BAB 1
Pendahuluan

1.1 Pendahuluan

Keamanan informasi merupakan ranah multi disiplin dalam konsentrasi pengembangan dan pelaksanaan dari berbagai mekanisme yang ada untuk menjaga informasi sesuai pada tempatnya. Mulai dari informasi tersebut dibuat, diproses, disimpan, dikirim, dan dihancurkan harus sesuai dengan haknya (Cherdantseva, Hilton, 2015). Secara umum, unsur keamanan informasi terdiri dari ketersediaan, integritas, dan kerahasiaan informasi tersebut. Keamanan informasi erat kaitannya dengan konsep manajemen resiko karena potensi ancaman yang diberikan akan menimbulkan kerentanan bagi aset suatu organisasi. Kegagalan dalam mengamankan informasi dapat menimbulkan dampak bagi organisasi (Shouran, Priyambodo, Ashari, 2019). Manajemen resiko dalam ranah keamanan informasi adalah serangkaian proses yang dilakukan untuk mengelola resiko mulai dari proses identifikasi sampai penanganan resiko (Basyarahil, Astuti, dan Hidayanto, 2017).

Menurut Asriyanik, Prajoko (2018) menyebutkan salah satu standar manajemen resiko keamanan informasi yang dianjurkan oleh pemerintah adalah ISO/IEC 27005 yang menginduk kepada ISO/IEC 27001 tentang manajemen keamanan informasi. Sedangkan manajemen keamanan informasi yang dijadikan acuan menurut Pratama, Suprapto, dan Perdanakusuma (2018) adalah SNI ISO/IEC 27001:2013. Dilanjutkan oleh Basyarahil, Astuti, dan Hidayanto (2017) dalam penelitiannya sebagai salah satu upaya untuk mengukur tingkat kematangan dan kesiapan suatu instansi dalam bidang keamanan informasi adalah dengan menggunakan penilaian indeks keamanan informasi (KAMI). Indeks KAMI terbaru adalah versi 4.0 yang menurut BSSN dalam (https://bssn.go.id/indeks-kami/) Indeks KAMI memiliki 5 area evaluasi yang terangkum dari area yang dimiliki oleh ISO/IEC 27001:2013. Kelima area tersebut adalah tata kelola, pengelolaan resiko, kerangka kerja, pengelolaan aset, dan aspek teknologi. Dalam Indeks KAMI 4.0, menambahan suplemen untuk membahas mengenai resiko keamanan informasi baru, resiko penyimpanan data di pihak ketiga, dan pengaturan data pribadi yang digunakan dalam instansi. Melalui indeks KAMI, diharapkan organisasi dapat melaukan manajemen keamanan informasi dan manajemen resiko yang akan timbul di area – area tersebut (Budi, Tarigan, 2018).

Pratama, Suprapto, dan Perdanakusuma (2018) pernah mengadakan penelitian tentang evaluasi tata kelola sistem keamanan teknologi informasi menggunakan indeks KAMI dan ISO 27001 sebagai acuan di Dinas Kominfo Provinsi Jawa Timur. Fokus penelitian adalah menilai kesiapan dan kematangan dinas tersebut untuk melakukan sertifikasi SNI ISO/IEC 27001:2013. Hasil yang didapatkan adalah dinas tersebut belum layak untuk mengajukan sertifikasi dikarenakan hasil nilai perhitungan indeks KAMI masih belum mencukupi. Akan tetapi, dalam penelitian tersebut tidak dijelaskan mengenai kondisi di lapangan dan belum dilakukan pengukuran ulang setelah diberikan rekomendasi untuk mengejar nilai indeks KAMI dengan kontrol dari ISO27001:2013 sebagai acuan.

Penelitian lain dilakukan oleh Arfanudin, Sugiantoro, Prayudi(2017) dilakukan di Dinas Kominfo Kota Tegal memuat tentang *monitoring traffic* serangan pada router dinas tersebut menggunakan *security information event and management* (SIEM) dan implikasinya terhadap nilai Indeks KAMI. Dalam penelitian tersebut dijelaskan mengenai penilaian Indeks KAMI sebelum diberlakukan pemantauan teradap *router* pusat milik Dinas tersebut dan kemudian dilakuan percobaan uji coba serangan dan dilakukan penilaian ulang. Hasil yang didapatkan adalah menggunakan SIEM, 4 dari 8 aktivitas serangan yang dilakukan dapat dipantau serta dapat menaikkan skor pada salah satu area Indeks KAMI.

Penelitian yang akan dilakukan selanjutnya adalah mencoba mengaplikasikan *Next-Generation Firewall*, yaitu Sangfor NGAF yang digunakan di Bidang LTI Dinas Kominfo DIY. Tata kelola jaringan yang digunakan pada Dinas Kominfo DIY didapati sering mengalami masalah yang bersumber dari sisi pengguna namun berdampak hingga sisi pengelola. Terjadinya serangan di sisi pengguna menjadikan kinerja distribusi pada sisi pusat terganggu dan membuat jaringan pusat dan Organisasi Perangkat Daerah (OPD) lainnya mengalami *down*. Kejadian seperti itu belum dapat diketahui secara pasti sebelum adanya laporan oleh pihak pengguna. Sisi pengelola juga masih lemah akan kesadaran keamanan informasi, khususnya keamanan jaringan komputer sehingga kurangnya pantauan terhadap lalu lintas yang ada.

Sangfor NGAF yang digunakan oleh Bidang LTI Dinas Kominfo DIY berupa *integrated appliance hardware firewall* yang dapat digunakan sebagai perlindungan terhadap jaringan komputer. Di dalamnya terdapat *firewall* secara umum, *web application firewall, threat prevention, data leakage prevention, user access management, ips, visibility report,* dan *risk assessment*. Penggunaan NGFW tersebut dilakukan untuk menangkap setiap lalu lintas data yang melalui jaringan Pemda DIY untuk kemudian

dievaluasi dan dapat dijadikan acuan oleh pengelola dalam mengambil tindakan mengamankan lalu lintas jaringan komputer di lingkungan Pemda DIY. Sangfor sendiri memiliki *firewall report center* yang dapat digunakan untuk memudahkan pengguna dalam membaca data yang didapatkan dari hasil *tapping* maupun tangkapan *firewal* yang dimiliki. Selain dapat menampilkan hasil hasil tangkapan, di dalam *firewall report center* tersebut, pengguna dapat membuat laporan seperti yang diinginkan. Pengukuran dari laporan Sangfor NGAF menggunakan Indeks KAMI, yaitu suatu alat yang disusun oleh tim Direktorat Keamanan Informasi Kementrian Komunikasi dan Informatika sebagai alat ukur untuk kesiapan terhadap keamanan informasi yang ada di suatu instansi. Hasil pengukuran tersebut digunakan untuk memberikan gambaran kepada pimpinan suatu instansi tentang kelayakan dan kesiapan kerangka kerja keamanan informasi.

1.1 Rumusan Masalah

1. Bagaimana penggunaan *Report* NGFW dapat dijadikan sebagai acuan untuk *security awareness*?
2. Bagaimana pengaruh nilai indeks KAMI antara sebelum dan sesudah dilakukan pemanfaatan *report* NGFW?

1.2 Batasan Masalah

1. Sumber data yang digunakan dalam penelitian ini berasal dari *traffic*, serangan dan *threat* sebenarnya dari jaringan Pemda DIY yang dikelola oleh Bidang LTI Diskominfo DIY;
2. Survey Indeks KAMI akan diisi oleh 3 ASN Bidang LTI Diskominfo DIY.

1.3 Tujuan Penelitian

1. Bidang LTI dapat menggunakan *report* NGFW untuk meningkatkan *security awareness* dan dapat memaksimalkan penggunaannya dalam jaringan Pemda DIY;
2. Mengetahui seberapa besar pengaruh nilai Indeks KAMI atas pemanfaatan *report* NGFW.