ANALISIS PENERAPAN SISTEM KEAMANAN FISIK PADA DATA CENTER UNTUK MELINDUNGI DATA ORGANISASI

(Studi Kasus Pada Unit Penerimaan Mahasiswa Baru Dan Sistem Informasi (PMBSI) IKIP PGRI MADIUN)

Digky Bima Priatmoko
Endang Siti Astuti
Riyadi
Fakultas Ilmu Administrasi
Universitas Brawijaya
Malang
digkybima@gmail.com

ABSTRACT

Physical security is an aspect that is seen can not be measured by the amount of money (intangible) but the actual losses incurred from a weak security system can be calculated in the amount of money. Management can calculate the amount of losses incurred, such a loss when data loss can direpesentasikan of the total cost required for the recovery of lost data. This study uses data collection techniques through media direct field observations, interviews, and documentation on several sources or informants at the Teachers' Training College PGRI Madiun. From the research process is to be obtained the following data Implementation of the system's security physical at Data Center Teachers 'Training College PGRI Madiun has been progressing quite positive after the formation PMBSI, and the application of physical security at Data Center Teachers' Training College PGRI Madiun basically able to protect, but still there is a facility that must be repaired.

Keywords: Physical Security Systems , Data Center, Data Organization

ABSTRAK

Keamanan fisik merupakan aspek yang terlihat tidak dapat diukur dengan besaran uang (intangible) namun sebenarnya kerugian yang ditimbulkan dari sistem keamanan yang lemah dapat dihitung dalam besaran uang. Manajemen dapat menghitung besarnya kerugian yang ditimbulkan, contohnya kerugian saat kehilangan data dapat direpesentasikan dari jumlah biaya yang dibutuhkan untuk recovery data yang hilang tersebut. Penelitian ini menggunakan teknik pengumpulan data melalui media observasi lapangan langsung, wawancara, dan dokumentasi pada beberapa sumber atau informan di IKIP PGRI Madiun. Dari proses penelitian yang dilakukan diperoleh data sebagai berikut Penerapan sistem keamananan fisik pada Data Center IKIP PGRI Madiun sudah mengalami perkembangan yang cukup positif setelah dibentuknya PMBSI dan penerapan sistem keamanan fisik pada Data Center IKIP PGRI Madiun pada dasarnya mampu untuk melindungi namun masih terdapat fasilitas yang harus diperbaiki.

Kata kunci : ***Sistem Keamanan Fisik, Data Center, Data Organisasi***

PENDAHULUAN

Informasi merupakan data yang telah diklasifikasikan atau diolah atau di interpretasikan untuk digunakan dalam proses pengambilan keputusan (Sutabri, 2005:23). Informasi adalah aset penting yang dimiliki oleh sebuah organisasi dalam rangka memelihara kelangsungan hidup suatu organisasi bisnis dan memelihara kepercayaan publik atau konsumen. Pentingnya informasi mengharuskan manajemen menjaga ketersediaan, ketepatan dan keutuhan informasi yang dimiliki oleh suatu organisasi. Informasi yang bersifat sangat penting hanya boleh diakses oleh pihak-pihak yang memiliki wewenang atas informasi tersebut. Apabila informasi dapat diakses oleh pihak-pihak yang berpotensi menyalahgunakan informasi tersebut, hal ini akan menjadi sebuah kerugian bagi organisasi. Manajemen pengelolaan informasi perlu diterapkan untuk melindungi kerahasiaan, integritas dan ketersediaan informasi yang dimiliki oleh sebuah organisasi, terutama informasi yang menyangkut kepentingan banyak pihak.

Organisasi menggunakan sistem terkomputerisasi yang terintegrasi agar data yang dibutuhkan dapat diproses dengan efektif dan efisien. Keamanan informasi dan data elektronik menjadi hal yang sangat penting di berbagai organisasi maupun perusahaan, seperti perusahaan eksport-import, transportasi, lembaga pendidikan, pemberitaan, hingga perbankan yang menggunakan fasilitas teknologi informasi dan menempatkannya sebagai infrastruktur penting dalam menjaga informasi yang dimiliki oleh organisasi. Keamanan pada hakikatnya adalah keadaan bebas dari bahaya seperti hubungan pada kejahatan, segala bentuk kecelakaan, dan lain-lain, karena dengan semakin banyak informasi yang disimpan, dikelola dan dipublikasi maka semakin besar pula resiko terjadinya kerusakan, kehilangan atau terekspsosnya data ke pihak luar yang tidak diinginkan.

Keamanan informasi terdiri dari perlindungan terhadap beberapa aspek. Aspek pertama adalah *Confidentality* (kerahasiaan), yaitu aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang, dan menjamin kerahasiaan data yang dikirim, diterima serta disimpan. Aspek berikutnya adalah *Integrity* (integritas), yaitu aspek yang menjamin bahwa data tidak di ubah tanpa ada ijin pihak yang berwenang *(authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek *integrity* ini. Aspek terakhir adalah *Availability* (ketersediaan), yaitu aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

Keamanan informasi pada umumnya dapat ditinjau dari dua sisi, yang pertama adalah physical *security* atau keamanan fisik yang meliputi bagaimana keamanan fisik sebuah data *center* dapat terjaga dengan baik dan yang kedua adalah *cyber security* atau keamanan non-fisik yang meliputi bagaimana data center aman dari hal hal non-fisik seperti serangan hacker, virus, *malware, denial of service attack*, dll. Pada perkembangan awal sistem keamanan informasi, keamanan fisik sering dianggap tidak penting dan diabaikan, mereka akan lebih mewaspadai ancaman hacker, virus, dan *cyber terrorist,* padahal pegawai yang tidak puas, pencuri, vandalism, dan musuh perusahaan dapat menimbulkan kerusakan fisik yang mungkin akan lebih susah untuk diperbaiki daripada serangan hacker atau malware dan akan lebih banyak pengeluaran dari segi biaya untuk memperbaikinya. Pada praktiknya*, cyber security* yang baik harus diimbangi dengan *physical security* yang memadai agar keamanan informasi terjaga. Keamanan fisik merupakan keamanan tahap awal dari *computer security*. Jika keamanan fisik tidak terjaga dengan baik, maka data-data bahkan *hardware computer* sendiri, tidak dapat diamankan (Ariyus, 2006:6).

Pandangan mengenai keamanan fisik mengalami perubahan ketika terjadi beberapa kasus yang mengancam keamanan fisik itu sendiri seperti terjadinya pencurian fisik data-data organisasi. Faktor lain yang mengubah pandangan manajemen organisasi mengenai pentingnya menjaga keamanan fisik yaitu terjadinya bencana alam. Manajemen harus menjaga data agar tetap aman jika terjadi bencana alam sekaligus strategi pemulihan setelah terjadi bencana. "*Controls in physical security can be partitioned into physical, technical and administrative types*" (Cole, Krutz, dan Conley, 68:2005). *Physical controls* merupakan implementasi dari batasan-batasan keamanan dalam sebuah struktur yang telah ditetapkan untuk mencegah atau menghalangi *unauthorized access* terhadap material yang dianggap penting. Contoh dari *physical controls* adalah penjaga, pagar, lampu, kunci, CCTV dan alarm. *Technical controls* menggunakan teknologi sebagai dasar untuk

melakukan pengawasan terhadap penggunaan data yang dianggap penting. *Technical controls* meliputi *smart cards* dan *biometric. Administrative controls* terdiri dari pembatasan wewenang, prosedur operasional, prosedur akuntabilitas, dan pembuatan pengawasan administrasi tambahan untuk memberikan perlindungan bagi sumber-sumber informasi.

Keamanan fisik merupakan aspek yang terlihat tidak dapat diukur dengan besaran uang (intangible) namun sebenarnya kerugian yang ditimbulkan dari sistem keamanan yang lemah dapat dihitung dalam besaran uang. Manajemen dapat menghitung besarnya kerugian yang ditimbulkan, contohnya kerugian saat kehilangan data dapat direpesentasikan dari jumlah biaya yang dibutuhkan untuk recovery data yang hilang tersebut. Reputasi sebuah instansi atau organisasi juga dapat turun apabila sering terjadi security insident dalam kegiatan operasional dan manajemennya.

Pentingnya keamanan fisik bagi lembaga pendidikan, khususnya perguruan tinggi, membuat peneliti berminat melakukan penelitian mengenai hal tersebut. Dalam penelitian ini, peneliti menentukan PMBSI IKIP PGRI Madiun sebagai obyek penelitian. IKIP PGRI Madiun merupakan sebuah perguruan tinggi swasta di Jawa Timur yang pada bulan Mei 2015 mendapatkan dua penghargaan sekaligus, yaitu sebagai Perguruan Tinggi Unggulan (Kelompok Institut) dan predikat sebagai Perguruan Tinggi Utama Kopertis Wilayah VII Jawa Timur. Prestasi sebagai Perguruan Tinggi Unggulan untuk kelompok institusi merupakan penghargaan kedelapan yang diterima oleh IKIP PGRI MADIUN mulai tahun 2008 berturut-turut setiap tahun hingga tahun 2015. IKIP PGRI MADIUN juga berencana dalam waktu dekat dapat bertransformasi menjadi Universitas PGRI Madiun. PMBSI adalah Unit Penerimaan Mahasiswa Baru dan Sistem Informasi (PMBSI) IKIP PGRI Madiun, merupakan sebuah unit khusus, yang selanjutnya di berikan kepercayaan untuk dapat bergerak dalam pengembangan dan penerapan penerimaan mahasiswa baru dan sistem informasi. Dibentuk secara khusus oleh IKIP PGRI Madiun pada tahun 2015 sebagai bentuk keseriusan IKIP PGRI Madiun dalam pengembangan dan penerapan penerimaan mahasiswa baru dan sistem informasi. Tujuan dalam penelitian ini yaitu mendeskripsikan penerapan Sistem Keamanan Fisik pada data center PMBSI IKIP PGRI Madiun dan menganalisis apakah penerapan Sistem Keamanan Fisik pada data center mampu melindungi data organisasi milik PMBSI IKIP PGRI Madiun.

KAJIAN PUSTAKA

Sistem Informasi

Robert A. Leitch dan K. Roscoe Davis dalam Jogiyanto (2005:11) menyatakan bahwa "Sistem informasi adalah sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategi dari suatu organisasi dan menyediakan pihak-pihak luar tertentu dangan laporan-laporan yang diperlukan". John Burch dan Gary Grudnitski dalam Jogiyanto (2005:12) mengemukakan bahwa sistem informasi terdiri dari komponen-komponen yang disebutnya dengan sebuah blok bangunan (*building block*), yaitu blok masukan (*input block*), blok model (*model block*), blok keluaran (*output block*), blok teknologi (*technology block*), blok basis data (*database block*) dan blok kendali (*controls block*). Sebagai suatu sistem keenam blok tersebut masing-masing saling berinteraksi satu dengan yang lainnya membentuk satu kesatuan untuk mencapai sasarannya.

Keamanan Informasi

Keamanan informasi didefinisikan sebagai sebuah perlindungan dan sumber daya terhadap upaya perubahan dan perusakan oleh seseorang yang tidak diijinkan. Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak. Keamanan informasi meliputi beberapa aspek diantaranya adalah :

1. *Confidentiality* (kerahasiaan)
   Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. *Integrity* (integritas)
   Aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk manajemen aspek *integrity* ini.
3. *Availability* (ketersediaan)
   Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat

terkait (aset yang berhubungan bilamana diperlukan) (Kristanto, 2003:2).

Confidentiality,integrity, dan *availability* merupakan tiga elemen yang menjadi dasar pengembangan program keamanan. Elemen-elemen tersebut saling berkaitan dalam membentuk keamanan informasi. Keamanan informasi yang terjaga dengan baik akan melindungi organisasi dari berbagai macam ancaman untuk memastikan keberlanjutan organisasi dan meminimalisir risiko-risiko yang mungkin terjadi.

Ancaman Terhadap Keamanan Fisik

Ancaman terhadap keamanan fisik ada bermacam-macam diantaranya : ancaman bencana alam, ancaman lingkungan, ancaman teknis, dan ancaman manusia.

Ancaman bencana alam merupakan sumber ancaman yang mencakup wilayah yang luas dan merupakan ancaman bagi *datacenter*, fasilitas pengolah informasi dan karyawan. Sangat mungkin untuk menilai resiko dari bermacam-macam bencana alam dan mengambil langkah-langkah pencegahan sehingga bencana kehilangan akibat bencana alam bisa dicegah. Ancaman lingkungan meliputi keadaan di mana terjadi perubahan kondisi di lingkungan sekitar *data center* yang dapat merusak atau menganggu pelayanan sistem informasi dan data yang disimpan

Ancaman teknis seperti contohnya kelistrikan, Listrik merupakan bagian penting bagi aktifitas sebuah sistem informasi. Semua peralatan listrik dan elektronik membutuhkan listrik agar dapat beroperasi. Pasokan listrik yang stabil juga diperlukan agar tidak terjadi kerusakan atau hal-hal yang tidak diinginkan seperti pelayanan yang terganggu. *Undervoltage* dan *overvoltage* merupakan gangguan listrik yang dapat mengganggu kegiatan operasional. Ancaman yang ditimbulkan oleh manusia lebih sulit dihadapi dibandingkan dengan ancaman bencana alam, lingkungan dan teknis karena ancaman dari manusia lebih sulit untuk diprediksi. Ancaman yang disebakan oleh manusia telah dirancang secara spesifik untuk mencari celah keamanan yang paling mudah untuk diserang. Vacca (936:2012) mengelompokkan ancaman manusia ke dalam beberapa kategori yaitu *Unauthorized Physical Access*, *Theft*, *Vandalism*, dan *Misuse*.

Kontrol Keamanan Fisik

1. *Physical Controls*

a. *Intrusion Prevention*

Intrusion prevention adalah proses yang dengan cerdas bertujuan untuk melakukan deteksi dini pada upaya serangan berbahaya, pelanggaran kebijakan, perlakuan yang tidak baik, dan pada saat yang sama mampu secara otomatis memblokir mereka secara efektif sebelum mereka berhasil mencapai sistem target atau korban (Tipton dan Krause, 998:2007). Adapun jenis-jenis dari *intrusion prevention* antara lain pagar, kunci *programmable,* penjaga, pencahayaan.

b. *Intrusion Detection*

Intrusion Prevention yang di dasarkan pada aktivitas atau tindakan untuk mengawasi memiliki kelemahan. Ketika aktivitas pengawasan mengalami penundaan atau tidak dilaksanakan sebagaimana mestinya, maka akan tercipta celah keamanan. Karena itu *intrusion detection* merupakan fasilitas yang sangat penting untuk melengkapi *Intrusion Prevention*. *Intrusion detection* adalah proses pemantauan peristiwa yang terjadi dalam sistem komputer atau jaringan dan menganalisis untuk memberikan tanda-tanda kemungkinan terjadinya insiden, yaitu pelanggaran atau ancaman pelanggaran yang akan terjadi terhadap kebijakan keamanan komputer, kebijakan penggunaan diterima, atau praktik keamanan standar (Scarfone dan Mell, 2007). Berikut ini adalah beberapa kelengkapan penunjang *intrusion detection*: alarm, *barrier detector, cctv,* dan *motion detectors.*

2. *Technical Controls*

Technical controls merupakan kontrol yang diimplementasikan melalui perangkat keras ataupun perangkat lunak. *Technical controls* biasanya sangat sulit untuk dibobol ketika telah diimplementasikan. *Technical controls* mampu bekerja tanpa intervensi manusia. *Technical controls* juga sering disebut sebagai *logical controls* (Killmeyer, 13:2006).

a. Smart Card

Smart card adalah kartu identitas sebesar kartu kredit, tanda pengenal, atau kartu akses kemanan dengan strip magnetik yang tertanam di dalamnya, barcode, atau integrated circuit chip (Stewart dkk., 760:2012). *Smart card* merupakan kartu yang dapat digunakan untuk tujuan identifikasi dan otentifikasi dan menyimpan informasi tentang kewenangan pemilik *smart card*. Beberapa *smart card* bahkan dapat melakukan

pemrosesan informasi dan penyimpanan data dalam chip memori dalam jumlah tertentu.

b. *Biometric*

Teknik lain dari otentikasi dan identifikasi yang biasanya digunakan adalah penggunaan biometrik. Karakteristik biometrik sering didefinisikan dengan *physiological* dan *behavioral*. Menurut Stewart dkk.,(2012:17), metode *physiological biometric* meliputi *fingerprinting*, *facial recognition*, *retina scans*, *iris scans*, *palm scans, hand geometry,* dan *voice pattern recognitio*n. Metode *behavioral biometric* mencakup *signature dynamics* dan *keystroke patterns*.

3. *Administrative Controls*

Administrative controls dapat didefinisikan sebagai kontrol yang dijalankan dan dikelola oleh manajemen administrasi untuk membantu mengurangi ancaman atau dampak dari pelanggaran pada keamanan komputer. Kontrol ini lebih berkaitan dengan administrasi sumber daya manusia dan kebijakan personil bukan pada perangkat keras atau perangkat lunak (Krutz dan Vines, 473:2004). *Administrative controls* terdiri atas *preventive administrative controls* dan *detective administrative controls.* Krause dan Tipton (1363:2007) menjelaskan bahwa yang termasuk dalam *preventive administrative controls* adalah *security awareness and technical training, separation of duties, recruitment and termination procedures, security policies and procedures, supervision*, *disaster recovery, contingency and emergency plan*, dan *user registration for computer access,* sedangkan yang termasuk dalam *detective administrative controls* adalah *Security Reviews and Audits*, *Performance Evaluation*, *Required Vacation*, *Background Investigation*, dan *Rotation of Duties.*

Penerapan Sistem Keamanan Fisik

Penerapan sistem keamanan fisik mengacu pada sebuah standar internasional yang ditetapkan oleh *International Organization for Standardization* (ISO). BS ISO/IEC 17799 yang diterbitkan pada tahun 2005 berisi praktik tentang kerahasiaan, integritas, dan ketersediaan informasi yang dapat digunakan oleh personil manajemen informasi dalam menerapkan Sistem Manajemen Keamanan Informasi (SMKI) pada organisasi. Menurut ceklist dan panduan *step-by-step* BS ISO/IEC 17799:2005 yang dikeluarkan oleh SANS Institute (www.sans.org,2005)Sistem Manajemen Keamanan Informasi (SMKI) terdiri atas 11 aspek salah satu diantaranya adalah aspek *Physical and Environmental Security,* yang memiliki poin-poin tentang: (1) Wilayah Aman (*Secure Areas*), dan (2) Keamanan Peralatan (*Equipments Security*). Penelitian ini hanya meneliti tentang aspek keamanan fisik sehingga hanya fokus pada aspek *Physical and Environmental Security* BS ISO/IEC 17799:2005.

METODE PENELTIAN

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian kualitatif. Lokasi penelitian yang dipilih adalah PMBSI IKIP PGRI Madiun dimana peneliti ingin menggambarkan bagaimana penerapan sistem keamanan fisik pada data center yang dijalankan di PMBSI IKIP PGRI Madiun dan untuk mengetahui apakah penerapan Sistem Keamanan Fisik Pada Data Center yang diterapkan di PMBSI IKIP PGRI Madiun telah mampu melindungi data organisasi milik PMBSI IKIP PGRI Madiun. Fokus dalam penelitian ini yaitu :

1. Deskripsi tentang penerapan Sistem Keamanan Fisik Pada Data Center PMBSI IKIP PGRI Madiun.
2. Analisa tentang bagaimana penerapan Sistem Keamanan Fisik Pada Data Center mampu melindungi data organisasi milik PMBSI IKIP PGRI Madiun.

Metode pengumpulan data pada penelitian ini adalah dengan observasi, wawancara, dan dokumentasi. Metode analisis data yang digunakan dalam penelitian ini adalah analisis kualitatif dengan metode Miles, Huberman yaitu pengumpulan data, kondensasi data, penyajian data, dan penarikan kesimpulan atau verifikasi.

HASIL DAN PEMBAHASAN

1. Deskripsi tentang Penerapan Sistem Keamanan Fisik pada Data Center IKIP PGRI Madiun

Salah satu kontrol dalam keamanan fisik adalah *Administrative Controls* yaitu kontrol yang dijalankan oleh manajemen PMBSI IKIP PGRI Madiun selaku pembuat kebijakan dan prosedur dalam rangka membantu meminimalisir ancaman dan dampak kerusakan fisik pada sebuah Data Center. PMBSI sebagai pihak yang bertanggung jawab sebagai pelaksana sistem informasi di IKIP PGRI Madiun memiliki pegawai berjumlah 7 orang dan 1 pegawai tidak tetap. Dalam kegiatan operasionalnya PMBSI menerima angaran rutin dari rektorat selaku pembuat kebijakan, dari

anggaran tersebut terlihat bahwa keamanan informasi di Data Center PMBSI IKIP PGRI cukup mendapat perhatian dari rektorat.

PMBSI bertanggung jawab untuk meningkatkan kualitas dan meningkatkan kewaspadaan pegawai dengan mengadakan pelatihan. Pelatihan terkait keamanan fisik yang pernah dilakukan di lingkungan IKIP PGRI Madiun adalah pelatihan tentang pemadaman kebakaran. Prosedur dan Kebijakan juga berperan penting dalam meminimalisir resiko keamanan Data Center, prosedur yang diterapkan ini membuat tidak sembarang orang bisa memasuki ruangan Data Center. Pengunjung yang ingin memasuki ruangan Data Center harus mendapat ijin resmi dari rektorat yang kemudian diteruskan kepada Kepala PMBSI dan selanjutnya dengan pendampingan dari pihak PMBSI mengantar pengunjung ke ruangan Data Center.

Prosedur dan kebijakan ketika berada di ruangan Data Center juga diperhatikan oleh PMBSI. Data Center PMBSI IKIP PGRI Madiun memiliki dua buah rak server, rak server pertama dalam kondisi yang tidak optimal dan sering terjadi masalah karena umur server tersebut cukup tua dibandngkan server kedua, jika timbul masalah pada server, perbaikan server yang rusak akan dilakukan di ruangan PMBSI yang terpisah dari ruang Data Center. Tidak ada ijin yang diperlukan untuk membawa barang keluar ruangan Data Center selama yang membawa barang tersebut pegawai PMBSI. Prosedur lain adalah pegawai PMBSI tidak diperbolahkan untuk makan, minum, dan merokok di lingkungan Data Center serta memiliki kewajiban untuk selalu mengunci ruangan ketika pegawai meninggalkan ruangan Data Center.

Kebersihan ruangan Data Center juga diperhatikan melalui prosedur dan kebijakan perawatan fasilitas Data Center. Pembersihan fasilitas Data Center dilakukan secara rutin oleh pihak yang berwenang yaitu pegawai PMBSI dibantu petugas kebersihan, hal yang dilakukan seperti membersihkan ruangan Data Center dari debu dan mengelap ruangan kaca yang mengembun. Debu yang menempel di peralatan elektronik dapat mengganggu sirkulasi udara sehingga dapat menyebabkan *overheat* pada server, sedangkan embun yang tercipta akibat ruangan Data Center yang dingin dapat berbahaya bagi *hardware* server dan peralatan elektronik di lingkungan Data Center.

Prosedur dan kebijakan yang belum dimiliki PMBSI adalah prosedur dan kebijakan terkait tentang *Disaster Recovery Plan*. *Disaster Recovery Plan* diperlukan ketika Data Center mengalami kerusakan akibat bencana alam maka dengan memiliki *Disaster Recovery Plan* pihak PMBSI akan memiliki panduan dan prosedur bagaimana mengatasi dan mengurangi resiko serta rencana pemulihan Data Center yang lebih cepat. Untungnya belum pernah terjadi kejadian bencana alam yang besar di lingkungan IKIP PGRI Madiun, yang pernah terjadi hanyalah banjir yang pernah menggenangi Jalan Setia Budi sehingga air sempat melewati pagar besi IKIP PGRI Madiun akan tetapi tidak sampai masuk ke pintu menuju ruangan Data Center karena ruangan Data Center memiliki ketinggian yang cukup ditambah dengan adanya penutupan jalur masuk air menggunakan karung pasir yang dilakukan oleh petugas keamanan IKIP PGRI Madiun.

Kontrol dalam Keamanan Fisik selanjutnya adalah *Physical Controls* dan *Technical Controls* yang merupakan kontol pengendalian keamanan Data center dengan melakukan pencegahan maupun pengawasan dengan parameter fisik dan teknikal. Alat keamanan fisik sebagai lapisan keamanan terluar adalah pagar. Pagar berfungsi sebagai pemisah antara lokasi yang ingin dilindungi dengan lingkungan disekitarnya, selain itu pagar juga berfungsi untuk membatasi jumlah akses atau jalan yang dapat dilalui untuk menuju lokasi yang dianggap penting. Ruangan Data Center milik PMBSI berada pada Gedung utama Kampus 1 IKIP PGRI Madiun yang bergabung di dalam ruangan kerja BAKA IKIP PGRI Madiun sebagai lokasi dimana Data Center berada memiliki pagar yang mengitarinya. Pagar ini merupakan lapisan terluar bagi lapisan keamanan gedung milik IKIP PGRI Madiun. Pagar ini mengelilingi lingkungan IKIP PGRI Madiun dengan ketinggian 1,5 sampai 5 meter. Pagar yang memisahkan IKIP PGRI Madiun dengan SDN 03 KANIGORO berupa dinding bata semen setinggi 2 meter, sedangkan di bagian belakang pagar yang memisahkan gedung IKIP PGRI Madiun dengan SMK GAMALIEL 1 berupa dinding bata semen setinggi 3 meter. Dibagian depan berbatasan dengan Jalan Setia Budi gedung IKIP PGRI dilindungi pagar besi setinggi 1,5 meter, sedangkan dibagian yang bersebelahan dengan gang Setia Mulya dilindungi pagar berupa bata semen diatasnya terdapat kawat besi setinggi 5 meter, dan di bagian parkiran belakang terdapat pagar besi setinggi 2 meter. Untuk memasuki lingkungan IKIP PGRI Madiun Kampus 1 terdapat 2 gerbang utama dan 1 jalan tikus. Disetiap gerbang besar

terdapat pos keamanan akan tetapi di 1 jalan tikus yang menembus SDN 03 KANIGORO tidak terdapat pos keamanan. Untuk memudahkan pengawasan pada waktu malam maka hanya gerbang utama yang berada di Jalan Setia Budi yang dibuka.

PMBSI tidak memiliki tenaga kemanan secara khusus maka tindakan pengamanan dijadikan satu dengan keamanan yang dimiliki IKIP PGRI Madiun. IKIP PGRI Madiun memiliki 5 tenaga keamanan yang terbagi menjadi 2 kelompok 2 shift dalam sehari, masing-masing shift bekerja selama 7 jam. Tenaga keamanan ditempatkan pada pos jaga yang terletak di gerbang utama dan gerbang lokasi parkir di Kampus 1 dan Kampus 2 IKIP PGRI Madiun. Tindakan pengamanan yang dilakukan antara lain adalah melakukan patrol rata-rata 7 kali dalam sehari, memeriksa pintu dan jendela gedung atau atau bangunan pada zona yang menjadi tanggung jawab masin-masing. Menutup semua jalan masuk kecuali gerbang utama.

Letak ruang Data Center PMBSI berada di sebuah gudang yang mejadi satu dengan ruang BAKA, untuk menuju ruang Data Center harus melewati 4 buah pintu, pintu pertama adalah pintu utama gedung yang pada jam kerja akan selalu terbuka, pintu kedua adalah pintu ruang BAKA yang pada jam kerja akan selalu terbuka juga, pintu ketiga adalah pintu masuk ke gudang selalu terkunci yang memiliki akses masuk hanya kepala BAKA dan mas Ma'ruf, dan keempat adalah pintu Data Center yang selalu dikunci yang memiliki kunci hanya mas Gilang dan mas Ma'ruf. Kunci ruangan Data Center belum menggunakan teknologi fingerprint atau biometric control yang lain. Data Center PMBSI tidak memiliki CCTV yang terdedikasi khusus. CCTV hanya berada di lorong setelah memasuki pintu masuk pertama berjumlah 3 buah. Kebutuhan pencahayaan ketika malam hari di lingkungan sekitar Data Center sudah tercukupi, hal ini dikarenakan selalu ada penjaga malam di lingkungan kampus sehingga kebutuhan akan penerangan sudah cukup baik. Didalam ruang Data Center terdapat dua buah pendingin ruangan dengan masing-masing berkapasitas 1pk yang bekerja bergantian masing-masing 12 jam dengan suhu rata-rata 23 derajat *celcius*. Kontrol suhu ruangan ini sangat penting untuk menjaga suhu dan sirkulasi udara di dalam ruangan agar server tidak mudah panas.

Penataan tempat didalam ruang server belum cukup baik, ini dikarenakan luas ruangan yang cukup sempit yaitu kurang lebih 2 x 3 meter persegi saja, sehingga didalam ruangan sekilas tampak tidak rapi. Penataan kabel listrik dan kabel LAN (*Local Area Network*) di didalam ruangan belum baik, beberapa hanya dirapikan seadanya. Kabel listrik dan kabel LAN belum terlindungi dari kerusakan atau tindakan penyadapan karena kabel listrik dan telefon di lingkungan Data Center hanya dirapikan seadanya. Pasokan listrik sangat penting bagi kelangsungan sebuah Data Center. Pasokan listrik Data Center PMBSI berasal dari listrik PLN (Perusahaan Listri Negara). Dalam keadaan darurat Data Center PMBSI tidak memiliki cadangan listrik alternatif dikarenakan tidak adanya genset. Untuk mengurangi resiko kerusakan akibat turunnya tegangan secara tiba-tiba ketika terjadi pemadam listrik, Data Center PMBSI memiliki *Uninterruptible Power Supply* (UPS) yang masih bekerja dengan baik. Untuk menghindari ancaman lonjakan arus tegangan akibat petir, diatas gedung terdapat penakal petir. Untuk menanggulangi kebakaran Data Center PMBSI hanya mengandalkan hand extinguisher yang terdapat di pos keamanan dekat gerbang utama. Peneliti juga tidak menemukan alat pendeteksi api atau asap di lingkunga ruangan Data Center.

2. Analisa tentang Bagaimana Penerapan Sistem Keamanan Fisik pada Data *Center* mampu melindungi data organisasi milik PMBSI IKIP PGRI Madiun

Analisa sistem keamanan fisik pada Data Center PMBSI IKIP PGRI Madiun ini peneliti menggunakan acuan landasan teori yang penulis paparkan pada BAB II dan sebuah standar internasional yang ditetapkan oleh *International Organization for Standardization* (ISO) yaitu BS ISO/IEC 17799 yang diterbitkan pada tahun 2005 berisi praktik tentang kerahasiaan, integritas, dan ketersediaan informasi yang dapat digunakan oleh personil manajemen informasi dalam menerapkan Sistem Manajemen Keamanan Informasi (SMKI).

Setelah melakukan observasi, wawancara, dan dokumentasi, terdapat beberapa kekurangan yang dimiliki Data Center PMBSI IKIP PGRI Madiun berdasarkan kajian pada BAB II dan BS ISO/IEC 17799. Kekurangan-kekurangan tersebut adalah sebagai berikut:

a. Jumlah pegawai, jumlah pegawai PMBSI yang dirasa belum mencukupi bagi beberapa pegawai, kekurangan pegawai ini terutama pada bagian jaringan. Semakin banyaknya layanan yang dimiliki PMBSI sehingga membuat kebutuhan akan pegawai tambahan sangat dibutuhkan. Pegawai yang jenuh karena

beban pekerjaan yang berat dapat mengurangi kualitas kinerja pegawai yang dapar berakibat terjadinya kelalaian prosedur di lapangan.

b. Anggaran, walaupun terdapat anggaran tahunan yang sudah direncanakan untuk keperluan PMBSI, namun birokrasi yang berbelit menyebabkan anggaran tersebut baru akan turun ketika terjadi permintaan pengadaan suatu barang, dimana hal tersebut dikeluhkan oleh anggota PMBSI.
c. Kurangnya pelatihan pegawai, kurangnya pelatihan terutama tentang Keamanan Fisik menyebabkan pegawai PMBSI nampak kurang mendalami pembahasan tentang Keamanan Fisik secara khusus dan mendetail, walaupun secara umum dan dasar mereka cukup mengerti pembahasan tentang Keamanan Fisik. Pelatihan yang pernah dilakukan dan terkait dengan Keamanan Fisik di lingkungan IKIP hanya pelatihan tentang pemadaman kebakaran.
d. Kebijakan makan, minum, dan merokok di lingkungan Data Center, terdapat kebijakan untuk tidak makan, minum, dan merokok di lingkungan Data Center, namun wawancara yang dilakukan peneliti mengungkap bahwa pernah terjadi pegawai PMBSI membawa makanan dan minman masuk ke ruang server ketika ada kerjaan lembur.
e. Letak kantor dan Data Center yang terpisah, ruang kerja PMBSI dengan Data Center yang berbeda gedung menyebabkan pengawasan tidak dapat dilakukan secara real-time juga merupakan kekurangan yang dimiliki Data Center PMBSI IKIP PGRI Madiun.
f. Kurang luasnya ruangan, ruangan Data Center yang sempit membuat jarak antar server kurang lebar yang dapat mengakibatkan timbulnya panas dan sirkulasi udara yang tidak baik. Ruangan yang sempit juga membuat kabel-kabel tidak teratur, beberapa hanya dirapikan seadanya sehingga rawan terjadi korsleting atau terjadi human error.
g. Kabel listrik dan kabel LAN, kabel listrik dan kabel LAN di lingkungan Data Center hanya dirapikan seadanya dan tidak terlindungi padahal sangat penting untuk merapikan dan melindungi kabel listrik dan kabel LAN agar terhindar dari kerusakan atau tindakan penyadapan yang mungkin dilakukan oleh orang-orang tidak bertanggung jawab..
h. Kunci, kunci ruangan Data Center belum menggunakan teknologi fingerprint atau biometric control yang lain. Kunci konvensional mengandung beberapa resiko seperti kemungkinan untuk hilang dan mudah digandakan.
i. CCTV, Data Center PMBSI tidak memiliki CCTV yang terdedikasi khusus, CCTV hanya berada di lorong setelah memasuki pintu masuk pertama berjumlah 3 buah hal ini membuat tidak semua wilayah di sekitar ruangan Data Center ter-cover oleh kamera CCTV.
j. Listrik, PMBSI tidak memiliki sumber listrik alternatif sendiri sebagai langkah antisipasi terhadap kemungkinan terputusnya aliran listrik dari PLN. Gangguan terhadap pasokan listrik menimbulkan kerugian karena terhambatnya layanan akibat server tidak dapat beroperasi.
k. Disaster Recovery Plan, PMBSI tidak memiliki Disaster Recovery Plan yang diperlukan ketika Data Center mengalami kerusakan akibat bencana alam yang bisa terjadi kapan saja dengan tidak terduga. Disaster Recovery Plan dapat membantu pihak PMBSI agar memiliki panduan dan prosedur bagaimana mengatasi dan mengurangi resiko serta rencana pemulihan Data Center yang lebih cepat.

KESIMPULAN DAN SARAN

Kesimpulan

1. Deskripsi tentang Penerapan Sistem Keamanan Fisik pada Data Center IKIP PGRI Madiun

Penerapan sistem keamananan fisik pada Data Center IKIP PGRI Madiun sudah mengalami perkembangan yang cukup positif setelah dibentuknya PMBSI, namun masih banyak kelemahan dan belum sesuai dengan standar BS ISO/IEC 17799. Tidak ada artinya pengamanan *software* yang baik dan pengamanan lainnya jika pengamanan dari ancaman fisik tidak diperhatikan, sehingga masih banyak yang perlu diperbaiki dalam Data Center IKIP PGRI Madiun.

2. Analisa tentang Bagaimana Penerapan Sistem Keamanan Fisik pada Data *Center* mampu melindungi data organisasi milik PMBSI IKIP PGRI Madiun

Penerapan sistem keamanan fisik pada Data Center IKIP PGRI Madiun pada dasarnya mampu untuk melindungi namun masih terdapat fasilitas yang harus diperbaiki. Masih terdapat beberapa celah keamanan yang memungkinkan adanya potensi ancaman secara fisik. Beberapa potensi tersebut antara lain tidak adanya kepastian bahwa

PMBSI akan mendapat pasokan listrik alternatif yang cukup untuk dapat terus beroperasi meskipun sedang terjadi pemadaman listrik. Kunci yang masih menggunakan kunci konvensional belum menggunakan teknologi *biometric control*. Sistem keamanan yang diterapkan selama ini lebih menekankan kepada potensi ancaman yang disebabkan oleh sumber daya manusia yang kurang memperhatikan potensi ancaman yang bersumber dari alam hal ini dibuktikan dengan tidak dimilikinya *Disaster Recovery Plan.*

Saran

Berdasarkan kesimpulan yang telah dijelaskan berikut saran yang dapat dilakukan untuk Data Center IKIP PGRI Madiun :

1. Penambahan jumlah pegawai PMBSI menjadi hal yang penting untuk sistem keamanan fisik pada data center. Hal itu dirasa penting karena jumlah pegawai masih belum mencukupi untuk keamanan fisik, kekurangan pegawai ini terutama pada bagian jaringan. Semakin banyaknya layanan yang dimiliki PMBSI sehingga membuat kebutuhan akan pegawai tambahan sangat dibutuhkan. Kurangnya pelatihan pegawai terutama tentang Keamanan Fisik menyebabkan pegawai PMBSI nampak kurang mendalami dan sadar tentang Keamanan Fisik secara khusus dan mendetail, walaupun secara umum dan dasar mereka cukup mengerti pembahasan tentang Keamanan Fisik.
2. Penerapan sistem keamanan fisik pada Data Center IKIP PGRI Madiun juga harus memperhatikan beberapa hal seperti Implementasi kebijakan makan, minum, dan merokok, terdapat kebijakan untuk tidak makan, minum, dan merokok di lingkungan Data Center, namun wawancara yang dilakukan peneliti mengungkap bahwa pernah terjadi pegawai PMBSI membawa makanan dan minman masuk ke ruang server ketika ada kerjaan lembur dimana hal ini cukup berbahaya bagi ruangan Data Center. Untuk itu pengawalan implementasi kebijakan di lingkungan PMBSI harus diperbaiki.
3. Menyatukan ruang kerja PMBSI dengan Data Center, letak yang berbeda gedung menyebabkan pengawasan tidak dapat dilakukan secara *real-time* juga merupakan kekurangan yang dimiliki Data Center PMBSI IKIP PGRI Madiun. Untuk itu menyatukkan ruang kerja PMBSI dengan Data center untuk alasan pengawasan keamanan dan efisiensi menjadi kebutuhan PMBSI.
4. Penambahan luas ruangan, ruangan Data Center yang sempit membuat jarak antar server kurang lebar yang dapat mengakibatkan timbulnya panas dan sirkulasi udara yang tidak baik. Ruangan yang sempit juga membuat kabel-kabel tidak teratur, beberapa hanya dirapikan seadanya sehingga rawan terjadi korsleting atau terjadi human error. Kebutuhan penambahan server seiring bertambahnya layanan juga menjadi pertimbangan bagi PMBSI, untuk itu penambahan luas ruang atau memindahkan ke ruangan yang lebih besar menjadi kebutuhan PMBSI.
5. Melindungi kabel listrik dan kabel LAN, kabel listrik dan kabel LAN di lingkungan Data Center hanya dirapikan seadanya dan tidak terlindungi padahal sangat penting untuk merapikan dan melindungi kabel listrik dan kabel LAN agar terhindar dari kerusakan atau tindakan penyadapan yang mungkin dilakukan oleh orang-orang tak bertanggung jawab. Untuk meminimalisir resiko kerusakan, peyadapan, dan sabotase, alangkah baiknya jika kabel-kabel di ruangan maupun di sekitar Data Center untuk lebih dirapikan dan diberi pelindung kabel.
6. Penggunaan *biometric control* pada kunci, kunci ruangan Data Center belum menggunakan teknologi *fingerprint* atau *biometric control* yang lain. Kunci konvensional mengandung beberapa resiko seperti kemungkinan untuk hilang dan mudah digandakan. Dengan menggunakan teknologi *biometric control* akses masuk ke Data Center akan benar benar terkontrol. Untuk meningkatkan akses keamanan tersebut peneliti menyarankan penggunaan kunci yang menggunakan teknologi *biometric control.*
7. Penambahan CCTV, Data Center PMBSI tidak memiliki CCTV yang terdedikasi khusus, CCTV hanya berada di lorong setelah memasuki pintu masuk pertama berjumlah 3 buah hal ini membuat tidak semua wilayah di sekitar ruangan Data Center ter-cover oleh kamera CCTV. Untuk itu penambahan CCTV yang terdedikasi khusus untuk *Data Center* menjadi kebutuhan PMBSI.
8. Memiliki sumber listrik alternatif, PMBSI tidak memiliki sumber listrik alternatif sendiri sebagai langkah antisipasi terhadap kemungkinan terputusnya aliran listrik dari PLN. Gangguan terhadap pasokan listrik

menimbulkan kerugian karena terhambatnya layanan server tidak dapat beroperasi. Untuk itu rencana pembelian sumber listrik alternatif menjadi kebutuhan PMBSI. Memiliki *Disaster Recovery Plan*, PMBSI tidak memiliki *Disaster Recovery Plan* yang diperlukan ketika Data Center mengalami kerusakan akibat bencana alam yang bisa terjadi kapan saja dengan tidak terduga. Dengan memiliki *Disaster Recovery* Plan dapat membantu pihak PMBSI agar memiliki panduan dan prosedur bagaimana mengatasi dan mengurangi resiko serta rencana pemulihan Data Center yang lebih cepat.

DAFTAR PUSTAKA

Ariyus, Dony. 2006. *Computer Security*. Yogyakarta : Andi.

Jogiyanto.2005. *Analisis&Desain Sistem Informai* . Yogyakarta : Andi

Jogiyanto. 2005. *Sistem Teknologi Informasi*. Yogyakarta : Andi.

Killmeyer, Jan. 2006. *Information Security Architecture, An Integrated Approach to Security in the Organization,* Second Edition. Auerbach Publication.

Kristanto, Andri. 2003. *Keamanan Data Pada Jaringan Komputer*. Yogyakarta : Gaya Media

Krutz, Ronald L. dan Vines, Russell Dean. 2004. *The CISSP Prep Guide, Second Edition: Mastering the CISSP and ISSEP Exams*. Indianapolis : Wiley Publishing, Inc

Scarfone, Karen dan Mell, Peter. 2007. *Guide to Intrusion Detection and Prevention Systems (IDPS): Recommendations of the National Institute of Standards and Technology*. Gaithersburg : U.S. Department of Commerce.

Stewart, James M., Chapple, Mike, dan Gibson, Darril. 2012. *CISSP: Certified Information Systems Security Professional Study Guide.* Indianapolis : Wiley Publishing, Inc.

Sutabri. 2005. *Sistem Informasi Manajemen*, Edisi I. Yogyakarta : Andi.

Thiagarajan, Val. 2006. The SANS Institute "Checklist and Step-by-step Guide ISO/IEC 17799:2005" diakses pada 27 Oktober 2015 dari www.sans.org

Tipton, Harold F. dan Krause, Micki. 2007. *Information Security Management Handbook*, Sixth Edition. Auerbach Publications.

Vacca, John R. 2013. *Computer and Infirmation Security Handbook,* Second Edition. Waltham : Morgan Kaufmann.