BAB I
PENDAHULUAN

1.1 Latar Belakang

Pemanfaatan teknologi informasi dan sistem informasi untuk aktivitas organisasi merupakan bagian yang tidak terpisahkan dari suatu perusahaan karena dapat membantu meningkatkan efektivitas dan efisiensi proses bisnis organisasi atau perusahaan. Tetapi untuk mencapai hal tersebut, diperlukan adanya pengelolaan TI yang baik dan benar agar keberadaan TI mampu menunjang kesuksesan organisasi dalam pencapaian tujuannya. Bagi sebuah organisasi baik kecil, menengah, maupun besar kebutuhan keamanan terhadap informasi dan data merupakan sesuatu yang harus dipenuhi karena hal itu dapat mempengaruhi reputasi dan kredibilitas organisasi tersebut. Sehingga, saat ini keamanan informasi menjadi sangat penting bagi organisasi atau perusahaan. ancaman terhadap integritas dan keamanan informasi dan data telah meningkat.

Setiap hari ditemukan kasus peretasan dan eksploitasi dengan cara yang baru. Untuk itu menemukan kerentanan pada sistem dan menginstal *patch* keamanan terbaru telah menjadi sesuatu yang penting bagi setiap organisasi yang terhubung ke internet (Bau, Bursztein, Gupta, & Mitchell, 2010). Pada tahun 2018, *Symantec Internet Security Threat Report* (ISTR) menemukan bahwa deteksi *malware* pada *coinminer* meningkat sebanyak 8500 %, dan peretasan terhadap perangkat IoT meningkat sebanyak 600% (Allisy-Roberts et al., 2006). Untuk memenuhi kebutuhan keamanan informasi sebaiknya organisasi mengikuti standar yang telah ditetapkan. Kerahasiaan (*confidentiality)*, keutuhan (*integrity)*, ketersediaan (*availability)* atau yang lebih sering disebut CIA triads adalah salah satu model keamanan yang bisa digunakan sebagai standar untuk mendesain keamanan informasi pada sebuah organisasi. Model keamanan ini memiliki 3 poin utama yaitu kerahasiaan (*confidentiality)*, keutuhan (*integrity)*, dan ketersediaan (*availability)* (Rouse, 2014).

Sebagai salah satu Perguruan Tinggi yang menerapkan teknologi informasi dan sistem informasi untuk menunjang proses bisnisnya Perguruan Tinggi XYZ

seharusnya memenuhi standar keamanan informasi yang ada. Tetapi, pada praktiknya Perguruan Tinggi XYZ belum melakukan evaluasi keamanan terhadap aset kritis teknologi informasi yang dimiliki, dikhawatirkan jika terjadi kegagalan proses pada aset dapat mengganggu proses bisnis dari Perguruan Tinggi XYZ. Evaluasi keamanan ini berfungsi untuk meminimalisir dampak kerusakan jika terjadi kegagalan proses pada aset kritis teknologi informasi yang dimiliki Perguruan Tinggi XYZ.

Mengacu pada penelitian sebelumnya, terdapat daftar aset kritis yang dimiliki Perguruan Tinggi XYZ (Yuhaz, 2018). Aset – aset tersebut diurutkan berdasarkan seberapa besar dampak yang ditimbulkan kepada Perguruan Tinggi jika terjadi kegagalan proses pada aset tersebut. Pada penelitian ini penulis memilih salah satu aset teknologi informasi yang akan dilakukan proses evaluasi keamanan yaitu aplikasi web MoU. Web MoU merupakan aplikasi berbasis web yang berfungsi untuk menyimpan hasil perjanjian dan nota kesepahaman dengan pihak lain. Penulis memilih aset ini dikarenakan belum ada dokumentasi tentang penanganan masalah yang baik jika terjadi kegagalan proses dan aset ini memiliki peranan penting ketika Perguruan Tinggi ingin melakukan perjanjian kesepahaman dengan pihak lain.

Berangkat dari hal ini, penulis akan melakukan evaluasi keamanan web MoU di Perguruan Tinggi XYZ. Dari hasil evaluasi keamanan penulis akan mengeksploitasi celah keamanan yang terdapat pada web MoU. Evaluasi keamanan akan dilakukan menggunakan kerangka kerja *Vulnerability Assessment & Penetration Testing* dan akan disesuaikan dengan kebutuhan penelitian nantinya.

1.2 Rumusan Masalah

Belum ada proses evaluasi keamanan terhadap asset teknologi informasi yang ada sehingga jika terjadi kegagalan proses belum diketahui dampak yang akan terjadi.

1.3 Tujuan Penelitian

Menemukan kerentanan keamanan dan memberi tahu dampak yang akan terjadi jika terjadi kegagalan proses pada asset teknologi informasi kepada perguruan tinggi XYZ.

1.4 Manfaat Penelitian

Dengan adanya penelitian ini diharapkan dapat membantu pihak Perguruan Tinggi XYZ dalam menemukan kerentanan keamanan, mengetahui dampak yang akan terjadi jika terjadi peretasan, dan mengetahui cara mengatasi dampak yang akan terjadi.

1.5 Sistematika Penulisan

Sistematika penulisan tugas akhir dibagi menjadi lima bab. Berikut penjelasan masing-masing bab:

BAB I PENDAHULUAN

Penjelasan mengenai latar belakang masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan tugas akhir.

BAB II LANDASAN TEORI

Mengenai dasar teori yang mendukung masalah yang sedang dikaji, antara lain *Information Technology Security Assessment, Vulnerability Assessment & Penetration Testing*, Nessus, SQL Injection, Nmap, SQLMap.

BAB III METODOLOGI PENELITIAN

Penjelasan tentang rencana, langkah dan tahapan kegiatan yang akan dilakukan dalam penelitian.

BAB IV HASIL DAN PEMBAHASAN

Penjelasan tentang dokumen daftar tindakan dan strategi perlindungan untuk Perguruan Tinggi XYZ.

BAB V KESIMPULAN DAN SARAN

Kesimpulan dari hasil penelitian dan saran yang diberikan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

Berisikan daftar jurnal, tesis, buku atau alamat *website* rujukan yang digunakan dalam penulisan.