

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Sekolah Darma Bangsa (SDB) adalah Sekolah Nasional di Provinsi Lampung, berdiri pada tahun 2007 di bawah naungan Yayasan Darma Bangsa Edukasi. Letak sekolah sangat strategis, terletak di jantung ibu kota provinsi Lampung, Bandarlampung. SDB memberikan pendidikan jenjang meliputi: TK, SD, SMP dan SMA, dengan izin operasional yang dikeluarkan oleh Dinas Pendidikan dan Perpustakaan Kota Bandarlampung. Dengan didukung sarana dan prasarana pendidikan yang modern, serta tenaga pengajar yang handal baik dari dalam maupun luar negeri. Sampai saat ini sudah 16 tahun umur perjalanan SDB dalam dunia pendidikan untuk mencerdaskan anak bangsa, sampai saat ini SDB memiliki 47 kelas dengan jumlah siswa sampai saat ini mencapai 920 siswa yang terus bertambah setiap tahunnya.[1]

Namun, seiring dengan perkembangan teknologi dan peningkatan penggunaan sistem informasi, keamanan informasi menjadi perhatian utama. Menurut Kementerian Komunikasi dan Informatika (Kominfo) 2012, 50% website diretas dengan domain go.id, biasanya digunakan instansi pemerintah. Djoko Purwono, Kepala Bidang Pengembangan Infrastruktur Teknologi Informasi dan Komunikasi Dinas Kominfo Jatim, menyebutkan serangan disebabkan ketidakpuasan terhadap pelayanan atau data di website pemerintah, merusak data, dan mengunci jaringan. Diperlukan pelatihan bagi operator website pemerintah untuk melawan serangan hacker dan menjaga kinerja pemerintah. Beberapa website pemerintah di Jatim, seperti [www.disnak-jatim.go.id](http://www.disnak-jatim.go.id), [www.dinsosjatim.go.id](http://www.dinsosjatim.go.id), diserang. Kerusakan data juga terjadi melalui akses jaringan internet WiFi. Monitoring Kominfo menunjukkan sekitar 400 dari 600 jaringan WiFi di Surabaya tak terkunci, meningkatkan potensi perusakan dan penyerangan data oleh hacker. Hacker yang menyerang dunia cyber berasal dari Cina, Rusia, dan Eropa. Hacker yang melakukan penyerangan belum tentu merusak, namun bisa juga

melakukan scanning, membaca data, mengcopy data, dan merubah angka.[2] Pelatihan bagi operator website pemerintah sangat diperlukan untuk melawan serangan hacker dan menjaga kinerja pemerintah.

Beberapa penelitian pernah melakukan perubahan pada tingkat keamanan sebuah website. Menurut (.R., RachmaniahM., & MustafaB. 2016) dalam tulisan berjudul Penilaian Risiko Kerawanan Informasi di Perpustakaan X, hasil penelitian menunjukkan bahwa dari 4 kategori kerentanan informasi di Perpustakaan X berada pada kategori 3 atau cukup rentan dengan 22 area perhatian atau sebesar 42,31% [3].

Penerapan sistem informasi perpustakaan yang berkembang pesat menimbulkan risiko yang dapat mengancam disebabkan kegagalan pustakawan dalam menilai sumber ancaman. Penilaian risiko merupakan bagian dari manajemen risiko, dilakukan untuk menilai seberapa besar kemungkinan adanya ancaman dan kerentanan terhadap sistem informasi beserta aset-asetnya. OCTAVE Allegro merupakan framework yang fokus pada penilaian risiko terhadap aset informasi kritical dan relatif mudah digunakan karena tidak membutuhkan banyak resource untuk melakukannya. Hasil akhir dari penelitian ini menunjukkan bahwa pada perpustakaan UIN Raden Fatah Palembang dampak yang paling tinggi risiko berdasarkan OCTAVE Allegro yaitu pada *IT Risk* dan *Financial*, karena belum adanya anggaran khusus untuk pembiayaan dalam pengelolaan dan perawatan untuk sistem SLiMS (*Senayan Library Management System*) di perpustakaan UIN Raden Fatah Palembang[4].

Penelitian lain di perusahaan percetakan Documedia menunjukkan bahwa instansi tersebut tidak menerapkan praktek keamanan yang baik, sehingga memiliki kelemahan di beberapa area. Documedia merupakan sebuah perusahaan yang bergerak di bidang percetakan. Untuk mengantisipasi hal-hal yang tidak diinginkan berkaitan dengan cara pelayanan dan pengerjaan yang tidak terorganisir maka dilakukan manajemen resiko. Penilaian risiko dan juga mitigasi risiko menggunakan framework OCTAVE Allegro yang terdiri dari tiga fase dengan pengumpulan data menggunakan wawancara terhadap 4 orang informan. Hasil dari penilaian mengungkapkan bahwa instansi tidak menerapkan praktek keamanan yang baik sehingga memiliki kelemahan di beberapa area. Strategi perlindungan

instansi kurang berjalan baik dikarenakan pegawai belum mendapatkan pelatihan mengenai keamanan informasi.[5].

Selain itu, aplikasi edukasi online seperti Edmodo juga menghadapi risiko keamanan informasi. Pada penelitian ini digunakan aplikasi Edmodo sebagai obyek studi kasus. Edmodo merupakan satu dari berbagai media edukasi terbesar di dunia berbasis online yang memiliki 100 juta member yang terdiri 400.000 sekolah yang bergabung dengan aplikasi ini. Jumlah yang lumayan besar ini memunculkan beberapa risiko yang dapat muncul terkait dengan Edmodo, seperti email resmi yang digunakan untuk daftar bisa disalahgunakan dan diperjual belikan, lalu di dalam Edmodo juga memiliki 700 juta lebih materi yang digunakan untuk edukasi yang memiliki kemungkinan terjadinya kebocoran materi. Dari proses penelitian, didapatkan hasil pada salah satu *worksheet* 10 OCTAVE Allegro dengan skor *relative risk score* 34 yang memiliki arti bahwa obyek yang dilakukan penilaian (*assessment*) memiliki kepentingan yang cukup tinggi untuk ditindaklanjuti.[6].

Oleh karena itu, tingkat keamanan informasi pada website sekolah menjadi hal yang perlu mendapatkan perhatian khusus. Metode evaluasi yang dapat digunakan adalah OCTAVE Allegro, yang memfokuskan pada evaluasi tingkat keamanan informasi.

## 1.2 Rumusan Masalah

Perumusan masalah dari tesis ini adalah sebagai berikut:

1. Bagaimana hasil tingkat keamanan informasi pada website sekolah menggunakan metode Octave Allegro?
2. Apa rekomendasi dan langkah perbaikan yang dapat diambil berdasarkan hasil evaluasi untuk meningkatkan keamanan website sekolah?

### **1.3 Ruang Lingkup**

Ruang lingkup penelitian ini meliputi:

1. Analisis tingkat keamanan informasi pada website sekolah.
2. Implementasi metode Octave Allegro dalam tingkat keamanan informasi pada website sekolah.
3. Studi kasus pada website sekolah sebagai objek penelitian.

### **1.4 Tujuan Penelitian**

Tujuan dari penelitian ini adalah:

1. Menganalisis Masalah Keamanan Informasi pada Website Sekolah.
2. Mengidentifikasi Faktor-faktor yang Mempengaruhi Keamanan Informasi.
3. Memberikan Rekomendasi untuk Peningkatan Keamanan dan Kualitas Website.

### **1.5 Manfaat Penelitian**

Manfaat dari penelitian ini adalah:

1. Peningkatan Kualitas Layanan Pendidikan.
2. Perlindungan Terhadap Serangan Siber pada website sekolah.
3. Kontribusi pada Pengembangan Metodologi Evaluasi Keamanan.
4. Penyediaan Informasi Strategis dari hasil evaluasi keamanan website.

### **1.6 Sistematika Penulisan**

#### **BAB I PENDAHULUAN**

Dalam pendahuluan tercantum antara lain latar belakang, ruang lingkup, rumusan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

## **BAB II TINJAUAN PUSTAKA**

Bab ini memuat tentang teori-teori yang mendukung penelitian yang akan dilakukan oleh penulis/peneliti. Penelitian yang menggunakan analisis statistik, bab ini memuat kerangka pikir dan hipotesis (bila diperlukan).

## **BAB III METODOLOGI PENELITIAN**

Dalam bab ini berisi objek penelitian, alat dan bahan, metode pengumpulan data, prosedur penelitian, pengukuran variabel dan metode analisis (metode-metode pendekatan penyelesaian permasalahan yang dipakai dan metode analisis data).

## **BAB IV HASIL DAN PEMBAHASAN**

Dalam bab ini disajikan hasil, implementasi, analisis dan pembahasan penelitian. Hasil dan implementasi dapat berupa gambar alat/program dan aplikasinya. Untuk penelitian lapangan hasil dapat berupa data (kualitatif maupun kuantitatif). Analisis dan pembahasan berupa hasil pengolahan data.

## **BAB V KESIMPULAN DAN SARAN**

Dalam bab ini disajikan simpulan dan saran dari hasil pembahasan.