BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1. Proses Pengumpulan Data Aset

Pada proses pengumpulan data aset, peneliti melakukan berbagai metode wawancara ke narasumber. Wawancara berupa rekaman dengan narasumber dan berupa pencatatan dari pemaparan yang dijelaskan oleh narasumber. Dalam proses pengumpulan data aset, peneliti melakukan studi literatur terkait kerangka kerja yang digunakan yaitu OCTAVE dan FMEA sebagai landasan peneliti untuk membuat daftar pertanyaan untuk wawancara.

4.2. Mendata Aset Kritis

Dari hasil wawancara yang sudah dilakukan untuk mendata dan mencari informasi dari Institusi Pendidikan XYZ maka diperoleh data aset kritis teknologi informasi yang dijelaskan pada Tabel.4.1 berikut :

Tabel 4. 1 Daftar Aset Kritis

Kategori Aset	Aset Kritis
Hardware	Server
	Switch
	Accesspoint
	Kabel LAN
	PC
	Core Switch
	PC Storage Hitachi
	Router
	WLC (Wireless LAN Controller)
	Firewall
Software	Web Kartu Rencana Studi Daring (KRS Daring).

	Web Repository
	Web E-Learning
	DHCP Server
	SIM Surat
	SIM Anggaran
	SIM Arsip
	SIM Aset
	SIM Kepegawaian
	SIM MoU
	Web Portal Institusi
	Web Portal Fakultas
	Web Portal Program Studi
	ASP .NET dan IIS
Data	Data Web Kartu Rencana Studi Daring (KRS Daring).

4.3. Identifikasi Kondisi Aset Saat Ini

Pada proses identifikasi kondisi aset saat ini hasil dari proses pengumpulan data aset yang sudah didapat, maka data tersebut akan diolah dan di identifikasi berdasarkan daftar aset. Selanjutnya akan dianalisis menggunakan kerangka kerja OCTAVE hasilnya berupa nilai *severity*, *occurrence*, dan *detection*. Dan selanjutnya digunakan untuk menghitung RPN (*Risk Priority Number*). Tabel 4.2 menampilkan daftar aset yang ada sekarang pada Insitusi Pendidikan XYZ.

Tabel 4. 2 Daftar aset Saat Ini

NO	Aset	Problem
1	Web Kartu Rencana Studi Online.	Percobaan manipulasi dan kebocoran data.
		Mahasiswa masih menggunakan password bawaan.
		Masih ada data mahasiswa yang tidak valid.
2	Web Repository	Paling banyak terkena serangan dari eksternal.
		Kebutuhan penyimpanan semakin meningkat.
		Web belum secure dan tidak ada SSL Certificate
3	Core Switch	Percobaan masuk kedalam sistem.
4	PC Storage Hitachi	Perlu pembaharuan storage secara berkala.
5	Web E-Learning	Kebutuhan penyimpanan semakin meningkat.
		Web belum secure dan tidak ada SSL Certificate
6	Kabel LAN	Terjadi kerusakan karena sudah lama dan dikarenakan faktor alam
7	Switch	Belum pernah dilakukan evaluasi pada perangkat tersebut.
8	Router	Rusak apabila karena factor alam.
		Belum pernah dilakukan evaluasi pada perangkat tersebut.
9	SIM Surat	Kebocoran dan Manipulasi data.
10	DHCP Server	Tidak ada.
11	Wireless LAN Controller	Perangkat mengalami kerusakan fisik.
		Kesalahan konfigurasi pada perangkat.
12	SIM Anggaran	Kebocoran dan Manipulasi data.
13	SIM Arsip	Kebocoran dan Manipulasi data.
14	SIM Aset	Kebocoran dan Manipulasi data
15	SIM Kepegawaian	Kebocoran dan Manipulasi data.
16	SIM MoU	Kebocoran dan Manipulasi data.
17	Web Portal Institusi	Web belum secure dan Tidak ada SSL Certificate.
18	Web Portal Fakultas	Web belum secure dan Tidak ada SSL Certificate.

19	Web Portal Prodi	Web belum secure dan Tidak ada SSL Certificate.
20	Access Point	Belum pernah dilakukan evaluasi pada perangkat tersebut.
21	Firewall	Tidak ada
22	ASP .NET dan IIS	Tidak ada

4.4. Mengidentifikasi Ancaman Aset Kritis

Proses identifikasi suatu ancaman dilakukan pada masing-masing aset kritis teknologi informasi yang dimiliki Institusi Pendidikan XYZ yang disertai dengan penyebab dari terjadinya ancaman tersebut. Daftar ancaman aset kritis dapat dilihat pada tabel 4.3, 4.4 dan 4.5

Tabel 4. 3 Daftar ancama aset dari lingkungan

NO	Ancaman dari lingkungan
1	Kerusakan pada bangunan
2	Banjir
3	Gempa bumi
4	Kebakaran
5	Perubahan regulasi
6	Badai

Tabel 4. 4 Daftar ancaman aset dari manusia

NO	Ancaman dari manusia
1	Pencurian data
2	Kelalaian pegawai
3	Peretasan
4	Data rusak
6	Kesalahan input data

Tabel 4. 5 Daftar ancaman aset dari infrastruktur

NO	Ancaman dari infrastruktur
Hardware	
1	Kerusakan komputer
3	Kerusakan genset
4	Kesalahan konfigurasi hardware
5	Pencurian komponen hardware
6	Kerusakan server
Software	
7	Bug pada software
8	Serangan virus
9	Pembobolan sistem
10	Kesalahan konfigurasi
11	Software tidak update
Jaringan	
12	Kerusakan kabel
13	Hilangnya komponen jaringan
14	Gangguan koneksi internet
15	Gangguan pada router

4.5. Mendata Keamanan Yang Sudah Diterapkan

Berdasarkan hasil pendataan wawancara yang sudah dilakukan kepada pihak Divisi Sistem Informasi Institusi Pendidikan XYZ tindakan yang sudah diterapkan yaitu:

1. Sudah memiliki firewall, konfigurasi password sudah di encrypt, kabel dibeberapa kondisi sudah di tutupi dan dirapikan.
2. Dalam melaksanakan kebijakan khusus untuk memproteksi aset-aset yang dimiliki yaitu dengan SOP (Standar Operasional Prosedur) pada saat user ingin mengambil data akan ada batasan data apa saja yang bisa diakses ke

publik atau yang tidak bisa diakses, praktiknya sesuai pada standar yang berlaku.

3. Dalam hal proteksi aset, hak akses tidak akan diperkenankan masuk keruang server yang diperkenankan hanya untuk orang tertentu. Pada kondisi tertentu tidak semua admin bisa mengakses route. Hanya admin yang mempunyai kepentingan yang bisa mengakses.
4. Untuk pelatihan dilakukan kepada pegawai tertentu seperti pegawai server dan network dalam memelihara atau meningkatkan praktik-praktik keamanan.

4.6. Mengidentifikasi Kelemahan Institusi Pendidikan XYZ

Dari hasil wawancara ditemukan beberapa kelemahan dalam mengamankan aset kritis teknologi informasi yang dimiliki Institusi Pendidikan XYZ diantaranya adalah belum terealisasinya DRC (*Disaster Recovery Center*) dan belum terlaksananya evaluasi komponen infrastruktur kelemahan secara rutin.

4.7. Melakukan Pengukuran Risiko Dengan FMEA

Untuk melakukan pengukuran risiko yaitu dengan metode FMEA (*Failure Modes and Effect Analysis*) sehingga akan menghasilkan nilai RPN (*Risk Priority Number*). RPN didapat dari hasil perkalian antara *severity*, *occurrence*, dan *detection. severity* yaitu seberapa besar dampak yang dihasilkan, *occurrence* merupakan seberapa sering terjadinya suatu kegagalan, dan *detection* merupakan kemampuan kontrol dari Organisasi/Institusi Pendidikan terkait dalam mengatasi suatu kegagalan, yang nantinya digunakan untuk melakukan perangkingan risiko. Jumlah dari nilai RPN digunakan untuk menentukan level masing-masing risiko. Setelah dilakukan perangkingan risiko maka diperoleh jumlah hasil penilaian level risiko *high* (tinggi), *medium* (sedang), *low* (rendah) yang tertera pada Tabel.4.6 :

Tabel 4. 6 Jumlah Hasil Penilaian Risiko

Level Risiko	Jumlah
High	3 Risiko
Medium	4 Risiko
Low	22 Risiko