

ABSTRAK

Setiap lembaga pemerintah pasti memiliki suatu pusat data yang menjadi tempat berkumpulnya seluruh data proses bisnis pemerintahan. Agar pusat data dapat bekerja dengan baik diperlukan jaringan komputer yang memiliki keamanan yang baik juga. Keamanan jaringan komputer menjadi kunci pertahanan informasi pemerintah disisi non fisik, karena jaringan komputer merupakan lalu lintas dari seluruh informasi atau komunikasi data. Bagi pemerintah, informasi yang dikirimkan dan diterima adalah rahasia dan tidak boleh bocor ke tangan yang salah.

Penelitian ini dilakukan di salah satu SKPD di Pemerintah Kabupaten Bandung, yaitu DISKOMINFO. Pada hasil analisis ditemukan celah keamanan seperti tembusnya keamanan *web protection* dengan menggunakan *proxy*, terjadinya kesalahan perangkat karena beban yang berlebih, dan terdapat *sub-domain* yang belum terpenuhi pada standar ISO/IEC 27001:2013. Solusinya adalah dengan melakukan optimasi keamanan *web protection*, perangkat, dan memberikan langkah yang harus dilakukan untuk memenuhi standar yang belum terpenuhi.

Hasil penelitian ini adalah optimasi keamanan jaringan dalam mencegah penggunaan *proxy* secara ilegal dengan 3 cara *block* yaitu mem-*block* IP address, menggunakan *regular expression*, dan menggunakan aturan *whitelist*. Hasil lainnya adalah usulan perangkat Sophos SG 450 yang dapat mengganti perangkat saat ini dalam mengelola pengguna, dan usulan berupa *template* dokumen yang seharusnya dibuat oleh DISKOMINFO agar memenuhi standar ISO/IEC 27001:2013.

Kata Kunci:

Blacklist, Internet, Keamanan, Keamanan Jaringan, Optimasi, Whitelist.