memiliki kendali proses dan teknis yang kuat, keamanan dapat dikompromikan dengan memanfaatkan personil dan membuat mereka melakukan tindakan yang sebaliknya tidak diizinkan. Tim penanganan insiden yang terampil merupakan komponen kunci dari penanganan dan penahanan yang efektif. Sebuah tim

penanganan insiden yang baik adalah sumber daya sangat berharga ketika dibutuhkan untuk menangani situasi yang mungkin timbul karena adanya malware, dengan cara yang efisien dan efektif. Sebagaimana orang adalah sumber daya organisasi utama yang akhirnya dirugikan oleh infeksi malware, kesadaran akan keamanan merupakan salah satu dari isu-isu yang perlu terus menerus dipantau dan ditingkatkan untuk perlindungan yang tepat dari berbagai serangan.

a. Kesadaran Keamanan :

   Kesadaran keamanan dapat dianggap sebagai yang paling penting dari semua langkah-langkah persiapan, yang dapat membantu dalam mengidentifikasi dan mencegah sebagian besar masalah yang akan timbul. Pengguna mengetahui cara melindungi informasi, apa yang harus dilakukan dan apa yang tidak harus dilakukan, siapa yang harus dihubungi pada keadaan darurat dan bagaimana cara menganalisis jika mendapatkan kesulitan

b. Matrik eskalasi penanganan insiden

   Setiap organisasi harus memiliki matrik eskalasi penanganan insiden yang secara jelas mendefinisikan siapa yang harus dihubungi dalam kasus insiden. Hal ini juga menunjukkan tingkat eskalasi untuk keterlibatan lebih jauh sesuai dengan kompleksitas atau dampak dari insiden.

c. Tim Terampil Penangan Insiden

   Sebuah tim penanganan insiden yang berpengetahuan dan terampil dapat mengurangi sebagian besar

dampak terhadap bisnis. Tim penanganan insiden harus memiliki pemahaman yang sangat baik dan tingkat keterampilan dalam berbagai teknologi yang digunakan oleh perusahaan. Karena, banyak perusahaan memiliki kantor-kantor cabang yang berlokasi di wilayah geografis yang berbeda, tim komando pusat dan tim lokal/regional yang sesuai sangat direkomendasikan untuk dibentuk. Tim Perintah Pusat Tentu saja, harus memandu tim lokal dalam menangani insiden .

Persiapan alat dan teknologi

Persiapan alat dan teknologi ditujukan untuk melakukan perbaikan terhadap infrastruktur fisik dari teknologi informasi. Beberapa peralatan yang dipersiapkan disini meliputi:

a. Peralatan instrumentasi

Peralatan instrumentasi merupakan peralatan uji atau ukur yang berfungsi untuk mengukur besaran fisis tertentu. Peralatan ini digunakan untuk memeriksa penyebab dari malfunctionnya suatu perangkat fisik infrastruktur jaringan. Contoh dari peralatan ini adalah multimeter, cable tester, signal analyser, dan lainnya

b. Peralatan pertukangan

Peralatan pertukangan digunakan untuk memperbaiki fasilitas penempatan dari perangkat infrastruktur teknologi informasi. Akibat dari pengrusakan dan vandalisme bisa diperbaiki dengan menggunakan pearalatan pertukangan ini. Contoh dari peralatan ini tang, obeng, hammer, gergaji, dan lainnya.

c. Peralatan Keselamatan kerja

Peralatan keselamatan kerja digunakan untuk melindungi diri ketika seseorang akan mengerjakan sesuatu yang membahayakan dirinya. Contoh dari

peralatan ini adalah sabuk pengaman, sarung tangan, alat anti listrik statis, dan lain-lain.

d. Peralatan forensik fisik

Peralatan forensik fisik digunakan untuk melakukan identifikasi terhadap pelaku pengrusakan pada fasilitas penempatan, maupun peralatan fisik yang menjadi korban dari gangguan. Peralatan ini biasanya digunakan untuk memindai jejak dari para pelaku pengrusakan (CCTV, rekaman kejadian, CSI).

Persiapan dokumen

Suatu dokumen kebijakan biasanya menguraikan persyaratan tertentu atau aturan yang harus dipenuhi. Suatu dokumen prosedur adalah dokumen yang memandu pengguna secara teknis dalam proses (langkah demi langkah) tentang cara untuk mencapai persyaratan yang telah ditetapkan dan diuraikan dalam dokumen kebijakan. Beberapa kebijakan, yang sering digunakan untuk membantu dalam penanganan insiden fisik adalah,

a. Kebijakan Keamanan :

Sebuah kebijakan keamanan adalah dokumen tingkat tinggi dari top manajemen yang menunjukkan pendekatan organisasi terhadap keamanan informasi. Menurut standar ISO 27001 Keamanan Informasi, dokumen harus memberikan arahan dan dukungan dari manajemen untukkeamanan informasi sesuai dengan kebutuhan bisnis, hukum, dan peraturan yang relevan.

b. Kebijakan penggunaan yang diperbolehkan (acceptable use)

Kebijakan ini berisi tentang sesuatu yang diperbolehkan atau tidak diperbolehkan, termasuk pemanfaatan semua sumber daya organisasi. Hal ini akan membantu pencegahan terhadap masuknya

penyusup ke dalam fasilitas penempatan peralatan fisik teknologi informasi.

c. Kebijakan penggunaan perangkat mobile

Kebijakan perangkat mobile harus menentukan bagaimana pengguna diarahkan untuk mengetahui tindakan apa saja yang bisa dan boleh dilakukan oleh pengguna dalam menggunakan perangkat mobilnya. Hal ini juga harus menetapkan langkah apa yang perlu diambil pengguna untuk memastikan keamanan, tidak hanya keamanan fisik dari perangkat mobile itu sendiri, tetapi juga dari informasi yang terkandung didalamnya.

d. Kebijakan melakukan Backup

Kebijakan melakukan backup harus mendefinisikan apa, kapan, dan bagaimana informasi harus dibackup. Hal ini harus mendefinisikan secara jelas mengenai jenis informasi dan kapan waktu proses backup harus dilakukan, dan bagaimana cara untuk melakukannya. Backup yang baik kadang-kadang bisa menjadi satu-satunya cara untuk pulih dari kerusakan serius yang disebabkan pada fisik.

e. Kebijakan pelaporan dan mekanisme pelacakan insiden

Keberhasilan di balik rencana penanganan insiden adalah memiliki mekanisme pelaporan dan pelacakan yang mudahdigunakan dan efektif. Pengguna umumnya mengharapkan mekanisme pelaporan yang dapat dengan mudah dipahami dan menangkap insiden denganinformasi sesedikit mungkin. Pengguna juga harus bisa memberikan tingkat prioritas formal yang dapat divalidasi dan diubah, jika diperlukan oleh helpdesk atau tim keamanan pusat. Nama, nomor telepon dan alamat email untuk menghubungi dalam kasus terjadinya

suatu aktivitas berbahaya yang dicurigai harus diberikan melalui semua media komunikasi seperti situs intranet perusahaan, buletin dan catatan kecil di sekitar workstation pengguna.

f. Prosedur dan formulir investigasi personil

Organisasi harus memiliki metode dan prosedur untuk melakukan investigasi terhadap personil IT. Investigasi ditujukan untuk mengetahui apakah terdapat adanya kelalaian atau kesengajaan yang bisa menjadi sebab terganggunya keamanan fisik infrastruktur teknologi informasi.

g. Prosedur dan formulir penanganan insiden

Organisasi harus memiliki rencana dan prosedur penanganan insiden yang tepat dan bisa dilakukan di tempat organisasi berada. Organisasi harus menyediakan form yang dapat digunakan untuk mencatat dan merekam semua kejadian secara rinci, selama penanganan insiden pada semua tahapan.

h. Dokumen audit

Catatan dari audit secara berkala pada sistem informasi akan membantu dalam mengungkap setiap aktivitas berbahaya yang ada. Catatan ini dapat mengungkap kegiatan yang dilakukan pengguna pada sistem yang mungkin tidak disadari. Tim audit biasanya terdiri dari personil terlatih yang tahu apa yang harus dicari.

i. Dokumen profil perangkat keras pada proses bisnis

Disarankan untuk memiliki profil dari semua perangkat keras danproses- proses yang harus berjalan pada sistem berdasarkan proyek atau departemen. Hal ini dapat membantu dalam identifikasi secara cepat dari keberadaan perangkat kerasdan fungsi utama dari perangkat keras tersebut.

j. Dokumen pengetahuan

Sebuah dokumentasi rinci dari pengetahuan dasar yang baik dan mudah mendapatkannya, dapat menghemat banyak waktu ketika insiden terjadi. Ketika sebuah insiden terjadi, semua dokumentasi mengenai penanganan kejadian harus ditambahkan ke dokumen basis pengetahuan. Jadi jika insiden yang sama terjadi lagi, proses penanganannya akan menjadi lebih cepat karena sudah ada catatan cara penanggulangannya. Hal ini akan menghemat banyak waktu yang akan dikonsumsi dalam analisis ulang insiden tersebut. Sebuah template analisa akar permasalahan (Root Cause Analysis) yang dapat menangkap sebagian besar rincian Insiden harus disiapkan dan digunakan.

2.2 Tahap Identifikasi (Identification)

Pada tahap ini dilakukan identifikasi terhadap insiden yang terjadi pada infrastruktur fisik teknologi informasi.Identifikasi dilakukan untuk menentukan obyek, penyebab, dan dampak dari gangguan pada infrastruktur fisik. Obyek dari infrastruktur teknologi informasi dapat dibedakan menjadi 2 macam, yaitu :

a. **Hardware**

Hardware (perangkat keras) dari infrastruktur teknologi informasi ini dapat dikategorikan menjadi 2 komponen, yaitu,

1. Komponen utama

   Komponen utama adalah peralatan dari infrastruktur teknologi informasi berupa komponen dasar yang dibutuhkan untuk menjalankan sistem informasi yang digunakan oleh suatu organisasi. Contoh dari peralatan ini adalah komputer, server, peralatan aktif jaringan, dan peralatan telekomunikasi

2. Komponen penunjang

   Komponen penunjang adalah alat dan bahan yang dibutuhkan untuk menunjang peralatan utama dari teknologi informasi. Contoh dari komponen ini adalah tempat penyimpanan (ruang, lemari, serta pelindungnya), media penghubung (kabel), peralatan back up (Stavol, UPS), media penyimpanan, penyejuk ruangan, dan sebagainya

b. Brainware

Brainware adalah orang/pelaku yang berfungsi untuk menjalankan dan mengelolah teknologi informasi yang digunakan dalam organisasi. Pelaku atau orang ini memiliki beberapa fungsi yaitu sebagai operator atau administrator, dimana juga harus mendapat pengamanan secara fisik, karena merupakan aset/sumber daya yang sangat berguna bagi organisasi. Sebuah kecelakaan yang menimpa operator/administrator, bisa jadi membuat roda bisnis dari organisasi menjadi terhambat. Penyebab dari gangguan terhadap infrastruktur fisik teknologi informasi, bisa dibedakan menjadi 2 macam:

a. **Berasal dari gejala alam**

Kondisi lingkungan dan alam bisa menjadi penyebab terjadinya gangguan pada fisik infrastruktur teknologi informasi. Contoh dari kondisi lingkungan adalah gempa bumi, banjir, kelembaban udara. Kondisi lingkungan ini akan berakibat pada operasional normal dari peralatan yang ada. Pada peralatan bisa terjadi malfunction, atau bahkan tidak dapat bekerja sama sekali.

b. **Berasal dari tingkah manusia**

Perilaku manusia bisa menjadi penyebab dari gangguan terhadap fisik dari infrastruktur teknologi informasi, baik disengaja maupun tidak disengaja. Kelalaian merupakan tingkah laku tidak disengaja yang

bisa menyebabkan tidak berjalannya secara normal dari peralatan teknologi informasi. Pencurian, tidakan pengrusakan, dan sabotase merupakan tingkah laku yang disengaja untuk mengganggu fungsi normal dari peralatan fisik dari teknologi informasi.

Identifikasi dampak, lebih ditekankah apakah terdapat dampak terhadap aset maya dari organisasi. Aset maya ini berupa data-data penting yang dimiliki oleh organisasi. Pengrusakan dan pencurian terhadap perangkat penyimpan (internal maupun ekternal) bisa menyebabkan rusak dan hilangnya data-data yang terdapat pada media penyimpan tersebut.

2.3 Tahap Isolasi dan penahanan obyek (Containment)

Pada tahap ini dilakukan pengambilan dan penahanan terhadap peralatan fisik yang mengalami gangguan secara fisik. Metode yang digunakan dapat mencakup pemeriksaan terhadap pelaku pengrusakan, pencurian, atau vandalisme untuk mengetahui penyebab mereka melakukan hal itu.

Izin/pemberitahuan untuk melakukan penahanan

Hal pertama setelah konfirmasi keberadaan suatu gangguan adalah memberitahukan kepada personil untuk melakukan penahanan terhadap peralatan yang menjadi korban. Hal ini dilakukan apabila gangguan terjadi pada fisik komputer yang sedang digunakan. Pengguna komputer harus diberi tahu kalau komputernya sedang ditahan untuk keperluan penyelidikan terhadap kerusakan yang terjadi. Selama hal ini dilakukan, maka harus disediakan komputer/peralatan pengganti yang bias digunakan oleh personil yang bersangkutan.

Mengambil data-data hasil monitoring

Data-data dari hasil monitoring bisa digunakan untuk melakukan analisa dari penyebab gangguan yang terjadi pada infrastruktur fisik teknologi informasi. Data-data itu bisa meliputi data suhu dan kelembaban udara, data gambar dan suara dari CCTV pemantau, data pengunjung dari buku tamu, dan data-data perawatan dari peralatan. Apabila terdapat bukti adanya penyusup dari pihak luar organisasi yang telah melakukan pencurian dan pengrusakan, maka segera menghubungi pihak berwajib dari luar institusi untuk menangkap pelaku penyusupan.

Melakukan Investigasi terhadap anggota organisasi

Investigasi dilakukan dengan tujuan untuk mengumpulkan data-data yang berhubungan dengan kesalahan yang tidak disengaja maupun disengaja(human error) yang bisa menyebabkan gangguan terhadap fisik peralatan infrastruktur teknologi informasi. Apabila telah ditemukan bukti awal tindakan keterlibatan kejahatan (pencurian dan vandalism), maka segera menghubungi pihak bagian hukum dan pihak berwajib dari luar organisasi (kepolisian).

Melihat insiden yang pernah ada (Basis Pengetahuan)

Langkah selanjutnya setelah mengidentifikasi kerusakan fisik yang telah terjadi adalah menelusuri dokumen untuk mencari pengetahuan yang berisi insiden yang pernah terjadi di masa lalu. Jika insiden tersebut merupakan pengulangan, maka prosedur yang diikuti sebelumnya harus dieksekusi dan dianalisis secaramendalam pada setiap langkah untuk mengetahui penyebab terulangnya kejadian dan memastikan apakah langkah-langkah tersebut cukup atau tidak. Jika belum, maka diperlukan perbaikan secara utuh pada prosedur.

2.4 Tahap Elimanasi Penyebab/Gangguan (Eradication)

Tahap ini merupakan tahapan dimana penyebab dari gangguan dianalisa dan dihilangkan. Beberapa teknik yang berbeda-beda dapat digunakan untuk melakukan analisa terhadap gangguan fisik dan menghilangkan gangguan tersebut.

Memeriksa Data-data hasil monitoring

Pada fasilitas infrastruktur fisik teknologi informasi hendaknya terpasang peralatan-peralatan untuk melakukan monitoring terhadap

a. Kondisi lingkungan

Kondisi lingkungan berhubungan dengan temperatur, kelembaban, dan sirkulasi udara pada fasilitas penempatan dari peralatan fisik infrastruktur teknologi informasi. Kondisi lingkungan itu sangat berpengaruh terhadap kinerja peralatan. Setiap peralatan memiliki standar lingkungan tertentu untuk operasi normalnya. Jika kondisi tidak memenuhi standar, bisa jadi umur peralatan akan menjadi pendek.

b. Situasi lingkungan

Situasi lingkungan berhubungan dengan keluar masuknya dan keberadaan obyek dan pelaku (orang). Apabila terjadi kasus pencurian, pengrusakan, maka peralatan monitoring seperti CCTV yang bisa digunakan untuk merekam situasi lingkungan, dari data-data hasil monitoring ini akan diketahui siapa yang telah melakukannya.

Menemukan Penyebab

Tahap ini adalah kegiatan yang paling penting dan juga merupakan salah satu kegiatan terberat dalam tahap

pemberantasan. Penyebab insiden (gangguan) harus dapat ditemukan, sehingga insiden tidak akan terjadi di masa depan. Jika penyebab sudah ditemukan maka harus dilakukan penghilangan terhadap penyebab tersebut, dengan memberikan rekomendasi kepada pihak yang berwenang, misalnya

- Rekomendasi untuk melakukan perbaikan terhadap pengaturan suhu, kelembaban, dan sirkulasi udara dalam suatu ruang
- Rekomendasi untuk memperbaiki metode akses ke dalam suatu ruangan
- Rekomendasi pemberian sanksi terhadap pelaku pencurian dan pengrusakan

Meningkatkan Pertahanan

Setelah penyebab gangguan ditemukan, langkah selanjutnya adalah memperkuat pertahanan dan mencegah penyebab terjadinya gangguan tidak terulang kembali. Hal ini bisadilakukan dengan memodifikasi aturan akses terhadapfisik dari perangkat teknologi informasi.

2.5 Tahap Pemulihan (Recovery)

Tahap pemulihan merupakan tahap dimana peralatan fisik (utama maupun penunjang) yang mengalami gangguan, harus dipulihkan kembali kepada operasional normalnya.

Memperbaiki peralatan

Pada fase ini akan dilakukan perbaikan terhadap peralatan yang mengalami gangguan. Proses ini bisa membutuhkan waktu yang lama, apa lagi kalau tim teknis yang ada tidak mampu melakukan perbaikan internal. Peralatan harus dikirim keluar untuk dilakukan perbaikan. Tetapi apabila

terjadi kerusakan yang parah, atau peristiwa pencurian, maka peralatan tersebut harus diganti.
Organisasi sebaiknya menyediakan peralatan cadangan untuk kebutuhan mendesak.

Memperbaiki fasilitas
Pengrusakan dan vandalisme bisa terjadi pada fasilitas penempatan peralatan fisik infrastruktur teknologi informasi. Fasilitas ini harus segera diperbaiki untuk memastikan tidak terganggunya proses bisnis dari organisasi. Pada tahap ini, sistem yang telah pulih divalidasi oleh suatu tim teknis dan keputusan mengenai kapan memulihkan sistem operasi secara lengkap akan dibuat. Sistem ini dijaga dalam pengamatan, untuk memeriksa dan memastikan peralatan fisik dari infrastruktur teknologi informasi telah beroperasi normal dengan baik.

Valida sistem
Sistem yang telah pulih, harus divalidasi terhadap kesalahan atau kekurangan konfigurasi apapun. Jika ada kekurangan pada perangkat lunak atau data yang ditemukan, maka akan ditambahkan. Sebuah tanda tangan dari pengguna harus dibubuhkan untuk mengkonfirmasikan pemulihan lengkap dan normal dari sistem.

Pemulihan Operasi
Setelah validasi sistem pulih selesai, pemilik sistem memutuskan kapan untuk menempatkan sistem kembali bekerja normal. Rekomendasi mengenai keamanan sistem dapat diberikan kepada pemilik sistem. Pemilik harus mengakui rekomendasi ini melalui memo yang telah ditandatangani .

Pemantauan Sistem

Akhirnya aktifitas penting pada tahap pemulihan adalah melakukan pemantauan secara cermat agar tidak terjadi lagi gangguan pada peralatan fisik infrastruktur teknologi informasi.

2.6 Tahap Tindak Lanjut (Follow Up)

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk kebutuhan dimasa mendatang. Fase ini dapat memberikan masukan kepada tahap persiapan untuk meningkatkan pertahanan.

Penambahan pengetahuan dasar tentang penangan insiden

Salah satu hal penting yang harus dilakukan setelah berhasil menanganisebuah insiden adalah memperbarui pengetahuan. Catatan tentang penambahan pengetahuan ini harus ditambahkan pada dokumen laporan dan direview oleh semua pihak yang telah berperan dalam penanganan insiden. Hal ini akan membantu dalam penanganan insiden serupa di masa depan dengan mudah, efisien, dan cepat.

Pelatihan untuk tim penanganan insiden

Tim penanganan harus melatih semua tim penanganan lainnya dalam penanganan insiden infrastruktur fisik. Hal ini akan membantu mereka lebih memahami proses penanganan insiden dan juga membantu dalam menanggulangi insiden serupa di masa mendatang dengan lebih terampil.

Memperbarui aturan penjagaan

Semua jalan masuknya penyusup yang teridentifikasi harus cepat diblokir untuk mencegah masuk ke dalamarea terlarang. Hal ini dapat dilakukan dengan menambahkan aturan baru untuk memasuki suatu ruangan atau area tertentu (seperti sensor biometrik).

Peningkatan Pertahanan

Setelah penanganan selesai, Root Cause Analysis digunakan untuk menguatkan berbagai kendali terhadap sistem keamanan yang terdapat dalam perusahaan. Tim teknis dapat dibuat lebih peka dan menyadari terjadinya gejala gangguan fisik yang sama pada saat melakukan pemeriksaan suatu obyek, tim penanganan insiden dapat diberikan insiden serupa untuk melatih diri dan manajemen dapat memperkenalkan kontrol keamanan baru untuk mengurangi risiko di masa depan.

LAMPIRAN A - Informatif

Keamanan fisik infrastruktur Teknologi Informasi

Domain keamanan fisik membahas ancaman, kerawanan, dan tindakan yang dapat diambil untuk memberi perlindungan fisik terhadap sumber daya organisasi dan informasi yang sensitif. Sumber daya ini meliputi personel, fasilitas tempat mereka bekerja, data, peralatan, system pendukung, dan media yang mereka gunakan, Keamanan fisik sering mengacu pada tindakan yang diambil untuk melindungi sistem, gedung, dan infrastruktur pendukung yang terkait terhadap ancaman yang berhubungan dengan lingkungan fisik. Keamanan fisik computer dapat juga didefinisikan sebagai proses yang digunakan untuk mengontrol personel, bangunan fisik, peralatan, dan data yang terlibat dalam pengolahan informasi.

Pengamanan secara fisik adalah pengamanan terhadap suatu obyek agar obyek tersebut tidak mengalami gangguan ataupun kerusakan secara fisik. Disamping itu dapat pula diartikan sebagai pengamanan supaya obyek tidak tersentuh secara fisik, yang dapat menimbulkangangguan atau kerusakan terhadap obyek. Beberapa contoh ancaman yang dapat menimbulkan gangguan atau kerusakan secara fisik terhadap peralatan teknologi informasi:

Emergensi

- Kebakaran dan kontaminasi asap
- Kerusakan bangunan
- Kehilangan fasilitas utilitas /infrastruktur (listrik, AC, dan pemanas)
- Kerusakan jaringan air (perusakan Pipa)
- Limbah atau bahan beracun

Bencana alam

- Aktivitas pergerakan tanah (gempa, longsor)

- Kerusakan oleh badai (petir, banjir)

Intervensi Manusia

- Sabotase
- Perusakan
- Perang
- Pemogokan

Penempatan dan Konstruksi

Penempatan/Lokasi

Pemilihan lokasi bagunan mejadi hal yang harus diperhatikan. Hal-hal berikut dapat dijadikan bahan pertimbangan dari segi aspek keamanan dalam pemilihan lokasi. Lokasi yang dipilih sebaiknya yang memiliki sedikit resiko baik dari ancaman bencana alam (jalur gempa, daerah rawan banjir atau daerah rawan tornado) maupun dari ancaman teroris dan vandalisme.

Gedung untuk menempatkan peralatan utama teknologi informasi sebaiknya dibangun terpisah dari kantor pusat. Cukup jauh dari jalan raya utama,tidak dekat dengan bandar udara, pabrik kimia, jalur pipa gas, pusat keramaian (pasar, stadium olahraga) dan pusat pembangkit listrik. Dan juga lokasi memiliki fasilitas yang memadai, seperti kecukupan tenaga listrik. Lokasi lingkungan dari fasilitas juga menjadi pertimbangan dalam perencanaa awal.

Beberapa pertanyaan yang perlu dipertimbangkan di antaranya :

- Visibilitas

Berada pada lingkungan seperti apakah sebuah lokasi diajukan? Apakah lokasi tersebut memiliki penanda eksternal yang akan mencirikannya sebagai area yang sensitif? Visibilitas yang rendah adalah keharusan.

- Pertimbangan

Apakah tempat yang diajukan berlokasi dekat dengan sumber bahaya (misal tempat pembuangan sampah)? Apakah daerah tersebut memiliki tingkat kriminalitas tinggi?

- Bencana Alam

Apakah tempat tersebut memiliki kemungkinan terjadinya bencana alam yang lebih tinggi dibanding daerah lainnya? Bencana alam bisa termasuk kendala cuaca (angin, petir, banjir, dsb) dan keberadaan lempengan gempa bumi.

- Transportasi

Apakah lokasi tersebut memiliki masalah akibat lalu lintas darat, laut, atau udara yang berlebihan?

- Layanan Eksternal

Berapakah jarak lokasi dengan layanan emergensi, seperti polisi, pemadam kebakaran, rumah sakit, atau fasilitas medis?

Konstruksi Bangunan

Setelah memilih lokasi yang baik, selanjutnya harus memperhatikan bagunan yang akan didirikan untuk peralatan teknologi informasi. Bangunan harus memperhatikan masalah sirkulasi udara karena hal ini terkait dengan suhu dansirkulasi udara yang cukup. Biasanya bangunan untuk peralatan teknologi informasi dibuat dengan sedikit atau bahkan tidak ada jendela dan tertutup. Bahan bangunan yang dipakai harus tidak mudah terbakar serta menggunakan kontruksi bangunan yang tahan gempa. Terdapatnya ruangan terpisah antara ruangan administratif dengan ruangan server dan data. Menetapkan standar pendingin ruangan dan memperhatikan pengaturan kabel yang melalui bawah lantai. Konstruksi bangunan juga harus menyediakan jalur untuk kabel standar instalasi listrik yang dibutuhkan. Pintu masuk dirancang sangat terbatas,pintu darurat untuk peristiwa kebakaran dirancang untuk keluar saja. Kontruksi dan arsitektur bangunan harus dapat mengakomodasi semua hal berkaitan dengan keamanan fisik. Secara spesifik bisa dijabarkan sebagai berikut :

- Tembok

Keseluruhan tembok, dari lantai hingga langit-langit, harus memiliki standar keamanan terhadap kebakaran yang cukup.

Lemari atau ruangan yang dijadikan tempat penyimpanan media harus memiliki standar yang tinggi.

- Langit-langit

Masalah yang dipertimbangkan adalah standar kemampuan menahan beban dan standar keamanan terhadap kebakaran

- Lantai

Berikut ini adalah hal yang perlu diperhatikan mengenai lantai: Lempengan, Jika lantai adalah lempengan beton, pertimbangannya adalah beban yang sanggup didukung (disebut sebagai loading, yang biasanya adalah 150 pon per kaki persegi), dan ketahanannya terhadap api. Raised, ketahanannya terhadap api, dan materinya yang tidak menghantarkan listrik menjadi pertimbangan.

- Jendela

Jendela biasanya tidak dibuat pada sebuah data center. Jika ada, jendela harus tembus cahaya dan anti pecah.

- Pintu

Pintu pada fasilitas teknologi informasi harus tahan terhadap pembobolan, dan memiliki ketahanan terhadap api yang sama seperti pada tembok. Jalan keluar darurat harus dicirikan dengan jelas, terawasi/termonitor, dan beralarm. Ketika emergensi, kunci pintu elektrik harus dalam keadaan tidak dapat digunakan jika daya listrik lumpuh agar memungkinkan evakuasi yang aman. Meskipun hal ini dianggap sebagai masalah bagi keamanan, keselamatan personel harus didahulukan, dan pintu ini harus dijaga dalam keadaan darurat.

- Sumber Pemancar Air

Lokasi dan tipe sistem pemadaman api harus direncanakan, supaya ketika terjadi kebakaran, sumber air untuk pemadaman mudah didapat.

- Jaringan pipa dan gas

Katup pipa air dan gas di seluruh bangunan harus diketahui. Begitu pula drainase yang baik, yaitu yang mengalir ke luar

bangunan, sehingga tidak membawa zat kontaminan ke dalam bangunan

- AC

Sumber daya listrik untuk AC harus disediakan khusus, dan diketahui dimana lokasi saklar EPO (Emergency Power Off)-nya. Sebagaimana halnya drainase air, udara dari sistem pendingin harus mengalir keluar dengan tekanan udara yang positif, serta memiliki ventilasi yang melindungi fasilitas dari udara yang mengandung racun.

- Kebutuhan Kelistrikan

Fasilitas harus memiliki sumber daya listrik cadangan dan alternatif yang layak. Kontrol akses terhadap panel distribusi listrik harus dijaga.

Akses terhadap Fisik Fasilitas

Pengamanan disekeliling bangunan

Disekeliling bangunan tempat peralatan teknologi informasi seharusnya adalah bidang kosong, bangunan ini sebaiknya memiliki jarak ± 10 meter dengan bangunan lain atau tanaman dan pohon, hal ini dimaksudkan untuk memudahkan pengawasan. Dinding dan tembok yang ada disekitarnya harus dapat dimonitor dengan baik. Penggunaan kamera CCTV sebagai pengawas adalah hal minimal yang harus dilakukan. Selain itu juga kamera yang digunakan sebaiknya memiliki kemampuan terhadap cahaya rendah, tahan terhadap suhu dan cuaca.

Pengawasan pada area parkir sekitar fasilitas juga harus mendapat perhatian. Pengawasan orang yang masuk dan keluar di kawasan gedung fasilitas teknologi informasi harus dimonitor dengan baik. Penggunaan detektor bom perlu dilakukan untuk memeriksa setiap mobil yang masuk ke kawasan ini. Penggunaan penjaga atau petugas keamanan yang profesional merupakan sebuah hal yang harus dilakukan. Intinya jadikanlah bangunan fasilitas utama teknologi informasi sebagai sebuah

benteng yang harus memiliki pengamanan baik diluarnya, agar orang yang tidak berkepentingan tidak mudah untuk masuk kedalam bangunan.

Pengawasan personil

Pengawasan personil adalah pengawasan terhadap personil/karyawan yang akan mengakses fasilitas dari sistem Teknologi informasi. Beberapa elemen dibutuhkan untuk memelihara keamanan fisik terhadap akses personil

Penjaga

Penjaga merupakan bentuk tertua dari pengawasan keamanan. Penjaga masih memiliki fungsi yang sangat penting dan utama dalam proses keamanan fisik, terutama dalam kontrol garis batas (perimeter). Seorang penjaga dapat melakukan sesuatu dimana perangkat keamanan otomatis lain tidak dapat melakukannya karena kemampuannya untuk menyesuaikan diri dengan kondisi yang berubah dengan cepat, belajar dan mengubah pola-pola yang telah dikenali, dan merespon berbagai keadaan di lingkungan. Penjaga memiliki kemampuan menangkis, merespon, dan mengontrol, sebagai tambahan dari fungsi resepsionis dan pemandu.

Pagar

Pemagaran adalah sarana utama untuk mengendalikan akses yang merupakan garis batas luar(perimeter) fasilitas. Kategori pemagaran mencakup pagar, gerbang, pintu pagar, dan mantrap. Kelemahan dari pemagaran adalah biaya, penampilannya (yang mungkinburuk),dan ketidakmampuannya untuk menghentikan penyusup yang gigih.

Mantrap

Mantrap adalah metode kontrol terhadap akses fisik dimana pintu masuk diarahkan melalui pintu ganda yang dapat dimonitor oleh penjaga.

Pencahayaan

Pencahayaan juga merupakan bentuk umum dari perlindungan fisik. Pencahayaan yang kuat dan mengarah keluar di pintu masuk dan area parkir dapat menyurutkan pencuri dan penyusup. Gedung atau bangunan yang terproteksi dengan kritis harus disinari sampai ketinggian 8 kaki. Tipe-tipe umum pencahayaan mencakup floodlight, lampu jalan, fresnel light, dan lampu pencari.

CCTV (Closed-Circuit Television)

Pengawasan visual atau perangkat perekam seperti CCTV digunakan sebagai tambahan penjaga untuk meningkatkan kemampuan pengawasan dan merekam peristiwa untuk analisis di masa depan atau untuk kepentingan bukti kejahatan dan penuntutan. Perangkat ini bisa berupa fotografik seperti kamera foto atau kamera video, atau elektronik seperti kamera CCTV. CCTV dapat digunakan untuk memonitor peristiwa langsung yang terjadi di daerah yang jauh dari jangkauan penjaga, atau dapat digunakan bersama VCR sebagai metode yang
efektif dalam biaya untuk merekam peristiwa. Perlu diingat, bahwa memonitor peristiwa adalah tindakan pencegahan, dan merekam peristiwa dianggap sebagai tindakan pendeteksian

Perangkat Kontrol Akses Fasilitas

Perangkat ini merupakan kontrol akses personel terhadap fasilitas teknologi informasi. Perangkat-perangkat ini adalah sebagai berikut,

Kunci

Kunci mungkin menjadi salah satu metode kontrol akses yang pernah digunakan. Kunci akan diberikan kepada seseorang yang memang berhak untuk membuka/mengakses suatu fasilitas. Kunci dapat dibagi menjadi dua jenis: preset dan yang dapat diprogram (programmable)

- Kunci Preset

Ini adalah kunci pintu pada umumnya. Kombinasi untuk membuka tidak dapat diubah kecuali dengan menghilangkannya

secara fisik dan mengganti mekanisme internalnya. Ada beberapa variasi kunci preset, termasuk key-in- knob, mortise, dan rim lock. Semua ini terdiri dari berbagai gerendel, silinder, dan slot.

- Kunci Programmable

Kunci ini bisa berbasis mekanik ataupun elektronik. Kunci programmable yang mekanik sering berupa kunci putar kombinasi, seperti yang digunakan pada loker di arena olahraga. Jenis lain dari kunci programmable yang mekanik adalah kunci tombol lima-angka yang membutuhkan pengguna untuk memasukkan kombinasi angka. Kunci ini sangat populer untuk pusat operasi TI.

Kunci programmable yang elektronik membutuhkan pengguna untuk memasukkan pola angka digit pada keypad numerik, dan mungkin menampilkan digit secara random setiap kalinya untuk mencegah pengintip pola input. Ini juga dikenal sebagai kunci sandi atau kontrol akses keypad.

Kartu Akses Keamanan (Security Access Card)

Kartu akses keamanan adalah metode umum dalam kontrol akses fisik. Ada dua tipe umum kartu, kartu gambar foto dan kartu bersandi digital. Kedua grup kartu ini juga disebut sebagai kartu bodoh (dumb card) dan kartu pintar (smart card). Kartu bodoh membutuhkan penjaga untuk membuat keputusan mengenai keabsahannya, sementara kartu pintar membuat keputusan masuk secara elektronik.

- Kartu berfoto (Photo-Image Card)

Kartu berfoto adalah kartu identifikasi yang sederhana dengan adanya foto pemegang kartu sebagai alat identifikasinya. Otentikasi dan otorisasi dilakukan dengan menunjukkan kartu ini kepada penjaga, keputusan dilakukan oleh personel di pintu masuk sebagai otentikasi

- Kartu Sandi Digital (Digital-Coded Card)

Kartu sandi digital mengandung chip atau sandi garis magnetik (sebagai tambahan atas foto pemegang kartu). Pembaca kartu

dapat diprogram untuk menerima akses berdasarkan komputer kontrol akses online yang juga menyediakan informasi mengenai tanggal dan waktu akses masuk. Kartu jenis ini juga bisa membuat pengelompokan akses banyak tingkat. Ada dua bentuk umum kartu sandi digital, yaitu smart card dan smarter card. Kartu smart card memiliki kode garis magnetik atau chip IC (Integrated Circuit) kecil yang tertanam di dalamnya. Penggunaan kartu ini membutuhkan pengetahuan password atau PIN (Personal Identification Number) untuk mendapat akses masuk. Dalam beberapa skenario kartu smart card dapat dipasangkan dengan token otentikasi yang membangkitkan password atau PIN yang sekali pakai (one-time) atau berupa challenge-response. Sementara otentikasi dual- factor paling banyak digunakan untuk akses logik layanan jaringan, kartu smart card bisa dikombinasikan dengan card reader yang pintar untuk menyediakan kontrol yang sangat kuat terhadap akses fasilitas.

- Wireless Proximity Reader

Proximity reader tidak membutuhkan pengguna untuk memasukkan kartu. Kartu ini juga biasa disebut sebagai wireless security card. Card reader mengindra kartu milik pengguna di area umum pada jarak atau kedekatan tertentu dan membolehkan akses

Perangkat Biometrik

Alternatif lain dari penggunaan password atau kartu identitas dalam kontrol akses secara lojik

maupun teknis adalah biometrik. Biometrik didasarkan pada faktor atau tipe ketiga dalam mekanisme otentikasi : siapa diri Anda (something you are). Biometrik didefinisikan sebagai alat otomasi untuk mengidentifikasi dan mengotentikasi identitas seseorang berdasarkan ciri- ciri fisiologis atau kebiasaan. Berikut ini adalah ciri-ciri biometrik yang umum digunakan untuk mengotentikasi identitas seseorang:

- Sidik jari
- Pemindai retina (retina scan)
- Pemindai iris (iris scan)
- Pemindai wajah (facial scan)
- Pemindai telapak tangan (palm scan)
- Geometri tangan
- Suara
- Pengenal tanda tangan (handwritten signature dynamics)

Pengamanan didalam bangunan

Pengamanan didalam bangunan dilakukan dengan tujuan untuk mendeteksi adanya penyusup(manusia) yang bisa mengancam secara fisik terhadap fasilitas teknologi informasi. Penggunaan kamera pengawas dan detektor penyusup merupakan hal standar yang harus diterapkan. Pendeteksian penyusup mengacu pada proses identifikasi usaha masuk ke dalam sistem atau gedung untuk memperoleh akses tak berwenang. Detektor Penyusup Area merupakan sistem yang bisa terdiri dari

1. Detektor Gerak

Detektor gerak digunakan untuk mengindra pergerakan yang tidak umum di dalam sebuah area keamanan. Bila terjadi pergerakkan yang tidak umum detekteor akan mengaktifkan sistem peringatan atau alarm. Perangkat ini dapat digolongkan menjadi tiga golongan: detektor gerak pola gelombang, detektor kapasitansi, dan alat amplifikasi audio.

2. Detektor Suara.

Detektor suara dalah alat yang pasif, dalam arti alat ini tidak membangkitkan medan atau pola apapun seperti halnya dua metode sebelumnya. Detektor suara hanya memonitor ruangan dari gelombang suara yang tidak normal dan membangkitkan alarm. Tipe pendeteksian seperti ini mempunyai angka kesalahan alarm yang lebih tinggi dari dua metode sebelumnya dan seharusnya digunakan pada area yang tidak memiliki banyak gangguan suara.

3. Sistem Alarm.
Perangkat deteksi yang telah disebutkan di atas memonitor dan melaporkan perubahan spesifik pada lingkungan. Detektor ini dapat dipasangkan bersama untuk menciptakan sebuah sistem alarm. Ada empat tipe umum sistem alarm:
- Sistem Alarm Lokal. Sebuah sistem alarm lokal membunyikan alarm yang dapat didengar di tempat yang dilindunginya. Alarm ini harus dilindungi dari perusakan dan harus dapat didengar pada jarak paling sedikit 400 kaki (130 meter). Sistem ini juga membutuhkan penjaga untuk bereaksi secara lokal terhadap penyusupan.
- Sistem Stasiun Pusat. Perusahaan keamanan swasta mengoperasikan sistem ini yang memonitor sepanjang waktu. Stasiun pusat dikirimkan sinyal oleh detektor melalui leased line. Stasiun ini biasanya menawarkan beberapa fitur tambahan, seperti monitor CCTV dan laporan cetakan, dan lokasi yang diamankan berjarak kurang dari 10 menit perjalanan dari kantor monitoring pusat.
- Sistem Propietary. Sistem ini serupa dengan sistem stasiun pusat, hanya saja
sistem monitoringnya dimiliki dan dioperasikan oleh pemilik. Sistem ini mirip dengan sistem alarm lokal, hanya saja sistem komputer yang canggih menyediakan banyak fitur yang disediakan seperti halnya sistem stasiun pusat.
- Sistem Stasiun Auxiliary. Ketiga sistem sebelumnya dapat memiliki sistem
alarm auxiliary (penolong) yang berbunyi pada kantor polisi atau kantor pemadam kebakaransetempat. Sebagian besar sistem stasiun pusat memiliki mencakup sistem ini, yang membutuhkan izin dari otoritas setempat sebelum pengimplementasiannya

Antisipasi Kondisi Lingkungan
Suhu

Peralatan komputer dan jaringan untuk sistem teknologi informasi sangat rentan terhadap temperatur yang tinggi. Oleh sebab itu penggunaan sensor suhu yang diletakkan di rack server menjadi sebuah solusi untuk mengendalikan suhu. Selain memperhatikan panas pada server, yang perlu diperhatikan adalah suhu ruangan. Untuk itu diperlukan sistem pendingin yang baik. Sejak mulai awal pembangunan fasilitas teknologi informasi hendaknya sudah diperhitungkan berapa kapasitas yang diperlukan untuk membuat ruangan tetap dingin, sehingga tidak kesulitan dalam menghitung listrik yang dibutuhkan. Meningkatnya suhu dapat diatasi dengan penambahan AC, namun akan dapat menimbulkan masalah karena membutuhkan listrik yang cukup besar.

Ada beberapa pendekatan yang dikembangkan untuk menghitung besarnya kebutuhan pendinginan. Pada dasarnya hal ini bergantung dari banyaknya jumlah peralatan yang ada didalam ruang komputer yang harus didinginkan. Cara sederhananya mungkin dengan melihat kapasitas ruangan yang dapat menampung berapa banyak rack server kemudian dari hal tersebut dapat diperkirakan berapa kebutuhan pendinginan yang diperlukan.

Sebuah teknologi baru yang dapat diterapkan untuk menyesuaikan kapasitas pendinginan dengan kebutuhan ruang komputer. Lantai terbaru meningkatkan ketepatan sistem pendingin yang secara otomatis menyesuaikan kapasitas dengan kebutuhan ruangan tanpa memutar kompresor dan meningkatkan efisiensi dan realibilitas. Hal ini memungkinkan peningkatan kapasitas ekstra dalam sistem tanpa peningkatan dalam biaya energi. Keuntungan menggunakan pre-piping adalah kemudahan untuk menambahkan atau memindahkan model

pendingin, selain itu juga realibilitas akan dapat tercapai.

Listrik/Tenaga

Kebutuhan listrik merupakan hal yang penting pada sebuah fasilitas teknologi informasi. Karena semua peralatan komputer, peralatan komunikasi dan jaringan serta pendingin membutuhkan energi. Selain itu juga penggunaan listrik cadangan seperti Genset dan UPS harus dilakukan. UPS yang digunakan harus memenuhi kebutuhan listrik dari semuaperalatan yang ada. Batere UPS diharapkan dapat bertahan cukup lama sebelum digantikan dengan listrik cadangan dari Genset.

Sekarang ini telah timbul semacam pandangan untuk mengurangi konsumsi energi pada sebuah infrastruktur TI, misalnya penggunaan teknologi pendingin terbaru, penggunaan energi lain seperti matahari atau hidrogen. Teknologi untuk hal ini masih terus dikembangkan seiring dengan kesadaran para manajer untuk lebih mengefisiensikan konsumsi energi di sebuah data center.

Pengawasan lingkungan yang tidak benar atau utilitas lingkungan yang tak diawasi bisa menyebabkan kerusakan layanan, perangkat keras, dan hidup itu sendiri. Layanan sistem dapat terganggu yang mengakibatkan hasil yang tidak diramalkan atau diperkirakan sebelumnya. Daya listrik, heating, ventilasi, pengaturan suhu udara (AC), dan kontrol mutu udara akan menjadi kompleks dan terdiri dari banyak variabel. Semuanya perlu dioperasikan
dengan semestinya dan diamati secara teratur.

Selama pembuatan fasilitas, harus dipastikan bahwa katup air, uap, dan jalur gas dalam keadaan shutoff, dan positive drains, yang berarti isinya akan mengalir keluar area. Bila ada gangguan di pipa air utama, aliran air harus dapat dimatikan. Kalaupun terjadi banjir disekitarnya, perusahaan ingin memastikan bahwa tidak ada fasilitas yang terendam air. Bila ada api didalam gedung, jalur gas harus dapat dihentikan. Bagian fasilitas, operasi, dan keamanan sebaiknya tahu di mana katup tersebut dan sebaiknya ada prosedur yang jelas untuk

diikuti bila terjadi keadaan darurat. Hal ini akan membantu mengurangi kerusakan yang mungkin terjadi secara keseluruhan akibat bencana yang terjadi.

Kebanyakan perlengkapan elektronik harus beroperasi dalam suasana iklim yang terkontrol. Walaupun penting untuk menjaga suasana kerja dalam suhu yang baik, perlu juga dimengerti bahwa ada komponen di dalam perlengkapan akan bermasalah bila mendapat panas berlebih.Sering kali kipas internal komputer dalam keadaan kotor atau mampet, sehingga bagian dalam komputer mengalami panas secara berlebihan. Bila perangkat terlalu panas, ada bagian yang dapat memuai, yang berakibat sifat elektroniknya berubah, mengurangi keefektifan atau bahkan merusak kerja sistem secara keseluruhan.

Memelihara tingkat suhu dan kelembaban yang baik, penting di bagian fasilitas yang mana pun, terutama fasilitas sistem komputer. Karena bila kedua hal tersebut tidak diperhatikan, bisa menyebabkan kerusakan pada komputer dan alat listrik. Kelembaban tinggi bisa menyebabkan korosi dan kelembaban rendah bisa menyebabkan listrik statis berlebihan. Kelembaban relatif antara 45 sampai 60 persen dapat diterima untuk area yang berfungsi mengolah data.

Suhu lebih rendah bisa membuat mekanisme menjadi lambat atau berhenti, dan suhu yang lebih tinggi bisa membuat alat menggunakan terlalu banyak daya kipas/fan dan akhirnya shutdown. Suhu di area yang berisi peralatan komputer sebaiknya pada tingkat 70 dan 74 derajat Fahrenheit. Di iklim yang lebih kering, atau selama musim dingin, udara hanya berisi sedikit embun, yang bisa mengakibatkan listrik statis bila dua objek berbeda saling bersentuhan. Listrik ini biasanya mengalir lewat badan dari peralatan dan mengeluarkan kilatan yang bisa melepaskan beberapa ribu volt. Ini bisa mengakibakan kerusakan lebih dari yang terpikirkan. Biasanya arus listrik dilepaskan di atas sistem casing, tetapi bila dilepaskan langsung ke komponen dalam, akibatnya bisa lebih buruk. Oleh

karena itu mengapa orang yang bekerja di bagian internal komputer biasanya memakai lengan anti-static untuk mengurangi kontak langsung.

Di iklim yang lebih lembab, atau selama musim panas, kelembaban tinggi di udara juga bisa mempengaruhi komponen. Partikel bisa berpindah dari konektor ke kontak tembaga, dimana semen konektor ke dalam stopkontak. Hal ini bisa mempengaruhi efisiensi hubungan listrik. Hygrometer biasanya digunakan untuk memantau kelembaban. Informasi dapat dibaca secara manual atau dipasang alarm-off otomatis jika kelembaban mencapai batas ambang tertentu.

Ventilasi

Ventilasi udara mempunyai beberapa syarat untuk membantu memberikan lingkungan aman dan nyaman. Sistem pengaturan suhu sirkulasi tertutup harus dipasang untuk memelihara kualitas udara. Tekanan udara positif dan ventilasi juga sebaiknya diimplementasi untuk mengawasi pencemaran/kontaminasi. Tekanan udara positif/positive pressurization artinya bahwa kalau seorang pegawai membuka pintu, udara akan keluar dan udara luar tidak masuk. Pengetahuan terhadap bagaimana kontaminan memasuki lingkungan, kerusakan yang terjadi, dan langkah untuk menjamin bahwa fasilitas terlindung dari bahan berbahaya dengan kadar tinggi yang melebihi rata-rata kontaminan. Bahan yang dapat mengudara dan konsentrasi partikel harus diamati bila mencapai tingkat yang tak seharusnya. Debu bisa menyumbat fan/kipas yang berfungsi untuk menyejukkan suhu peralatan. Konsentrasi gas yang berlebihan bisa mempercepat korosi dan menyebabkan masalah performance atau kegagalan perangkat elektronik. Walaupun kebanyakan disk drives ditutup rapat, alat penyimpanan lain bisa dipengaruhi oleh kontaminan yang berada dalam udara. Perangkat penjaga kualitas udara dan sistem ventilasi cocok untuk persoalan ini.

Pencegahan, Deteksi, dan Pemadaman api

Masalah keamanan fisik tidak akan lengkap bila tidak membahas mengenai fire safety. Ada standar lokal dan standar nasional yang harus dipenuhi untuk metode pencegahan, deteksi, dan pemadam api. Pencegahan kebakaran dimulai dengan pemberian latihan kepada pegawai bagaimana caranya untuk bereaksi dengan semestinya kalau menghadapi api, menyediakan perlengkapan yang benar dan jaminan bahwa perlengkapan itu bekerja dengan baik, meyakinkan ada persediaan air yang mudah dicapai, dan menyimpan elemen yang mudah terbakar di tempat tertentu.

Sistem respon pendeteksi api terdiri dari bentuk yang berbeda. Ada the red manual pull boxes yang dapat kita lihat di banyak tembok gedung perusahaan. Ada detektor yang otomatis, mempunyai sensors yang bereaksi kalau mereka mengetahui adanya api. Sistem otomatis bisa berupa sistem alat penyembur (sprinkler system) atau Halon discharge system. Automatic sprinkler system secara luas dipakai dan sangat efektif untuk melindungi gedung dan isinya. Ketika memutuskan tipe sistem pemadam api mana yang akan dipasang, banyak faktor yang perlu dievaluasi termasuk perkiraan tingkat kemungkinan terjadinya kebakaran, banyaknya kerusakan yang diakibatkan, dan tipe sistem mana yang akan dipilih.

Perlindungan terhadap api terdiri atas deteksi asap awal dan shutdown sistem sampai sumber panas dapat dihilangkan sehingga kebakaran tidak terjadi. Jika perlu, sistem otomatis sebaiknya men-shutdown semua sistem. Tanda peringatan terlebih dulu berbunyi dan menahan tombol yang ada untuk menunda proses shutdown bila masalah dapat diatasi dan bahaya sudah terlewati.

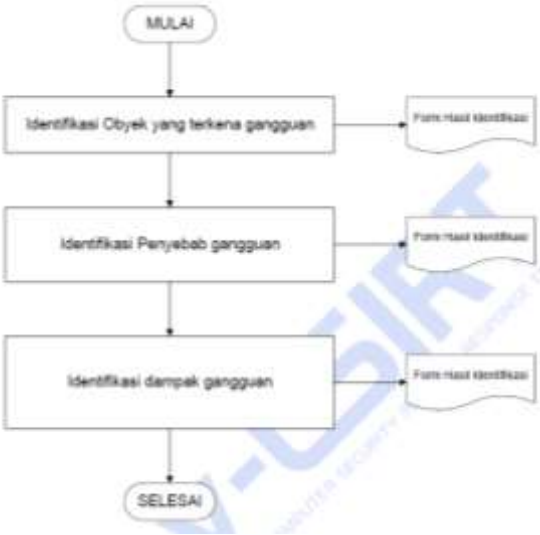
Kebakaran api menimbulkan ancaman keamanan yang sangat berbahaya karena api bisa merusak perangkat keras, data, dan resiko hidup manusia. Asap, suhu tinggi, dan gas korosif dari api

bisa menyebabkan kehancuran; dengan begitu, penting mengevaluasi ukuran keamanan api terhadap gedung dan bagian-bagiannya. Kebakaran api dimulai karena sesuatu sebagai sumbernya. Sumber nyala bisa terjadi karena kegagalan alat listrik, penyimpanan tidak patut dari bahan yang mudah terbakar, membuang rokok sembarangan, panas yang tinggi dari perangkat yang gagal fungsi, dan pembakaran yang disengaja. Api memerlukan bahan bakar dan oksigen untuk terus membakar dan bertambah besar; lebih banyak bahan bakar permeter persegi, lebih hebat api akan menjadi. Fasilitas sebaiknya dibuat, dipelihara, dan dijalankan dengan sesedikit mungkin penumpukan bahan bakar yang bisa mengakibatkan kebakaran.

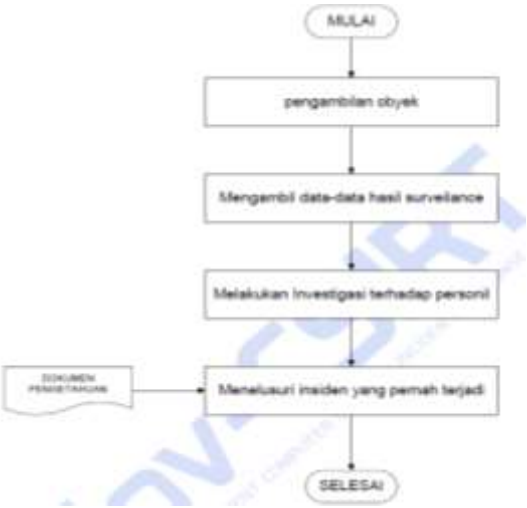
Ada tiga kelas (A, B, dan C) api yang mungkin terjadi. Penting diketahui perbedaan di antara tipe api sehingga kita tahu bagaimana cara untuk membedakannya. Alat pemadam api mempunyai tanda yang menunjukkan alat tersebut dipakai untuk tipe api tertentu. Tanda menunjukkan jenis bahan kimia didalam teromol dan tipe api yang dapat dipadamkan. Alat pemadam yang mudah dibawa biasanya diisi dengan karbon dioksida (CO_2) atau asam soda dan sebaiknya ditempatkan dalam radius 50 kaki dari perlengkapan listrik yang mana pun dan dapat ditemukan dekat jalan keluar. Alat pemadam sebaiknya ditandai secara jelas, dengan pandangan yang tak terhalang. Peralatan itu sebaiknya dengan mudah dapat dicapai dan mudah dioperasikan oleh pegawai, dan diperiksa setiap bulan.

LAMPIRAN B – Diagram Alir

LANGKAH-LANGKAH PADA TAHAP PERSIAPAN



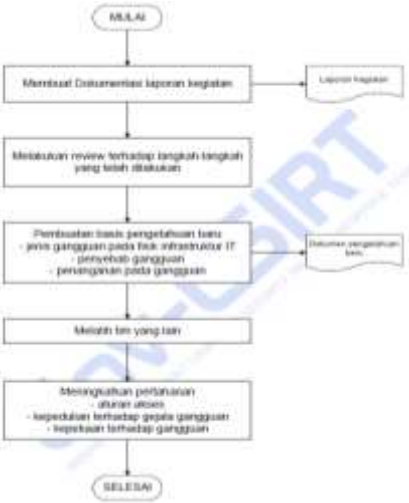
LANGKAH-LANGKAH PADA TAHAP IDENTIFIKASI



LANGKAH-LANGKAH PADA TAHAP CONTAINMENT

LANGKAH-LANGKAH PADA TAHAP ERADICATION

LANGKAH-LANGKAH PADA TAHAP RECOVERY



LANGKAH-LANGKAH PADA TAHAP TINDAK LANJUT

LAMPIRAN C – Formulir

Formulir Laporan penanganan insiden

1. Informasi Pembuat Laporan	
Nama Lengkap	
Jabatan pada tim	
Internal/External	
Nama Institusi (external)	
Nomor Telepon tempat kerja	
Nomor HP	
Alamat E-mail	
Nomor Fax	
Informasi tambahan :	

3. Jenis insiden : fisik Nomor Insiden :	
□ Akses ilegal □ Kerusakan peralatan utama □ Kerusakan peralatan pendukung □ Hilangnya peralatan	□ Bencana Alam
Deskripsi singkat insiden :	

3. Cakupan dari insiden (pilih salah satu)	
☐ Kritis (misal, berpengaruh pada sumber daya informasi yang membahayakan keamanan umum secara luas di luar institusi/lembaga) ☐ Besar (misal, berpengaruh pada seluruh jaringan dan/atau sistem bisnis utama dari institusi/lembaga) ☐ Sedang (misal, hanya berpengaruh pada infrastruktur jaringan, server, atau akun admin pada institusi/lembaga) ☐ Kecil (misal, hanya berpengaruh pada komputer atau akun pengguna pada institusi/lembaga)	
Perkiraan jumlah sistem yang terkena dampak:	
Perkiraan jumlah pengguna yang terkena dampak:	
Pihak ketiga yang terkena dampak: (misal: vendor, kontraktor, partner)	
Informasi tambahan dari cakupan insiden:	

4. Dampak dari insiden	
☐ Berhenti/hilangnya layanan ☐ Berhenti/hilangnya produktifitas ☐ Hilangnya reputasi ☐ Berkurang/hilangnya pendapatan	☐ Penjalaran ke jaringan lain ☐ Pengungkapan tidak sah dari data/informasi ☐ Pengubahan tidak sah dari data/informasi ☐ Lainnya, _____
Informasi lain dari dampak insiden:	

5. Sensitivitas dari data yang terkena insiden	
☐ Data/info rahasia/sensitiv ☐ Data/info Non-sensitive ☐ Data/info yang disediakan untuk publik ☐ Data/info keuangan	☐ Informasi Identitas Pribadi Personil ☐ Data/info tentang HAKI/*copyrighted* ☐ Data/info tentang *critical infrastructure*/*key resources* ☐ Lainnya, _____
Data dienkripsi ? Ya ____ tidak ____	
Besarnya data/informasi yang terkena insiden:	
(ukuran file, jumlah record)	
Informasi tambahan:	

6. Sistem yang terkena insiden	
Sumber serangan (alamat IP, port):	
Tujuan serangan (alamat IP, port):	
Alamat IP dari sistem:	
Nama Domain dari sistem:	
Fungsi dari sistem : (web server, domain controller)	
Sistem Operasi dari sistem: (version, service pack, configuration)	
Level Patching dari sistem : (latest patches loaded, hotfixes)	
Perangkat lunak security pada sistem: (anti-virus, anti-spyware, firewall, versions, date of latest definitions)	
Lokasi fisik dari sistem: (ampimo, suite, gedung,lisong,meja/rak/lemari)	
Informasi/ tambahan dari sistem:	

7. Pengguna yang terkena dampak	
Nama dan jenis pekerjaan pengguna:	
Level hak akses dari pengguna: (regular user, domain administrator, root)	
Informasi/ tambahan pengguna:	

8. Timeline dari insiden	
Tanggal dan waktu kejadian pertama kali terdeteksi, ditemukan, atau diberitahu tentang insiden itu:	
Tanggal dan waktu saat kejadian yang sebenarnya terjadi (perkiraan, jika tanggal dan waktu yang tepat tidak diketahui):	
Tanggal dan waktu ketika insiden itu ditangani atau ketika semua sistem/fungsi telah dipulihkan (menggunakan tanggal dan waktu terlambat):	
Tanggang waktu antara penemuan dan kejadian : Tanggang waktu antara penemuan dan pemulihan :	
Keterangan tambahan:	

9. Pemulihan dari insiden	
Tindakan yang dilakukan untuk mengidentifikasi sumber daya yang terkena dampak: Tindakan yang dilakukan untuk memulihkan insiden: Rencana tindakan untuk mencegah terulangnya insiden:	