BAB I
PENDAHULUAN

I.1 Latar Belakang

Kemajuan perkembangan teknologi informasi memiliki peranan penting di kehidupan masyarakat dalam berkomunikasi. Kebutuhan akan adanya komunikasi yang instan menjadi hal yang sangat diperlukan. Komunikasi adalah pertukaran informasi antara dua individu. Maksud dari komunikasi yaitu pertukaran informasi atau data dari komputer satu ke komputer lainnya. Saat ini informasi menjadi hal penting dalam sebuah organisasi, bahkan dapat dikatakan "*information-based society*" (Ariyus, 2008). Nilai informasi menjadi sangat penting dan menuntut pengelolaan sistem keamanan agar tidak terjadi kebocoran informasi atau data. Dalam bidang pemerintahan informasi atau data yang penting seperti identitas, keuangan, dan lain sebagainya. Sebagai contoh yaitu peretasan data identitas sebanyak 50 juta warga Turki (VOA, 2016). Selain di Turki, peretasan juga terdapat di Indonesia contohnya yaitu terjadi pada situs *website* DPRD Sidoarjo yang menyebabkan terdapat informasi yang tidak pantas untuk diberikan (Sugiyarto, 2016). Berdasarkan kedua kasus tersebut, membuktikan bahwa semua orang dapat menjadi target peretasan, untuk itu keamanan jaringan untuk entitas pemerintahan harus ditingkatkan.

Untuk menghubungkan informasi, data atau aplikasi dari beberapa tempat perlu adanya sebuah pusat data sebagai tampat mengatur segala proses yang ada. Salah satu faktor yang sangat penting pada pusat data adalah faktor keamanan, karena pusat data menjadi akar dari semua informasi atau data yang tersimpan. Pada keamanan pusat data terbagi menjadi dua hal yaitu *physical security* dan *logical security*. Kriteria dalam keamanan informasi harus meliputi *confidentiality*, *availability*, dan *integrity*.

Pentingnya nilai sebuah informasi menyebabkan hanya orang-orang tertentu saja yang dapat mengakses informasi tersebut. Sehingga untuk melindungi sebuah informasi dan untuk mencegah dampak yang tidak diinginkan perlu adanya keamanan dari sistem informasi yang digunakan telah sesuai dengan standar

keamanan yang sudah ditetapkan oleh federasi internasional. Perancangan sebuah jaringan komputer harus memenuhi standar diberbagai aspek salah satunya yaitu aspek keamanan jaringan. Dalam sebuah jaringan perlu adanya aturan untuk pengguna yang menggunakan jaringan tersebut. Aturan tersebut berfungsi yaitu sebagai hak akses yang membatasi pengguna untuk menghindari adanya peretasan yang dapat menyebabkan terjadinya kerusakan atau pencurian serta pemalsuan data.

Objek pada penelitian ini dilakukan pada pusat data Pemerintah Kabupaten Bandung. Keamanan sistem informasi penting bagi suatu organisasi khususnya pada Pemerintah Kabupaten Bandung karena dapat berfungsi sebagai *enabler* dari suatu sistem contohnya yaitu *e-government*. Dalam penggunaan sistem *e-government* jika tidak terdapat keamanan sistem informasi maka sistem *e-government* tidak dapat berjalan dikarenakan kerentanan terhapat peretasan. Banyak sistem informasi tidak bisa dirancang keamanannya secara optimal karena keterbatasan informasi, untuk itu dibutuhkan manajemen dan prosedur yang sesuai untuk mengatasinya (ISO/IEC, *Information technology — Security techniques — Code of practice for information security management*, 2005).

Proses perancangan suatu desain keamanan jaringan membutuhkan standar sebagai pedoman *best practice* dan mempermudah dalam hal pengembangan selanjutnya, dan pada penelitian ini menggunakan standar keamanan yaitu ISO/IEC (*International Organization for Standardization / International Electrotechnical Commission*) yaitu ISO/IEC 27001. ISO adalah organisasi internasional yang beranggotakan 162 badan standar nasional yang bertujuan dalam hal ilmu pengetahuan dan untuk memberikan solusi terhadap tantangan global (ISO, 2010).

Mengacu pada standar ISO/IEC 27001, bahwa DISKOMINFO Pemerintah Kabupaten Bandung belum menerapkan beberapa *domain* manajemen dan kontrol keamanan informasi. Berikut merupakan tabel *domain* yang belum terpenuhi:

Tabel I. 1 Kondisi Manajemen dan Kontrol Keamanan Informasi Saat Ini

Domain	Control
Kebijakan Keamanan informasi	Kebijakan keamanan informasi harus dipublikasikan dan dikomunikasikan, dikaji dan evaluasi keamanan informasi harus disesuaikan dengan perkembangan aset
Prosedur Operasional dan Tanggung Jawab	Kebijakan prosedur operasi dan tanggung jawab tugas
Backup	Salinan informasi, *software*, dan *system image* yang diambil dan diuji secara teratur sesuai dengan kebijakan mengenai *backup* yang disepakati
Tanggung Jawab Pengguna	Pengguna bertanggung jawab untuk melindungi autentikasi
Sistem dan Aplikasi Akses Kontrol	Pencegahan akses tidak sah ke sistem operasi dan manajemen *password* berupa perjanjian menjaga kerahasiaan *password*, edukasi pemilihan *password* dan pemeliharaan *password*

Pengembangan suatu sistem membutuhkan tahapan yang terstruktur dalam proses perancangan, maka diperlukan suatu metodologi yang dapat digunakan sebagai kerangka dalam penelitian. Adapun pada penelitian ini menggunakan metodologi NDLC (*Network Development Life Cycle*). Metodologi NDLC memungkinkan pengembangan dapat dilakukan secara berulang, artinya jika masih terdapat kekurangan atau kelemahan dalam sekali siklus pengembangan maka dapat dilakukan perbaikan.

I.2 Perumusan Masalah

Perumusan masalah berfungsi sebagai fokus dari suatu permasalahan pada sebuah penelitian. Berdasarkan latar belakang permasalahan, masalah yang dirumuskan pada penelitian ini adalah sebagai berikut:

1. Bagaimana kondisi keamanan jaringan komputer saat ini pada DISKOMINFO Pemerintah Kabupaten Bandung?
2. Bagaimana usulan rancangan kemanan jaringan sesuai standar ISO 27001:2013 pusat data Pemerintah Kabupaten Bandung?

I.3 Tujuan Penelitian

Tujuan penelitian adalah informasi yang ingin diperoleh atau hasil yang ingin diusulkan di dalam sebuah penelitian. Tujuan diadakannya penelitian ini adalah sebagai berikut:

1. Memperoleh kondisi keamanan jaringan komputer saat ini pada DISKOMINFO Pemerintah Kabupaten Bandung.
2. Memperoleh usulan rancangan kemanan jaringan sesuai standar ISO 27001:2013 pusat data Pemerintah Kabupaten Bandung.

I.4 Manfaat Penelitian

Manfaat yang didapat dari penelitian ini adalah sebagai berikut:

1. Memberikan rekomendasi usulan pengembangan keamanan jaringan pada bagian DMZ area pusat data di Pemerintah Kabupaten Bandung yang memenuhi standar ISO/IEC 27001.
2. Meminimalisir kemungkinan terjadinya serangan *brute force attack* dari luar pada jaringan internal pusat data di Pemerintah Kabupaten Bandung.

I.5 Batasan Penelitian

Batasan penelitian dilakukan agar pengamatan tidak keluar dari pokok pembahasan penelitian. Batasan-batasan ini berfungsi sebagai fokus untuk penelitian, berikut ini adalah beberapa batasan penelitian:

1. Penelitian ini hanya dilakukan pada jaringan pusat data bagian area DMZ di Pemerintah Kabupaten Bandung dan melakukan *sampling* untuk

mengambil data pada DMZ area pusat data Pemerintahan Kabupaten Bandung.

2. Penelitian ini menggunakan standar keamanan ISO/IEC 27001:2013.
3. Pada proses penelitian ini, penulis menggunakan metodologi NDLC sampai tahap simulasi/*prototype*.
4. Simulasi dari usulan pada penelitian ini tidak dilakukan secara langsung di objek penelitian.
5. Penelitian ini hanya memberikan rekomendasi desain usulan dan keputusan untuk melakukan implementasi diserahkan seluruhnya kepada pihak Pemerintah Kabupaten Bandung.

I.6 Sistematika Penulisan

Untuk memudahkan membaca penelitian ini, maka pada bagian ini dibuat gambaran mengenai sistematika penulisan terhadap penelitian ini.

1. Bab I Pendahuluan

   Bab ini berisi mengenai uraian latar belakang, perumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian dan sistematika penelitian.
2. Bab II Tinjauan Pustaka

   Bagian ini menjelaskan tinjauan pustaka dan teori-teori yang digunakan dalam penelitian ini.
3. Bab III Metode Penelitian

   Bagian ini menjelaskan metodologi yang digunakan dalam proses analisa dan perancangan penelitian ini.
4. Bab IV Analisis Kondisi Saat Ini

   Bab ini berisi mengenai kondisi jaringan pada DMZ area pusat data saat ini pada Pemerintah Kabupaten Bandung beserta dengan profil lembaga.
5. Bab V Perancangan Keamanan Jaringan Komputer Usulan

   Bagian ini menjelaskan mengenai analisis dan usulan perancangan, serta hasil dari pengujiannya.
6. Bab VI Kesimpulan Dan Saran

Bagian ini menjelaskan mengenai kesimpulan yang didapat dari penelitian yang telah diselesaikan dan saran yang ditujukan untuk para pembaca.