

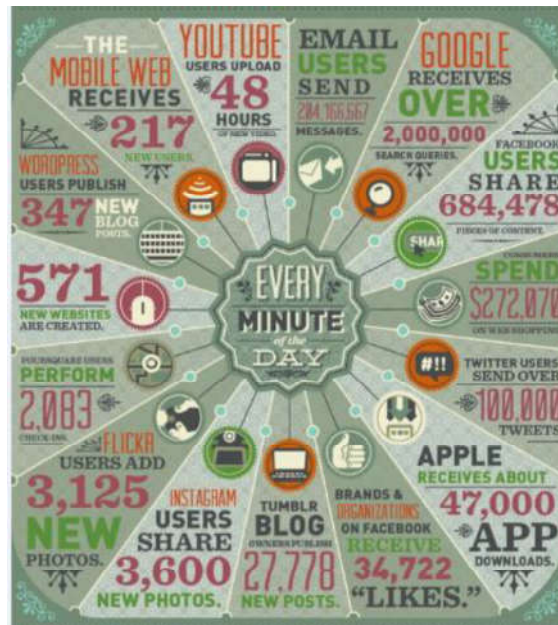
BAB I

PENDAHULUAN

I.1 Latar Belakang

Perkembangan zaman yang sangat cepat dimotori oleh arus globalisasi yang meningkat secara signifikan. Salah satu pengaruh globalisasi adalah perkembangan teknologi informasi yang sangat cepat. Teknologi informasi saat ini telah menjadi kebutuhan primer bagi manusia dan digunakan sebagai solusi untuk menyelesaikan aktivitas dan permasalahan sehari-hari dalam kehidupan manusia. Dengan meningkatnya kebutuhan teknologi informasi, pertukaran data digital yang terjadi juga semakin banyak. Data dalam bentuk digital sudah sangat banyak dan sangat mudah ditemukan, bahkan pada beberapa pihak data digital merupakan aset yang sangat penting. Contohnya, data digital pada perusahaan, kampus, bank, dan pemerintahan.

Berikut beberapa fakta penggunaan data digital dalam kehidupan sehari-hari:



Gambar I. 1 Pertukaran Data Digital dalam Satu Menit (*Antariksa, 2014*)

Gambar I.1 menunjukkan jumlah pertukaran data digital yang terjadi dalam satu menit. Hal tersebut membuktikan bahwa kebutuhan *data center* sebagai teknologi

penyimpanan data digital semakin meningkat dan kehandalan *data center* adalah salah satu aspek yang diperhatikan saat organisasi ingin menggunakan *data center*.



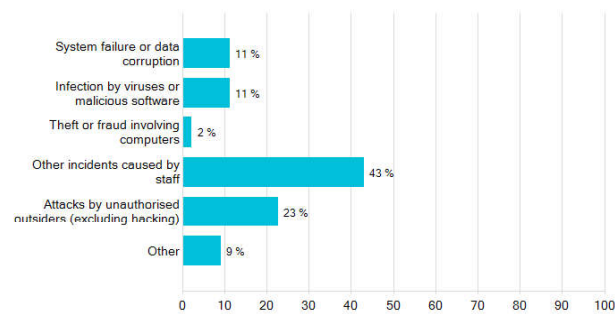
Gambar I. 2 Data Digital di Indonesia (*Wijaya, 2015*)

Gambar I.2 menunjukkan fakta mengenai data digital di Indonesia. Dari gambar I.2 tersebut terlihat bahwa penggunaan teknologi informasi untuk kehidupan sosial sudah sangat masif di Indonesia dan sudah pasti pertukaran data digital yang terjadi sangat besar. Dari gambar I.1 dan I.2, menunjukkan besarnya pertukaran dan penggunaan data digital sehingga dibutuhkan teknologi informasi yang dapat menyimpan, mengelola, dan mengolah data dalam jumlah besar tersebut. Teknologi tersebut adalah *data center*. Semakin seringnya pertukaran data digital terjadi, maka peran *data center* menjadi semakin penting dan vital.

Data Center dikenal sebagai *server farm* atau ruang komputer, *Data Center* merupakan tempat dimana mayoritas dari *enterprise server* dan penyimpanan berada, dioperasikan, dan dikelola (Bullock, 2009). Bagi perusahaan, berjalannya proses bisnis selaras dengan tujuan perusahaan adalah kebutuhan yang mendasar. Berdasarkan hal tersebut, perusahaan harus mempunyai *data center*, apalagi perusahaan yang berbasis IT yang sudah menerapkan *internet*. Karena data digital yang dimiliki perusahaan sangat banyak dan merupakan data yang sangat penting. Perusahaan berbasis IT adalah perusahaan yang sudah menggunakan teknologi informasi dalam menyelesaikan dan mendukung seluruh aktivitas di dalam perusahaan tersebut. Peran *data center* semakin vital dalam kehidupan khususnya

sebagai komponen tercapainya tujuan dari perusahaan. *Data center* harus memberikan layanan yang optimal sebagai pusat dari layanan bisnis perusahaan.

Kriteria desain dari perancangan *data center* harus memenuhi beberapa aspek, yaitu *Availability, Scalability, Security, Performance, dan Manageability* (Arregoces, 2004). Salah satu aspek penting dalam perancangan *data center* adalah aspek keamanan. *Information Security* adalah langkah-langkah yang diadopsi untuk mencegah penggunaan yang tidak sah, penyalahgunaan modifikasi, atau penolakan penggunaan pengetahuan, fakta, data, atau kemampuan (Maiwald, 2011).



Gambar I. 3 Grafik Insiden Keamanan (Coopers, 2015)

Gambar I.3 menunjukkan survei yang dilakukan oleh *PricewaterhouseCoopers* tahun 2015 mengenai *Cyber Security Breaches Survey 2015*, dari grafik tersebut terlihat bahwa insiden keamanan yang sering terjadi dan sangat buruk dampaknya adalah kesalahan yang disebabkan oleh *human error* dan *unauthorized access* dari luar organisasi. Dua sampai tiga persen pendapatan tahunan organisasi hilang karena insiden yang jadi pada keamanan informasi terutama yang disebabkan oleh perilaku manusia (Alnatheer, 2015). Hal tersebut semakin menguatkan bahwa sangat dibutuhkan keamanan jaringan khususnya keamanan secara fisik dan logik dalam sebuah organisasi sehingga memastikan keberlangsungan organisasi berjalan sesuai dengan tujuan yang ingin dicapainya.

Dikaitkan dengan peran *data center* sebagai media pengolahan data digital dan sebagai pusat dari layanan bisnis perusahaan serta sangat pentingnya data untuk perusahaan. *Data center* harus memiliki sistem keamanan yang ketat baik pengamanan secara fisik maupun logikal sehingga meminimalisir terjadinya kerugian bagi organisasi.

Lembaga Ilmu Pengetahuan Indonesia (LIPI) merupakan lembaga Pemerintah non Kementerian Republik Indonesia yang dikoordinasikan oleh Kementerian Negara Riset dan Teknologi. Pusat Dokumentasi dan Informasi Ilmiah (PDII) merupakan organisasi dibawah naungan Lembaga Ilmu Pengetahuan Indonesia. PDII yang dulunya bernama PDIN (Pusat Dokumentasi dan Informasi Ilmiah) mempunyai visi menjadi lembaga yang terdepan dibidang dokumentasi dan informasi dalam rangka ikut membangun masyarakat yang adil, cerdas, kreatif, dan dinamis berbasis ilmu pengetahuan dan teknologi yang humanistik. Tugas pokok PDII-LIPI yaitu melaksanakan pembinaan dan pemberian jasa dokumentasi informasi (PDII-LIPI, 2011).

Dalam kegiatannya PDII berfokus pada tiga kegiatan utama, yaitu: jasa dokumentasi, jasa informasi, dan pembinaan dan pengembangan di bidang dokumentasi informasi. PDII-LIPI mempunyai *database* yang berisi jurnal, *e-proceeding*, buku, koleksi audio visual dari seluruh universitas yang ada di Indonesia. PDII-LIPI memiliki beberapa proses bisnis inti, yaitu perpustakaan, layanan ISSN, pelatihan, pengembangan perpustakaan di daerah, pengemasan dokumentasi digital, pembuatan diversifikasi jurnal, pembuatan pohon industri terkait penelitian yang sudah dilakukan. Untuk mendukung kegiatannya, PDII-LIPI tentunya harus menggunakan teknologi informasi untuk memudahkan masyarakat khususnya kalangan cendekiawan dan peneliti untuk mendokumentasikan karyanya. Keberagaman data yang dimiliki oleh PDII-LIPI menjadikannya salah satu penyedia jasa informasi terbesar di Indonesia. Dengan data yang dimiliki oleh PDII-LIPI dapat memudahkan pelajar, kalangan akademisi, kalangan praktisi, dan perusahaan dalam hal pencarian data untuk riset dan pengambilan suatu keputusan strategik. Tetapi dengan kekayaan data yang dimiliki oleh PDII-LIPI, mengakibatkan peluang besar dalam kerentanan data baik secara fisik maupun logik. Jika tidak dikelola dengan baik, maka data yang ada di PDII-LIPI bisa saja dimanfaatkan untuk hal yang tidak baik. Kerentanan fisik yang mungkin terjadi adalah pencurian data, pencurian infrastruktur, sabotase serta bencana alam. Kerentanan logik yang mungkin terjadi adalah *Denial of Service Attack*, *unauthorized access*, *malware*, dan *scanning*. Solusi yang bisa dimanfaatkan untuk menghindari kerentana tersebut adalah tersedianya infrastruktur *data center* yang

memiliki sistem keamanan yang ideal baik secara fisik maupun logik dan mampu menunjang kegiatan bisnis dari PDII-LIPI.

Berdasarkan hasil observasi kondisi saat ini, PDII-LIPI sebelumnya telah memanfaatkan *data center* dengan kapasitas hingga *terabyte*. Tetapi, terdapat masalah yang muncul akibat kelemahan perencanaan terkait penerapan *data center* pada PDII-LIPI. Masalah tersebut adalah *server-server* yang digunakan untuk mendukung proses bisnis PDII-LIPI masih memiliki kerentanan baik secara fisik maupun logik. Kerentanan tersebut seperti penempatan *data center* yang tidak sesuai, tidak adanya pengamanan khusus untuk ruangan *data center*, layanan keamanan logik *data center* masih minim, serta minimnya pengamanan *data center* terhadap bencana, seperti kebakaran. Dari permasalahan pada PDII-LIPI tersebut dapat disimpulkan bahwa permasalahan utama pada penerapan *data center* di PDII-LIPI adalah tidak adanya standar yang digunakan untuk mengelola *data center* khususnya standar keamanan fisik dan logik. Sehingga PDII-LIPI berencana melakukan pengembangan *data center* sesuai dengan standar. Hal tersebut menjadi dasar dalam pembangunan desain keamanan *data center* dalam penelitian ini.

Dalam melakukan penelitian ini, metode yang digunakan adalah metode *Prepare, Plan, Design, Implement, Operate, Optimize* (PPDIOO) dan mengacu pada standar TIA 942 untuk keamanan fisik dan standar *ISO/IEC 27000 Series* untuk keamanan logikal. Metode pendekatan PPDIOO berisi tentang bagaimana merancang jaringan yang baik, termasuk siklus hidupnya. Metode ini membantu perusahaan untuk berhasil dalam pengembangan teknologi layanan *end-to-end* yang selaras dengan bisnis inti dari CISO. Metode ini menyelaraskan bisnis dan persyaratan teknis dari setiap fase (Cisco, 2005).

Penelitian ini menghasilkan desain keamanan data center baik secara fisik maupun logik yang sesuai dengan standar TIA-942 dan ISO/IEC 27000 series untuk data center PDII-LIPI.

I.2 Perumusan Masalah

1. Bagaimana mengidentifikasi kondisi saat ini keamanan *data center* pada PDII-LIPI?

2. Bagaimana rancangan sistem keamanan ideal *data center* pada PDII-LIPI menggunakan metode PPDIIO serta standar ISO/IEC 27000 *Series* dan TIA-942?

I.3 Tujuan Penelitian

1. Melakukan identifikasi kondisi saat ini keamanan *data center* di PDII-LIPI
2. Merancang desain keamanan infrastruktur *data center* yang ideal secara fisik dan logik pada PDII-LIPI menggunakan metode PPDIIO serta menggunakan standar TIA-942 dan standar ISO/IEC 27000 *Series*

I.4 Batasan Penelitian

Batasan penelitian tugas akhir ini adalah:

1. Penelitian ini hanya dilakukan didalam ruang lingkup PDII-LIPI
2. Penelitian ini mengesampingkan biaya yang dikeluarkan dalam proses implementasi keamanan infrastruktur *data center*
3. Penelitian ini hanya memberikan rekomendasi dan implementasi diserahkan sepenuhnya kepada PDII-LIPI
4. Penggunaan metode PPDIIO dalam penelitian ini hanya sampai pada tahap *design*
5. Kustomisasi standar TIA-942 dan ISO/IEC 27000 *series* dibatasi berdasarkan kebutuhan keamanan *data center* PDII-LIPI

I.5 Manfaat Penelitian

Manfaat dari penelitian tugas akhir ini, yaitu:

1. Mengevaluasi kondisi saat ini keamanan *data center* yang digunakan sebagai input proses desain keamanan infrastruktur *data center* di PDII-LIPI
2. Memberikan rancangan ideal terkait keamanan secara fisik dan logik pada infrastruktur *data center* yang ada di PDII-LIPI
3. PDII-LIPI memiliki rancangan desain infrastruktur *data center* yang memiliki sistem keamanan yang ideal baik secara fisik maupun logik.

I.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi mengenai uraian latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi literatur yang relevan dengan permasalahan yang dihadapi, penelitian terdahulu yang memiliki keterkaitan dengan penelitian yang sedang dilakukan, dan teori-teori yang digunakan seperti jaringan computer, *data center*, *best practice security* fisik & logikal *data center*, standar TIA-942 dan standar ISO/IEC 27000 *series*, serta metode PPDIOO.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan model untuk merumuskan solusi dari permasalahan yang ada. Selain itu dijelaskan juga langkah-langkah penelitian secara rinci meliputi tahap identifikasi, tahap analisis, tahap desain, tahap simulasi, dan tahap akhir dari penelitian ini.

BAB IV ANALISIS KONDISI SAAT INI

Bab ini menjelaskan kondisi saat ini *data center* pada PDII-LIPI meliputi profil lembaga, kondisi saat ini meliputi denah ruangan, topologi logik, kondisi keamanan fisik saat ini, dan kondisi keamanan logik saat ini. Selain itu, dijelaskan juga tentang analisis kondisi saat ini meliputi analisis gap keamanan fisik dan logik *data center*.

BAB V PERANCANGAN DESAIN USULAN

Bab ini menjelaskan perancangan usulan terhadap hasil analisis kondisi saat ini meliputi desain rancangan, spesifikasi produk usulan, harga produk usulan hingga manfaat yang didapatkan dari implmentasi usulan tersebut.

BAB VI KESIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan dari penelitian yang dilakukan serta saran untuk penelitian selanjutnya tentang topik yang sama.