

ABSTRAK

Internet adalah salah satu teknologi informasi yang perkembangannya sangat pesat dan merata hampir di seluruh dunia. Seperti surat-menyurat yang berawal dari kertas biasa telah tergantikan oleh surat elektronik atau *email* karena keberadaan Internet. Internet membawa banyak keuntungan, namun tidak meninggalkan dampak negatif yang dapat ditimbulkan. Internet dapat berdampak negatif apabila pemanfaatannya tidak diawasi. Misalnya, terjadi peretasan data sebuah perusahaan oleh pihak yang tidak bertanggung jawab, hal tersebut dapat terjadi karena Internet yang menghubungkan perusahaan tidak dilindungi oleh sistem proteksi. Risiko yang dimiliki oleh teknologi Internet tidak sebatas peretasan dari jaringan eksternal ke jaringan internal melainkan memungkinkan untuk sebaliknya. Seperti contoh ketika seorang pegawai perusahaan melakukan *surfing* di Internet kemudian tanpa sengaja mengakses situs yang menyimpan *malware* dan menginfeksi komputer yang digunakannya sehingga merusak data penting yang terdapat pada komputer tersebut.

Penelitian yang dilakukan di kantor Pemerintah Kabupaten Bandung mendapatkan hasil bahwa jaringan internal yang seharusnya diperuntukan bagi urusan kelembagaan belum optimal dalam penggunaannya, karena terdapat celah keamanan dalam mengakses *website* yang seharusnya diblokir. Maka dari itu, perlu dilakukan optimasi. Optimasi pada penelitian ini dilakukan diawali dari identifikasi infrastruktur keamanan jaringan yang ada, kemudian dianalisa berdasarkan kebutuhan dan standar ISO/IEC 27000 *Series*. Metodologi yang digunakan dalam melakukan penelitian ini yaitu NDLC (*Network Development Life Cycle*).

Hasil dari penelitian ini dapat dijadikan cetak biru atau pedoman bagi pihak Pemerintah Kabupaten Bandung dalam upaya optimasi keamanan infrastruktur jaringan yang ada.

Kata kunci:

Internet, keamanan jaringan, ISO/IEC 27000 *Series*, NDLC.