BAB I
PENDAHULUAN

I.1 Latar Belakang

Di era globalisasi saat ini, perkembangan teknologi informasi semakin pesat dan mampu menjadi sumber kebutuhan utama bagi manusia dalam menyelesaikan permasalahan kesehariannya. Contohnya adalah semakin mudahnya informasi yang dapat kita dapatkan dengan adanya *Internet*. *Internet* sendiri merupakan sekumpulan komputer yang saling terhubung di dunia ini dan setiap detiknya terjadi proses pertukaran data antar individu (Tanenbaum & Wetherall, 2011). Dalam proses tersebut sangat diperlukan keamanan terhadap data yang dikirimkan. Keamanan jaringan komputer sangat diperlukan dalam urusan pemerintahan dimana data yang ditransmisikan merupakan data-data penting yang tidak boleh dibocorkan ke publik (Stallings, 2013). Selain itu pada pusat pemerintah terdapat sebuah pusat data yang digunakan sebagai pusat penyimpanan arsip-arsip pemerintahan, aplikasi pelayanan publik, dan data-data penting lainnya.

Pada pusat data diperlukan infrastruktur jaringan komputer yang kokoh dan memiliki keamanan yang baik, karena pusat data menjadi akar dari semua data/informasi itu tersimpan. Jaringan komputer yang kokoh disini diartikan sebagai jaringan komputer yang dibangun sesuai dengan standar yang telah ditetapkan agar terlindungi oleh tindakan kriminal seperti peretasan sistem ataupun pencurian data, contohnya kasus mengenai peretasan yang terjadi di badan Pemerintah Federal Amerika Serikat yang mengakibatkan bocornya informasi 22 juta pegawai (CNN Indonesia, 2015). Kasus lainnya adalah peretasan situs Badan Pengaduan Masyarakat Kementrian Komunikasi dan Informatika (DUMAS KOMINFO) dimana situs tersebut dilakukan *deface* (Liputan 6, 2016). Dilihat dari dua kasus sebelumnya dapat dijelaskan bahwa keamanan jaringan komputer dan pusat data pada pemerintah sangat dibutuhkan optimasi secara berkala, baik pada keamanan komunikasi data dari *Internet* ke jaringan internal pemerintah maupun dari jaringan internal itu sendiri menuju ke *Internet*.

Lokasi yang dijadikan tempat untuk penelitian ini adalah salah satu SKPD pada Pemerintah Kabupaten Bandung yaitu Dinas Komunikasi, Informatika, dan Statistik (DISKOMINFO). Fokus penelitian ini adalah perancangan keamanan jaringan komputer dari sisi pegawai pemerintah dimana hal yang diperhatikan adalah hak akses pegawai menuju *Internet*. Penelitian ini membahas cara dalam menangani penggunaan *proxy* ilegal yang dilakukan oleh pegawai untuk membuka situs *streaming media* demi kepentingan pribadi. Penggunaan *proxy* dan mengakses *streaming media* merupakan larangan pada Pemerintah Kabupaten Bandung. Buktikan adanya insiden tersebut adalah ditemukannya penggunaan *proxy* ilegal sebesar 0.26% dan akses menuju *streaming media* sebesar 1.91% pada *log* perangkat keamanan di DISKOMINFO. Dengan adanya penyalahgunaan akses tersebut, *bandwidth* yang seharusnya digunakan untuk pekerjaan Pemerintah Kabupaten Bandung menjadi terbuang sia-sia dan mengakibatkan kerugian pada proses bisnis pemerintah, melihat Pemerintah Kabupaten Bandung merupakan inti dari sistem *e-government* wilayah Kabupaten Bandung. Jika jaringan komputer tidak dikelola dengan baik maka sistem pemerintahan atau *e-government* itu tidak akan berjalan dengan baik.

Pada penelitian ini digunakan standar ISO/IEC 27001 sebagai pedoman dalam proses pembuatan desain keamanan jaringan dan pengembangan sistem selanjutnya karena telah mengacu pada standar yang digunakan. ISO/IEC adalah kependekan dari *International Organization for Standardization / International Electrotechnical Commision* yang merupakan organisasi internasional independen dan tidak bersifat pemerintahan, dimana para ahlinya berbagi pengetahuan bersama untuk memberi solusi terhadap masalah dan tantangan global mendatang (ISO, 2010).

Penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC) sebagai kerangka dan pedoman pada proses pengembangannya. Alasan menggunakan metode *Network Development Life Cycle* (NDLC) adalah karena metode ini dapat digunakan untuk melakukan pengembangan secara berulang yang

artinya dapat dilakukan perbaikan saat terjadi kekurangan dalam sekali proses pengembangan.

I.2 Perumusan Masalah

Berdasarkan pemaparan latar belakang, dibuat perumusan masalah yang akan menjadi acuan untuk penelitian. Permasalahan yang dibahas adalah:

1. Bagaimana kondisi keamanan jaringan komputer Pemerintah Kabupaten Bandung saat ini?
2. Bagaimana langkah pengembangan untuk meningkatkan keamanan jaringan komputer Pemerintah Kabupaten Bandung?

I.3 Tujuan Penelitian

Berdasarkan perumusan masalah yang telah ditentukan, maka dibuat juga tujuan dari penelitian ini, yaitu:

1. Melakukan identifikasi kondisi keamanan jaringan komputer Pemerintah Kabupaten Bandung saat ini.
2. Memberikan hasil rancangan pengembangan keamanan jaringan komputer berdasarkan permasalahan pada kondisi saat ini.

I.4 Batasan Penelitian

Pada penelitian ini diberikan batasan-batasan yang berfungsi sebagai fokus untuk penelitian yang akan dilakukan. Batasan penelitian adalah sebagai berikut:

1. Penelitian ini hanya dilakukan pada jaringan komputer wilayah kantor Pemerintah Kabupaten Bandung.
2. Penelitian ini menggunakan standar keamanan ISO/IEC 27001 dan poin kebutuhan yang diambil sesuai dengan yang diperlukan pada penelitian ini.
3. Proses penelitian ini menggunakan metode NDLC sampai tahap simulasi.
4. Penelitian ini hanya memberikan rekomendasi desain usulan dan keputusan untuk melakukan implementasi diserahkan seluruhnya kepada pihak DISKOMINFO Pemerintah Kabupaten Bandung.

I.5 Manfaat Penelitian

Manfaat yang diinginkan dalam penelitian ini adalah:

1. Memberikan rekomendasi usulan pengembangan keamanan jaringan komputer Pemerintah Kabupaten Bandung dan memenuhi standar ISO/IEC 27001.
2. Meminimalisir kemungkinan adanya masalah yang terjadi pada proses bisnis Pemerintah Kabupaten Bandung yang dikarenakan oleh kelalaian penggunaan akses *Internet* yang dilakukan oleh pegawai.

I.6 Sistematika Penulisan

Dibagian ini dijelaskan mengenai gambaran sistematika penulisan penelitian untuk mempermudah proses membaca penelitian ini.

1. BAB I Pendahuluan

   Bagian ini menjelaskan mengenai latar belakang, perumusan penelitian, tujuan penelitian, batasan penelitian, dan manfaat penelitian yang akan menjadi inti penelitian.
2. BAB II Tinjauan Pustaka

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

   Bagian ini menjelaskan metodologi yang digunakan dalam proses analisa dan perancangan penelitian ini.
4. BAB IV Analisa Kondisi Keamanan Saat Ini

   Bagian ini menjelaskan data yang didapatkan menganai kondisi keamanan jaringan komputer Pemerintah Kabupaten Bandung saat ini beserta dengan profilnya.
5. BAB V Perancangan Keamanan Usulan

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

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