BAB I

PENDAHULUAN

1.1 Latar Belakang

PT. BPR XYZ merupakan salah satu bank pekreditan rakyat (BPR) ada di provinsi Bali. Dalam menjalankan bisnisnya PT. BPR XYZ memiliki satu kantor pusat, dua kantor cabang dan dua kantor kas. PT. BPR XYZ menguatkan posisinya di empat besar BPR di provinsi Bali (sumber: InfoBank April 2020) sebagai BPR dengan asset besar dan berkinerja baik. PT. BPR XYZ siap untuk memberikan pelayanan terbaik kepada masyarakat dan mendukung perkembangan usaha mikro dan kecil ada di Bali.

Perkembangan teknologi informasi telah menghasilkan berbagai produk dan layanan yang sangat dinamis mengikuti kebutuhan masyarakat termasuk dalam bidang perbankan. Dalam meningkatkan kualitas pelayanan terhadap masyarakat perbankan menyelenggarakan teknologi informasi. Penyelenggaraan teknologi informasi yang dimaksud yaitu sistem elektronik berupa CBS (*core banking system*) yang digunakan untuk proses akhir seluruh transaksi perbankan serta pengkinian data dalam pembukuan. Untuk dapat menjalankan sistem elektronik ini, infrastruktur pusat data (*data center*) menjadi unsur penting yang harus dimiliki oleh institusi perbankan. Pusat Data *(data center)* merupakan tempat untuk sistem elektronik dan komponen lainnya. Tempat ini berfungsi untuk penempatan, penyimpanan maupun pengolahan data (Komisioner & Jasa, 2016).

Dengan demikian data dan informasi yang tersimpan dalam *data center* harus diperhatikan dengan baik. PT. BPR XYZ memiliki *data center* yang digunakan untuk menunjang kegiatan operasional perbankan khususnya menempatkan *server* database, *server* aplikasi maupun *server* lainnya.

Berdasarkan hasil pengamatan pada *data center* PT. BPR XYZ didapatkan bahwa *server* belum terkelola maupun terlindungi dengan baik dan infrastruktur jaringan belum cukup aman sehingga memiliki kerentanan secara logikal. Kerentanan ini terjadi karena berupa *server* yang berjalan sistem operasinya belum diperbarui dan layanan pada *server* yang tidak digunakan status *protocol/port* masih ada yang terbuka (*open*). Infrastruktur jaringan antar kantor yang menghubungkan antar kantor masih menggunakan perangkat teknologi berbasis *wireless* yang memanfaatkan frekuensi untuk menghantarkan sebuah komunikasi sehingga kerentanan terhadap keamanan lebih tinggi dibandingkan teknologi komunikasi lainnya. Selain itu terdapat juga permasalahan terhadap infrastruktur jaringan belum memiliki layanan untuk pendeteksian serangan. Ini terjadi karena *data center* yang berada di PT. BPR XYZ belum ada standarisasinya. Standarisasi yang belum tepenuhi dan dibahas pada penelitian ini yaitu pada aspek keamanan *data center*. *Data center* tidak memiliki standarisasi atau kurang aman ini sangat berbahaya bagi perbankan. Akibat dari *data center* yang kurang aman salah satunya akan adanya kebocoran data. (Budi & Rahardjo, 2005) menyatakan bahwa masalah keamanan pada sistem informasi adalah aspek penting yang sangat penting.

Hasil penelitian yang membahas desain dan analisis *data center* oleh (I Gede Iswara Darmawan, 2015) menyatakan bahwa *server* dan jaringan ada di lingkungan

Fakultas Rekayasa Industri (FRI) Universitas Telkom memiliki celah keamanan. Kendala pada penelitian tersebut adalah belum diketahui lebih detail mengenai kerentanan yang ada sehingga perlu dilakukan prosedur *vulnerability assessment* yang lebih dalam. Selain itu juga belum dijelaskan secara detail desain yang diusulkan. Berdasarkan uraian tersebut maka akan dilakukan analisis lebih dalam pada keamanan *data center* PT. BPR XYZ dan merancang suatu konsep keamanan *data center* usulan dengan menggunakan *framework Open Enterprise Security Architecture* (O-ESA). Metode yang digunakan yaitu metode pengembangan sistem *Network Development Life Cycle* (NDLC). Metode NDLC akan dijadikan metode yang akan digunakan sebagai acuan pada proses pengembangan keamanan *data center* di PT. BPR XYZ. Pada penelitian akan diusulkan desain jaringan antar kantor dan akan dilakukan simulasi untuk membuktikan desain usulan lebih baik dari desain yang ada saat ini.

1.2 Identifikasi Masalah

Berdasarkan latar belakang diatas terdapat identifikasi permasalahan yang ada yaitu :

1. Perusahaan belum pernah menganalisis terhadap keamanan *data center* yang berada di PT. BPR XYZ.
2. Perusahaan belum pernah merancang desain keamanan *data center* dengan standar yang ada.

1.3 Batasan Masalah

Agar penelitian terfokus dan tidak terjadi perluasan pembahasan dari yang dimaksudkan, adapun batasan penelitian ini sebagai berikut :

1. Penelitian ini hanya membahas pada aspek keamanan.
2. Keamanan yang dibahas yaitu keamanan logikal *data center*.
3. Keamanan logikal *data center* hanya membahas kontrol akses jaringan dan pengelolaan terhadap *server*.
4. Penggunaan metode *Network Development Life Cycle* (NDLC) pada penelitian hanya dilakukan sampai tahap ketiga yaitu *simulation prototyping*.
5. Pada metode tahap ketiga hanya disimulasi jaringan antar kantor dengan *virtual private network* (VPN).
6. Standar *Open Enterprise Security Architecture* (O-ESA) pada perancangan keamanan logikal difokuskan pada penggunaan *Security Technology Architecture* hanya pada bagian arsitektur layanan keamanan (*security services*).
7. Penelitian ini hanya memberikan rekomendasi konsep keamanan *data center* kepada PT. BPR XYZ.

1.4 Rumusan Masalah

Adapun rumusan masalah yang dibahas dalam penelitian ini adalah sebagai berikut :

1. Bagaimana kebutuhan desain keamanan *data center* pada PT. BPR XYZ ?
2. Bagaimana solusi perancangan keamanan *data center* pada PT. BPR XYZ menggunakan standar *Open Enterprise Security Architecture* (O-ESA) ?

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Mengidentifikasi kebutuhan desain keamanan *data center* pada PT. BPR XYZ.
2. Merancang desain usulan keamanan *logical security data center* pada PT. BPR XYZ sesuai dengan kebutuhan.

1.6 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut :

1. Memberikan rekomendasi kepada perbankan mengenai bagaimana desain keamanan *data center* usulan yang dapat diterapkan pada nantinya.
2. Desain *data center* usulan memiliki tingkat keamanan yang lebih baik daripada desain *data center* yang ada saat ini.

3. Jika desain *data center* usulan diimplentasikan, perbankan tidak lagi menggunakan jasa pihak ketiga untuk jaringan atau komunikasi antar kantor karena pada desain usulan perbankan sudah mempunyai jaringan *private* sendiri sehingga memberikan efisiensi biaya terhadap perbankan.