ABSTRAK

Penggunaan *e-mail* sekarang sudah menjadi bagian penting dari komunikasi data karena kemudahan dan efisiensinya. Keberadaan *e-mail* tentunya tidak lepas dari adanya *server* yang mengelolanya. Pemilihan *server* sangat bergantung pada kebutuhan. Zimbra menjadi salah satu pilihan alternative *mail server* yang cocok saat aspek kemudahan dan kemurahan pembangunan *mail server* menjadi prioritas, karena sifatnya yang *open source*. Hal ini akan menjadi lebih efisien lagi saat pengadaan *mail server* tersebut juga bisa dilakukan tanpa perlu menyediakan *resource* untuk sebuah *server*. Teknologi yang memungkinkan adalah dengan *cloud computing*, dan salah satu *platform* yang sedang banyak dikembangkan adalah Ubuntu Enterprise Cloud (UEC). Namun karena layanan *cloud computing* ini sebagian besar berada di lingkup area jaringan paket maka aspek keamanannya juga perlu perhatian yang cukup. Dikarenakan rentannya aspek keamanan ini maka diperlukan suatu sistem keamanan untuk menjaga data pada *server* penyedia layanan.

Tugas Akhir ini akan membahas lebih lanjut aspek keamanan data pada Zimbra berbasis UEC tersebut. Pada pengujiannya diimplementasikan salah satu sistem keamanan pencegahan kebocoran data yaitu dengan metode *Data Loss Prevention* (DLP) menggunakan MyDLP yang dilengkapi firewall. MyDLP sendiri merupakan *software* gratis dan *open source data loss prevention* yang bisa mencegah *data flow* yang mengandung informasi penting, misalkan nomer kartu kredit, ataupun data – data penting perusahaan lain yang tidak boleh diakses oleh pihak yang tidak berwenang. Setelah pengujian akan dianalisis aspek *privacy*, *confidentiality*, *acces control* dan *availability* data terhadap pengaruh adanya *data loss prevention* tersebut pada Zimbra *mail server*.

Dari pengujian dapat disimpulkan bahwa tidak semua aspek keamanan bisa diatasi dengan penambahan *data loss prevention* dengan firewall. Sistem hanya mampu memberikan keamanan *acces control,availability* dan *confidentiality* data, namun tidak untuk *privacy*. terlihat dari pengujian *sniffing* yang berhasil dilakukan oleh *attacker*. Ini memperlihatkan bahwa *data loss prevention* masih memiliki kekurangan dan dirancang hanya sebagai pertahanan keamanan terakhir terhadap keberadaan data.

Kata kunci : C*loud Computing, UEC, Zimbra, MyDLP*