BAB V

PENUTUP

5.1. Kesimpulan

Dari proses penelitian dengan melakukan sebuah pengujian menggunakan metode terhadap keamanan web portal Pemerintah, maka dapat menyimpulkan beberapa hal :

1. Salah satu faktor pendukung dalam membangun keamanan web portal Pemerintah adalah faktor dari *Confidentiality, Availability* dan *Integrity* yang dijabarkan berdasarkan kelemahan pada web Portal yang mengancam pada konsep keamanan informasi itu sendiri yaitu : *Confidentiality, Integrity* dan *Availability.* Dengan begitu rumusan masalah pada point satu sudah terpenuhi jawabannya.
2. Dengan menggunakan BSIMM (*Building Security In Maturity Model*) dengan berdasarkan kategori *Attack Model,* bisa menjadikan solusi atas kerawanan dan kelemahan terhadap keamanan web portal Pemerintah yang mengancam pada salahsatu faktor pendukung dalam membangun keamanan web portal Pemerintah yaitu : *Confidentiality, Integrity* dan *Availability* dan menghasilkan sebuah model keamanan web portal Pemerintah. Dengan begitu pertanyaan kedua dalam rumusan masalah sudah terjawab.
3. Metode *Penetration Testing,* merupakan cara yang cukup baik dan optimal dalam mengukur suatu kemanan web portal
4. Berdasarkan hasil analisa terhadap data yang sudah di kumpulkan oleh penulis, hampir 98% web portal Pemerintah terancam serangan *Injection Flaw* dan *Cross Site Scripting*, sehingga bisa dikatakan tidak aman dan teridentifikasi serangan – serangan yang mengganggu *confidentiality, integrity* dan *availability.*
5. Pendekatan BSIMM (*Building Security in Maturity Model*) dapat digunakan sebagai perancangan setrategi maupun rencana dalam membangun keamanan informasi.

6. Perlu adanya c*entralized Server* khusus atau hosting maupun *collocation server* khusus web portal Pemerintah agar terjaga keamanannya
7. Hasil analisa disini, terbukti bahwa pada level Pemerintah masih belum *aware* terhadap keamanan web portal untuk jangka panjang dan pertimbangan terhadap *value asset* .

Setiap organisasi memiliki kebijakan masing-masing dalam menangani keamanan sistem informasi, sehingga tidak ada sebuah cara spesifik yang dapat digunakan pada semua organisasi.

5.2. Saran

1. Membentuk suatu organisasi keamanan response cepat terhadap insiden keamanan informasi pusat, seperti : *Indonesian Computer Security Response Centre* (CSRC), dalam hal ini Penulis sedang mengembangkannya menggunakan *OpenFisma* sebagai *Knowledge Management*nya, untuk Pemerintahan sebagai induk *Computer Security Incident Response Team* (CSIRT) *Coordinating Centre*, guna mengoptimalkan strategi dan model keamanan web portal Pemerintah serta monitoring model ancaman web aplikasi saat ini, khususnya Pemerintah.
2. Membuat sebuah *Centre of Exellence for Information Security* sebagai pendukung dan pengkajian sebuah keamanan informasi Indonesia, khususnya Pemerintah, guna menyeimbangkan antara *Technology*, *People* dan *Process* pada sebuah keamanan informasi.
3. Mengimplemtasikan standar keamanan web portal Pemerintah yang sudah teruji dalam penelitiannya, sebagai contoh : pengimplementasian *web application firewall* pada setiap *web server* Pemerintah Pusat dan Daerah.
4. Pihak instansi Pemerintah terkait yang menangani keamanan informasi khususnya, untuk selalu mengevaluasi keamanan web portal Pemerintah, mulai dari level Pemerintah Pusat hingga Daerah.
5. Perlunya pemahaman prosedur dalam membangun sebuah web portal, tak hanya pada sisi desain ataupun konten. Tetapi sisi *development life cycle*

wajib untuk dipahami, khususnya *Secure Development Lifecycle* (SDL).

6. Dengan hasil penelitian keamanan web portal Pemerintah ini khususnya tingkat Pusat. Maka untuk web portal Pemerintah Daerah, ada baiknya diadakan audit keamanan web portal juga. Agar terselenggaranya keamanan informasi yang menyeluruh.
7. Mungkin hasil penelitian ini dapat di jadikan sebuah surat edaran dari instansi terkait, sebagai *warning* bahwa masih adanya indikasi ancaman terhadap web portal tersebut.

Demikian kesimpulan dan saran ini, dipaparkan secara garis besar secara keseluruhan. Semoga dapat mengisi kekurangan dalam penelitian berikutnya.