BAB I

PENDAHULUAN

1.1 Latar Belakang

Dewasa ini, pengguna email (*electronic mail*/surat elektronik) sebagai salah satu sarana komunikasi modern sudah merupakan hal yang sangat umum. Terbukti dengan luasnya cakupan pengguna dari email itu sendiri. *Email* saat ini selain digunakan untuk berkirim surat antar pribadi, juga digunakan sebagai sarana komunikasi antar instansi. *Email* memiliki beberapa keunggulan dibandingkan surat konvensional terutama dalam kaitannya dengan efisien waktu dan biaya. Tetapi hal tersebut pulalah yang menjadi kelemahan *email* itu sendiri. Oleh karena dalam mengirim *email* tidak memerlukan biaya serta sangat cepat, seringkali hal ini dimanfaatkan oleh para *spammer* (orang yang mengirimkan *email spam*/sampah) untuk dengan mudah melakukan aktivitasnya.

Spam merupakan istilah umum untuk menyebut *email* komersial maupun non komersial yang tidak diinginkan. Contoh dari *email spam* adalah *email* promosi produk, iklan program investasi, *virus, spyware*, dan lain-lain. Kehadiran *email spam* ini selain membuang waktu *user* untuk membaca dan menghapusnya, juga mengakibatkan melonjaknya pemakaian *network bandwidth* secara signifikan. Apabila hal ini dibiarkan terus menerus, akan mengakibatkan kerugian yang besar baik bagi user sebagai individu maupun bagi perusahaan yang notabene memerlukan kinerja jaringan yang optimal.

Sementara itu, serangan-serangan *spam, virus*, dan *malware* mengakibatkan kerugian. Waktu yang dipakai rata-rata pengguna adalah sekitar 5 hingga 10 menit untuk mengatasi *spam*. Biaya pembersihannya diperkirakan mencapai USD 500 per *desktop*. Hal yang lebih merugikan lagi adalah kehilangan data. Kehilangan data bisa merusak nama baik sebuah perusahaan, menurunkan nilai saham, dan merusak reputasi.

Komunikasi elektronik dan data berjalan adalah titik kehilangan data yang paling signifikan bagi enterprise. *Firewall* dan solusi keamanan jaringan lain yang ada saat ini tidak memiliki kemampuan pencegahan hilangnya data untuk mengamankan data berjalan. Kendali-kendali penting, seperti pemeriksaan konten, blokir komunikasi yang berisi data penting dan *enkripsi* tidak ada. Diperkirakan sekitar 60 juta orang memiliki data pribadi yang terlihat ke luar dalam 13 bulan terakhir. Selain itu, diperkirakan 20 milyar dolar terbuang untuk biaya-biaya pembersihan dan hilangnya produktivitas.

Jika pada PT. Telekomunikasi Indonesia, Tbk tidak memiliki perlindungan terhadap *spam*, bisa menerima banyak sekali *email-email* sampah ini, sehingga terpaksa membacanya satu per satu sebelum menentukan apakah *email* ini sampah atau informasi penting. Akibatnya produktivitas pegawai juga akan menurun.

Bila kita menerima satu *email* yang mencurigakan, kita bisa memeriksa reputasi si pengirim dengan memeriksanya di *senderbase.org*, sebuah *website* yang memberikan informasi mengenai statistik seluruh *traffic* di *Internet*. Informasi ini dipakai oleh

beberapa perangkat *anti-spam* untuk menentukan apakah *email-email* tertentu adalah *spam* atau *legitimate*.

Solusi yang diambil oleh PT. Telekomunikasi Indonesia, Tbk adalah menggunakan *Vendor Ironport* dari *Cisco System* yang seperti telah diketahui merupakan langkah baik agar produktivitas, kenyamanan bisnis dan kemanan data terjaga dengan baik. Melihat kasus seperti yang diatas, tentu saja perlu melakukan sebuah pemecahan masalah secara tepat. Secara terurai kasus tersebut dapat diatasi oleh *Ironport* yang merupakan penggambaran langkah tepat bagi PT. Telekomunikasi Indonesia, Tbk untuk menanggulangi email spam.

Akan tetapi dengan adanya *Ironport* pada perusahaan tersebut tidak selamanya akan membantu dalam mengatasi masalah yang telah disebutkan diatas. Maka pentingnya melakukan monitoring demi kelancaran produktifitas perusahaan dalam mengelola email, maka dari itu dapat dibuat sebuah karya ilmiah dengan judul "MONITORING EMAIL MENGGUNAKAN CISCO IRONPORT C360 PADA PT. TELEKOMUNIKASI INDONESIA, TBK".

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah disebutkan di atas maka masalah yang terjadi adalah bagaimana cara melakukan penganalisaan dengan menggunakan Cisco Ironport terhadap email keluar maupun email yang masuk.

1.3 Maksud dan Tujuan

1.3.1 Maksud

Untuk mengetahui bagaimana cara menggunakan Cisco Ironport, selain itu maksud yang ingin dicapai adalah melakukan monitoring sistem keamanan email gateway dengan menggunakan Vendor Cisco Ironport untuk membantu produktivitas kerja pada Intern PT. Telekomunikasi Indonesia,Tbk.

1.3.2 Tujuan

Adapun tujuan dari penelitian ini adalah memberikan informasi adanya Threats yang berada pada email yang masuk maupun keluar bagi pihak yang membutuhkan.

1.4 Batasan Masalah

Memonitoring email yang masuk maupun keluar dengan menggunakan Cisco Ironport C360 dan memberikan penanganan terhadap email yang bermasalah di PT. Telekomunikasi Indonesia, Tbk.

1.5 Metode Penelitian

Dalam melaksanakan system pelaksnaan kerja praktek ini, penulis melakukannya dengan cara menerapkan metodologi-metodologi. Adapun metodologi yang digunakan dalam pendekatan system pelaksanaan dalam menyusun laporan kerja praktek sebagai berikut :

a. Metode Literatur

   Dalam hal ini penulis mengambil dan menggunakan beberapa buku sebagai sumber referensi dalam membuat teori-teori yang sangat menunjang materi dalam pelaksanaan kerja praktek ini, sehingga penulis dapat membuat laporan sesuai dengan yang diharapkan.

b. Metode Praktek

   Dalam hal ini penulis melakukan praktek secara nyata dalam hal monitoring email masuk maupun keluar dengan menggunakan Cisco Ironport C360 di PT. Telekomunikasi Indonesia, Tbk.

c. Metode Wawancara

Dalam hal ini dilakukan wawancara dengan pegawai PT. Telekomunikasi Indonesia, Tbk divisi IS Security Operation guna mendapatkan pengetahuan yang terkait dengan kegiatan kerja praktek.

1.6 Sistematika Penulisan

Untuk memberikan gambaran dengan jelas mengenai penulisan laporan ini, maka dibawah ini akan dijelaskan mengenai sistematika penulisan laporan, sebagai berikut :

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang masalah, perumusan masalah, maksud dan tujuan, batasan masalah, metoda penelitian dan sistematika laporan kerja praktek.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan ruang lingkup instansi tempat penulis melakukan Kerja Praktek, yaitu PT. Telekomunikasi Indonesia, TBK, seperti sejarah singkat, tempat dan kedudukan, bentuk dan badan hukum, bidang pekerjaan hingga struktur organisasi instansi tersebut. Serta landasan teori yang digunakan sebagai bahan penelitian kerja praktek tersebut.

BAB III PEMBAHASAN

Bab ini menguraikan kegiatan penulis selama melakukan kerja praktek, mulai dari observasi, kemudian tahap analisis sampai dengan tahap perancangan dan implementasi, berdasarkan landasan teori yang telah penulis dapatkan.

BAB IV PENUTUP

Bab ini berisi kesimpulan dari pekerjaan yang telah dilakukan dan saran untuk pengembangan sistem yang lebih baik lagi.

Daftar Pustaka

Lampiran