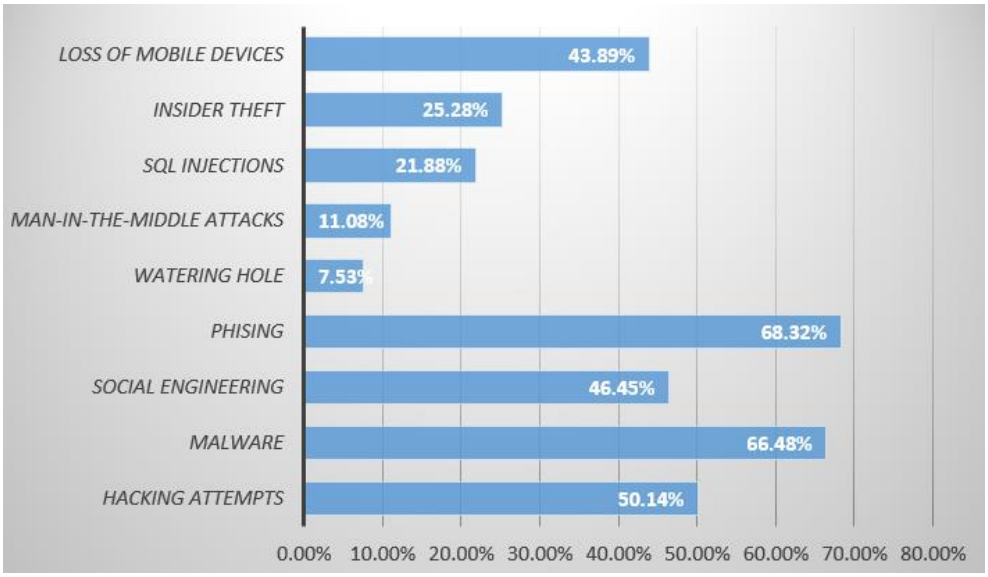
BAB I
PENDAHULUAN

I.1 Latar Belakang

Dewasa ini Teknologi Informasi (TI) telah menjadi suatu hal yang penting dalam menjalankan aktivitas bisnis sebuah organisasi berupa komunikasi untuk pertukaran informasi dan data antar perangkat komputer. Teknologi informasi mencakup berbagai bidang teknologi yang mewadahi seluruh aktivitas bisnis perusahaan dan memicu beralihnya proses bisnis konvensional menjadi proses bisnis yang bersinergi dengan teknologi sehingga memudahkan organisasi dalam menjalankan fungsinya. Untuk penerapannya, TI memerlukan infrastruktur jaringan komputer yang mampu menghubungkan setiap bidang pada sebuah organisasi, sehingga dapat dilakukan integrasi berbagai aplikasi yang digunakan agar akses data dapat dilakukan secara global dan terpusat.

Di lain sisi, perkembangan TI justru mempermudah terjadinya pelanggaran terhadap akses data yang tidak sah dan banyak menyita perhatian publik saat ini, termasuk tim regulasi *cyber* di Indonesia. Bersesuaian dengan Peraturan Menteri Komunikasi dan lnformatika Nomor: 16/PER/M.KOMINF0/10/2010 tentang tentang pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol *Internet*, aspek keamanan teknologi informasi menjadi salah satu aspek penting yang harus diperhatikan. Aspek keamanan teknologi informasi perlu diperhatikan untuk mengamankan setiap informasi yang dimiliki masyarakat, pemerintah sipil, militer, dan dunia usaha. Pengamanan informasi secara teori pada dasarnya ditujukan untuk menjamin integritas informasi, pengamanan kerahasiaan data, ketersediaan informasi, dan pemastian memenuhi peraturan dan hukum yang berlaku (Postel, 2013).

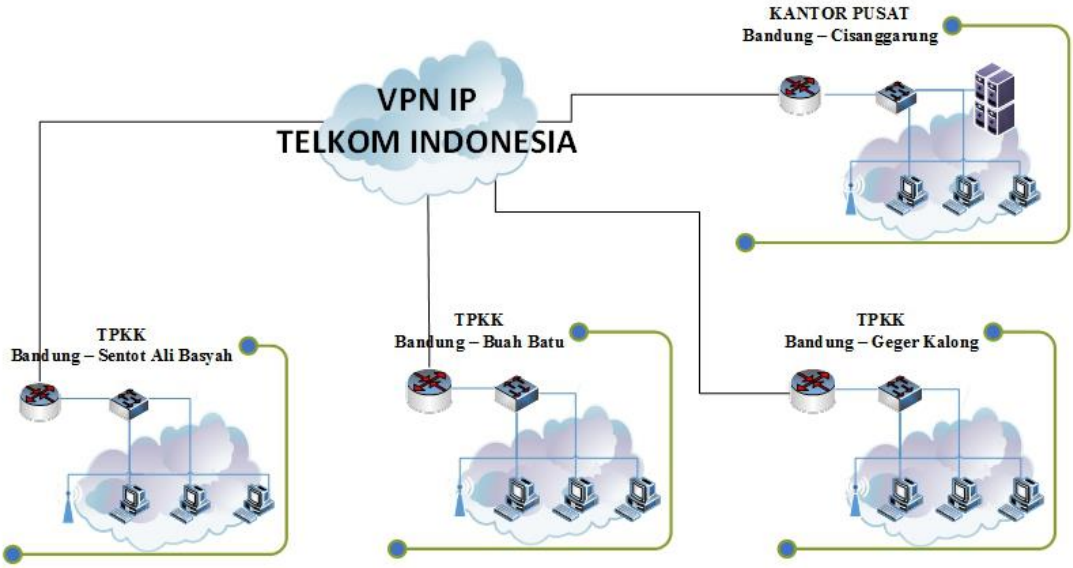
Keamanan informasi pada sebuah organisasi merupakan isu penting mengingat pada tahun 2014 terdapat 48,4 juta serangan di dunia maya dan situs yang paling banyak diserang adalah situs yang memiliki domain go.id. (Kemkominfo, Program Prioritas Tata Kelola Internet, 2016).



Gambar I. 1 Presentase serangan pada organisasi
Sumber: (ISACA, 2015)

Berdasarkan data dari *Information Systems Audit and Control Association (ISACA)* seperti Gambar I.1, jenis serangan yang dialami organisasi pada tahun 2014 adalah *phishing*, *malware*, *hacking*, dan rekayasa sosial (ISACA, 2015). Kasus penyalahgunaan data dapat dialami oleh siapapun dan tidak menutup kemungkinan akan kembali terjadi apabila aspek keamanan jaringan komputer sebuah organisasi tidak ditingkatkan.

Dilihat dari kasus tersebut, keamanan jaringan komputer menjadi kebutuhan bagi setiap organisasi untuk keamanan transaksi data dan informasi tak terkecuali pada sektor kesehatan. Perkembangan TI pada bidang kesehatan didukung dengan adanya pertemuan Menteri Telekomunikasi/TIK dan Menteri Kesehatan dari beberapa negara anggota *Intenational Telecommunication Union* (ITU) dan *World Health Organization* (WHO) dalam upaya menempatkan kemajuan dan pembangunan IT dalam transformasi sektor kesehatan khususnya *e-Health* (Kemkominfo, Digital Health Untuk Kesejahteraan Semua, 2016). Upaya implementasi *e-Health* ini memerlukan faktor pendukung salah satunya adalah teknologi dan keamanan jaringan untuk transaksi pertukaran data.



Gambar I. 2 Topologi jaringan Yakes Telkom saat ini
Sumber: (Yakes, 2016)

Salah satu instansi pemerintah yang bergerak pada bidang kesehatan, yaitu Yayasan Kesehatan Telkom, yang kemudian disebut Yakes Telkom. Yakes Telkom berfungsi untuk memelihara kesehatan karyawan dan pensiunan Telkom beserta keluarganya (Yakes, 2016). Gambar I.2 menggambarkan topologi jaringan pada Yakes Telkom saat ini yang terdiri dari Kantor pusat TPKK Sentot Ali Basyah, TPKK Buah Batu, dan TPKK Geger Kalong.

Saat ini, kantor pusat Yakes Telkom berada di Bandung dan memiliki enam belas TPKK yang tersebar di seluruh Indonesia, yaitu di Medan, Padang, Palembang, Jakarta, Bandung, Surabaya, Makassar, Bali, Jayapura, Jawa Tengah dan Balikpapan. Dengan pasien yang berjumlah lebih kurang 70.000 se-Indonesia. Yakes Telkom didukung oleh beberapa aplikasi untuk menjalankan proses bisnisnya. Aplikasi tersebut berupa *medical record*, *e-apotek* dan aplikasi kepesertaan yang mengelola data peserta Yakes Telkom. Semua aplikasi tersebut berjalan di kantor pusat serta di TPKK dan saling terintegrasi.

Dari hasil observasi yang dilakukan pada Yakes Telkom, keamanan jaringan untuk transaksi pertukaran data pada jaringan LAN saat ini dinilai kurang baik masih terdapat banyak celah kerentanan terhadap aset yang dimiliki. Seperti belum adanya

kebijakan yang membatasi hak akses user dalam menggunakan jaringan *Internet.* Selain itu juga belum optimalnya manajemen terhadap *server,* sehingga penomoran pada *port server* masih *default* dan *port server* tersebut dalam keadaan terbuka.

Mengacu pada Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi, salah satu standar keamanan sistem informasi yang digunakan, yaitu ISO/IEC (*International Organization for Standardization/International Electrotechnical Commission*). ISO/IEC merupakan standar internasional yang dapat digunakan organisasi sebagai pedoman dalam pembuatan desain keamanan infrastruktur jaringan serta pengembangan selanjutnya. ISO/IEC 27000 *series* memberikan rekomendasi praktik terbaik untuk keamanan sistem informasi (ISMS, *Information Security Management System*) yang didefinisikan oleh standar ini dalam konteks C-I-A: *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availabity* (ketersediaan). *International Organization for Standardization* adalah organisasi internasional *non*-pemerintah (bersifat independen) yang beranggotakan 163 badan standar nasional. Melalui anggotanya, menyatukan para ahli untuk berbagi pengetahuan dan mengembangkan pasar standar internasional yang relevan yang mendukung inovasi dan memberikan solusi untuk tantangan global (ISO 27000, 2016).

Mengacu pada standar ISO/IEC 27000 *series,* Tabel I.1 menggambarkan beberapa *domain* manajemen dan kontrol keamanan informasi yang belum diterapkan pada Yakes Telkom.

Tabel I. 1 Manajemen dan kontrol keamanan informasi Yakes Telkom saat ini
Sumber: (Data Penelitian Yakes Telkom, 2017)

Domain	Control
Operations security	• Penerapan sistem *logging* dan *monitoring* untuk merekam setiap aktivitas *user,* kegagalan sistem, ataupun keperluan dokumentasi • Penerapan sistem untuk *management vulnerability*
Organization of information security	Kebijakan keamanan dan kontrol hak akses jaringan pada organisasi

Information security incident management	Adanya sistem deteksi terhadap insiden terkait keamanan informasi

Aspek keamanan teknologi menjadi sangat penting karena berkaitan langsung dengan keamanan sistem informasi. Keamanan sistem informasi dapat diartikan sebagai kebijakan, prosedur, dan pengukuran teknis yang digunakan untuk mencegah akses yang tidak sah, perubahan program, pencurian atau kerusakan fisik terhadap sistem informasi yang menyebabkan kerugian pada organisasi. Penerapan keamanan sistem informasi akan memberikan perlindungan terhadap proses bisnis organisasi agar dapat terhindar dari kemungkinan risiko yang terjadi (ISO/IEC, 2014).

Pengembangan dan implementasi sistem merupakan sebuah alternatif dalam berapresiasi untuk mendalami suatu kajian ilmu. Untuk itu diperlukan landasan atau metodologi yang dijadikan pedoman pada proses pelaksanaanya. Pada penelitian ini, metode pengembangan yang digunakan adalah *Network Development Life Cycle* (NDLC). *Network Development Life Cycle* merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, siklus pengembangan aplikasi dan analisis distribusi data. Jika masih terdapat kelemahan atau kekurangan, NDLC memungkinkan untuk melakukan pengembangan secara berulang (Goldam, 2001).

I.2 Perumusan Masalah

Setelah membahas mengenai latar belakang, dibuat perumusan masalah yang akan dijadikan acuan untuk menentukan arah penilitan. Adapun rumusan masalah penelitian ini adalah:

1. Bagaimana kondisi keamanan infrastruktur LAN pada Yakes Telkom Bandung saat ini?
2. Bagaimana usulan rancangan keamanan infrastruktur LAN pada Yakes Telkom Bandung dengan menggunakan metode NDLC dan standar IEC/ISO 27000 *series*?

I.3 Tujuan Penelitian

Tujuan adanya penelitian sebagai berikut:

1. Memperoleh kondisi keamanan infrastruktur LAN saat ini pada Yakes Telkom Bandung.
2. Memperoleh usulan rancangan keamanan infrastruktur LAN pada Yakes Telkom Bandung dengan menggunakan metode NDLC dan standar IEC/ISO 27000 *series*.

I.4 Batasan Penelitian

Batasan dari penelitian ini adalah sebagai berikut:

1. Penelitian ini fokus terhadap keamanan infrastruktur LAN (wilayah kantor pusat Yakes Telkom Bandung).
2. Penggunaan metode NDLC pada penelitian ini hanya dilakukan sampai tahap *simulation prototyping.*
3. Penelitian ini disesuaikan dengan menggunakan standar ISO/IEC 27002:2013
4. Penelitian ini menggunakan Mikrotik *RouterOS* dan *Packet Tracer* versi 6.2 dalam melakukan pengujian keamanan jaringan usulan.

I.5 Manfaat Penelitian

Manfaat yang didapatkan penelitian ini adalah sebagai berikut:

I.5.1 Manfaat Teoritis

1. Menambah pengetahuan peneliti mengenai bagaimana merancang keamanan infrastruktur jaringan yang efektif dan efisien.
2. Sebagai informasi masukan untuk mengembangkan penelitian lebih lanjut khususnya mengenai perancangan keamanan infrastruktur LAN.

I.5.2 Manfaat Praktis

1. Menyediakan rancangan keamanan infrastruktur LAN yang sesuai dengan kebutuhan Yakes Telkom Bandung.

2. Memberikan rekomendasi dari segi keamanan infrastruktur LAN dan referensi perangkat yang harus digunakan.

I.6 Sistematika Penulisan

Penelitian ini akan diuraikan dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

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

BAB II LANDASAN TEORI

Bab ini berisi literatur yang sesuai dengan permasalahan yang dihadapi, penelitian terdahulu yang memiliki keterkaitan dengan penelitian yang sedang dilakukan, dan menjelaskan metode NDLC yang digunakan.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan mengenai langkah-langkah penelitian secara rinci meliputi tahapan mengidentifikasi, tahap analisis, tahap desain, tahap simulasi, dan tahap akhir dari penelitian ini.

BAB IV ANALISIS KONDISI SAAT INI

Bab ini berisi penjelasan kondisi keamanan infrastruktur LAN pada Yakes Telkom yang meliputi profil lembaga, keamanan jaringan LAN, dan perangkat keamanan jaringan yang digunakan saat ini.

BAB V PERANCANGAN KEAMANAN JARINGAN USULAN

Bab ini berisi penjelasan mengenai hasil perancangan keamanan LAN usulan yang meliputi keamanan jaringan, perangkat keamanan jaringan usulan, pengujian keamanan jaringan usulan pada *simulator*, dan hasil pengujian keamanan jaringan usulan.

BAB VI KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan apa yang dapat diambil dari hasil perancangan yang dilakukan selama melakukan penelitian dan saran untuk perusahan kedepannya.