Audit dan Investigasi Intrusion Detection System (IDS) pada Infrastruktur Jaringan Kampus dengan menggunakan Metode Indeks KAMI (Studi Kasus: STMIK Rosma)

Anggi Elanda[1], Daniel Richi Roynaldi Simamora[2]
[1,2] Program Studi Teknik Informatika, STMIK ROSMA
Karawang, Indonesia
anggi@rosma.ac.id, daniel.richi@rosma.ac.id

ABSTRAK

Keamanan adalah prioritas utama untuk jaringan. Oleh karena itu, diperlukan perangkat lunak atau perangkat keras yang dapat mendeteksi serangan pada suatu jaringan. Salah satu perangkat lunak yang dapat digunakan untuk mendeteksi serangan pada jaringan adalah aplikasi Instrusion Detection System (IDS). Penelitian ini bertujuan untuk melakukan audit dan investigasi serangan terhadap infrastruktur jaringan maupaun aplikasi yang ada pada STMIK Rosma STMIK Rosma. Aplikasi yang digunakan dalam proses investigasi menggunakan SmoothSec merupakan produk IDS yang bersifat OpenSource, sedangkan metode yang digunakan untuk penilaian audit infarstruktur jaringan adalah metode Information Security Management System (ISMS), yaitu SNI ISO 27001 yang dikenal dengan nama Indeks KAMI. Hasil indeks KAMI, yang mencakup Peran TIK, Tata kelola, resiko, kerangka kerja, aset dan teknologi keamanan informasi menunjukkan bahwa tingkat kematangan keamanan informasi pada STMIK Rosma berada pada level I+ sampai dengan II+, sedangkan untuk mendapatkan sertifikasi ISO 27001 level keamanan informasi pada suatu institusi minimal pada level III. Artinya, kemanan informasi yang terdapat pada STMIK Rosma masih perlu perbaikan.

Kata kunci: *Indeks KAMI, IDS (Intrusion Detection System), Infrastruktur Jaringan*

ABSTRACT

Security is the top priority for the network. Therefore, software or hardware is needed that can detect attacks on a network. One of the software that can be used to detect attacks on the network is the Intrusion Detection System (IDS) application. This study aims to audit and investigate attacks on network infrastructure and existing applications on STMIK Rosma STMIK Rosma. The application used in the investigation process using SmoothSec is an IDS product that is OpenSource, while the method used for network infrastructure audit assessment is the Information Security Management System (ISMS) method, namely SNI ISO

27001, known as the KAMI Index. The US index results, which cover the role of ICT, governance, risk, framework, assets and information security technology show that the level of information security maturity at STMIK Rosma is at levels I+ to II+, while to get ISO 27001 certification the information security level is at a level I+ to II+. institution at least at level III. This means that the information security contained in STMIK Rosma still needs improvement.

***Key words**: KAMI Index, IDS (Intrusion Detection System), Network Infrastructure*

Pendahuluan

Perkembangan teknologi informasi (TI) setiap hari semakin maju dengan sangat pesat, akibat perkembangan ini seluruh organisasi atau perusahaan harus selalu beradaptasi serta mengimplementasikan kemajuan TI. Didalam teknologi yang perkembangannya semakin pesat tersebut terdapat informasi yang diolah dan disimpan. Informasi merupakan data yang dapat digunakan dalam proses pengambilan keputusan dan juga nilai dari sebuah informasi digambarkan paling berarti dalam sebuah pengambilan keputusan (Pratama et al., 2018)(Slamet et al., 2019).

Dalam organisasi perguruan tinggi sangat dituntut tata kelola manajemen yang baik dan dapat meningkatkan kegiatan pelayanan Pendidikan perguruan tinggi bagi masyarakat dan bangsa. Dengan demikian informasi-informasi dapat dikelola dan bermanfaat bagi pengambilan keputusan manajemen perguruan tinggi tersebut, dan disamping itu pengelolaan manajemen juga dapat memberikaan manfaat bagi stakeholder/sivitas akademika. Dalam Implementasi Keamanan Jaringan khususnya Infrastruktur harus dapat mengevaluasi resiko yang kemungkinan timbul dalam tata Kelola infrastruktur pada perguruan tinggi. Dalam kegiatan Audit Sistem Pendeteksi IDS (Intrusion Detection System) yang berfungsi sebagai alat deteksi serangan terhadap infrastruktur maupaun aplikasi yang dimiliki oleh STMIK Rosma. Maka, dipilih penilaian audit infarstruktur jaringan menggunakan metode Information Security Management System (ISMS), yaitu SNI ISO 27001 yang dikenal dengan nama Indeks KAMI (Studi Kasus: STMIK Rosma). Indeks Keamanan Informasi (Indeks KAMI) digunakan sebagai alat bantu yang disusun oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika untuk mengukur, menganalisa dan mengevaluasi tingkat kesiapan penerapan keamanan informasi berdasarkan kesesuaian dengan kriteria pada SNI ISO/IEC 27001, yang fungsinya sebagai indikator penerapan keamanan informasi secara nasional (Wowor et al., 2018).

Hasil dari pengukuran ini nantinya akan didapatkan skor tingkat kematangan keamanan informasi di STMIK Rosma Karawang yang nantinya digunakan sebagai evaluasi untuk meningkatkan tingkat keamanan informasi kampus tersebut kedepannya.

Indeks KAMI

Pada tahun 2008 Kementrian Departemen Komunikasi dan Informasi Indonesia telah mengeluarkan standar keamanan yang diadopsi dari ISO/IEC 27001 mengenai Information Security Management System (ISMS), yaitu SNI ISO 27001 yang dikenal dengan nama Indeks KAMI (Setiawan, 2013). SO 27001 merupakan standar keamanan informasi yang terbitkan oleh The International Organization for Standardization (ISO) dan The Electrotechnical Commission (IEC) yang dipergunakan membantu organisasi dalam mengamankan aset informasi. ISO 27001 menjelaskan berbagai prasyarat bagi penetapan, penerapan, pelaksanaan, pemantauan, peninjauan ulang, pemeliharaan dan pendokumentasian Sistem Manajemen Keamanan Informasi (SMKI) (Darmawan & Tarigan, 2018). Oleh karena itu, untuk mengetahui tingkat pengamanan dan kelengkapan yang dimiliki oleh Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi. Alat evaluasi ini memberikan gambaran kondisi kesiapan kerangka kerja keamanan system dan dilakukan terhapad area yang memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2005.

Proses evaluasi Indeks KAMI ini dilakukan dengan 2 metode:

1. Jumlah kelengkapan bentuk pengamanan,
2. Tingkat Kematangan proses pengolaan pengamanan informasi

Area yang akan diaudit meliputi:

1. Peran TIK di dalam Instansi
2. Tata Kelola Keamanan Informasi
3. Pengelolaan Risiko Keamanan Informasi
4. Kerangka Kerja Keamanan Informasi
5. Pengelolaan Aset Informasi
6. Teknologi dan Keamanan Informasi

Infrastruktur Jaringan

Infrastruktur Jaringan merupakan sebuah kumpulan sistem komputer yang saling berhubungan, dihubungkan oleh berbagai macam bagian dari sebuah arsitektur telekomunikasi (Heryana & Putra, 2018). Secara khusus, infrastruktur ini mengacu pada organisasi dan berbagai bagian konfigurasi mereka dari jaringan komputer individu sampai pada router, kabel, wireless access point, switch, backbone, network protocol, dan network access methodologies. Infrastruktur dapat berupa (open) atau tertutup (close). Bentuk paling sederhana dari infrastruktur jaringan biasanya terdiri dari satu atau lebih komputer, sebuah jaringan atau koneksi internet, sebuah hub yang menghubungkan komputer yang satu dengan yang lainnya sampai dengan sistem jaringan yang terhubung dengan sistem jaringan lainnya.

IDS (Intrusion Detection System)

Klasifikasi adalah salah satu pendekatan solusi yang paling dikenal. National Institute of Standards and Technology (NIST) menyediakan dokumen panduan tentang IDS (Intrusion Detection System) (Jabez & Muthukumar, 2015). IDS (Intrusion Detection System) secara singkat diklasifikasikan ke dalam tiga kategori berbeda :

- IDS berbasis host,
- IDS berbasis jaringan,
- IDS penilaian kerentanan

Ada dua model dasar yang digunakan untuk menganalisis peristiwa dan menemukan serangan :

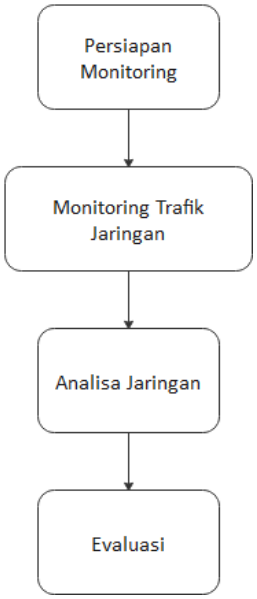
1. Model deteksi penyalahgunaan - Sistem Deteksi Intrusi mendeteksi penyusupan dengan mencari aktivitas serupa seperti kerentanan atau tanda tangan penyusupan yang diketahui.
2. Model deteksi anomali - IDS mendeteksi intrusi dengan mencari lalu lintas jaringan (abnormal).

Model deteksi penyalahgunaan biasanya disebut sebagai alat komersial IDS; selalu Vendor harus memperbarui intrusi tanda tangan. Model IDS berbasis deteksi anomali memiliki kemampuan untuk mendeteksi gejala serangan tanpa menentukan model serangan, tetapi model ini sangat sensitif terhadap alarm palsu.

Materi dan Metode

Ada 2 hal yang dilakuan oleh peneliti dalam penelitian ini, yang pertama dilakukan investigasi dengan Aplikasi IDS dan kedua melakukan audit dengan Indeks KAMI. Untuk pembahasan kedua hal ini akan dijelaskan secara terpisah dimulai dengan investigasi kemudian dilanjutkan dengan audit. Proses investigasi yang dilakukan terdapat beberapa proses dan dapat dilihat pada Gambar 1.

Pertama tahap persiapan meliputi : a. Kontruksi, b. Pengaturan Rencana., Kedua monitoring trafik jaringan meliputi : a. Koleksi Data Trafik, b. Penyimpanan Data., Ketiga analisa meliputi : a. Pemeriksaan, b. Hipotesis, c. Pelaporan., Dan keempat tahap evaluasi meliputi : a. Penyajian, b. Pembenaran dan peninjauan. Model investigasi diatas digunakan untuk mendapatkan data berupa serangan apa saja yang terjadi selama proses investigasi dilakukan.



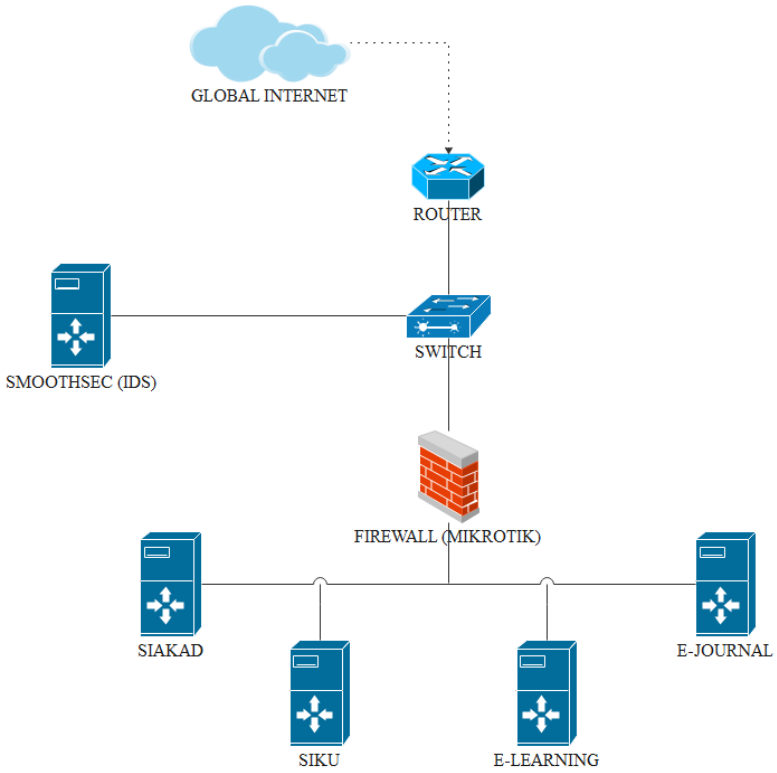
Gambar 1. Model Investigasi pada Infrastruktur Jaringan Kampus

Aplikasi yang digunakan dalam proses investigasi menggunakan SmoothSec merupakan produk IDS yang bersifat OpenSource, kemudian di konfigurasi ke dalam jaringan kampus dalam mode port mirror, yaitu metode untuk mengirimkan paket jaringan pada suatu port switch ke sebuah jaringan pemantau di port switch yang lain. Sehingga penggunaan SmoothSec untuk IDS tidak mengganggu kinerja sistem jaringan komputer di lingkungan kampus yang sudah berjalan. Berdasarkan standar Indeks KAMI langkah-langkah audit sistem keamanan diantaranya :

1. Mendefiniskan Ruang Lingkup
   Ruang lingkup yang dapat dievaluasi ini harus didefinisikan sesuai kepentingan kampus.
2. Menetapkan Peran TIK
   Bagian TIK memberi tingkatan peran dan kepentingan TIK dengan meninjau bahan evaluasi.
3. Menilai Kelengkapan Pengamanan 5 Area
   Dari 6 area pengolompokan tersebut, pada tahap ini pertanyaan evaluasi akan dikelompokkan berdasarkan 3 kategori, yaitu :
   a. Kerangka Kerja Pengamanan Informasi
   b. Tata Kelola Keamanan Informasi
   c. Efektivitas dan Konsistensi Pengamanan Informasi
   Dengan penilaian : Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh.
4. Mengkaji Hasil Indeks KAMI dan Menetapkan Langkah Perbaikan Penetapan Prioritas.
5. Mengkaji Ulang Tingkat Kelengkapan dan Kematangan Indeks KAMI.

Hasil dan Pembahasan

Bagian ini membahas tentang serangan yang masuk atau berada di lingkungan jaringan kampus khususnya terhadap service atau aplikasi yang sering digunakan, misalnya SIAKAD, SIKU, PMB, SISTER dll. Aplikasi yang digunakan adalah SmoothSec diletakkan pada mode (demilitarized zone) DMZ seperti pada Gambar 2. Penempatan pada DMZ dipilih karena lalu lintas yang paling padat ada dijalur ini dan memudahkan mendeteksi trafik jaringan dan analisa jaringan oleh SmoothSec.



Gambar 2. Penempatan SmoothSec dalam jaringan dalam kampus

Dengan Metode port mirroring, lalu lintas jaringan yang menuju DMZ disalin lalu salinannya dialirkan ke switch yang terdapat SmoothSec atau Snort. Teknik ini bermanfaat untuk lalu lintas yang asli tetapi tidak mengganggu lalu lintas yang lainnya. Selama SmoothSec dijalankan, dengan dimulai mendapatkan 80 jenis aktifitas yang dianggap bahaya oleh SmoothSec.

Percobaan atau serangan yang dideteksi oleh SmoothSec selama 30 hari dalam jaringan kampus antara lain :

- SSH Bruteforce
- SQL MySQL/MariaDB

- Web-Misc Multiple Products Excessive HTTP 304 Not Modified Responses Exploit Attempt
- SPECIFIC-THREATS Havij advanced SQL injection tool user-agent string

Hasil evaluasi dalam jaringan kampus adalah peran dan tingkat kepentingan TIK di lingkungan kampus memiliki skor 29 yang termasuk dalam kategori tinggi. Hasil ini menunjukan bahwa peran TIK dilingkungan kampus merupakan bagian yang tidak terpisahkan dari proses kerja yang berjalan.

Tabel masing-masing area setelah proses evaluasi dilingkungan kampus dapat terlihat pada Tabel. 1 berikut. Pada table ini, dapat dilihat seberapa besar tingkat kelengkapan masing-masing area yang telah dicapai.

Tabel 1. Hasil Indeks KAMI

Peran/Tingkat Kepentingan TIK	29	Tingkat Ketergantungan	Tinggi
Tata Kelola	37	Tingkat Kematangan	I+
Pengelolaan Resiko	24	Tingkat Kematangan	I
Kerangka Kerja Keamanan Informasi	41	Tingkat Kematangan	I+
Pengeloaan Aset	107	Tingkat Kematangan	II
Teknologi dan Keamanan Informasi	82	Tingkat Kematangan	II

Berdasarkan diagram pada Gambar 2 menunjukan hasil evaluasi berdasarkan setiap area terhadap kepatuhan ISO 27001, dari kelima area keamanan informasi dapat dicermati bahwa STMIK Rosma memiliki pengolaan aset yang jauh lebih mendekati standar dalam ISO 27001 dan juga seluruh area keamanan informasi dalam STMIK Rosma sudah memenuhi kerangka kerja dasar dalam pengelolaan keamanan informasi.

Gambar 3. Diagram Radar Tingkat Kelengkapan Keamanan Informasi

Kesimpulan

Berdasarkan hasil penelitian yang dilakukan pada STMIK Rosma dapat disimpulkan bahwa tingkat kelengkapan dan kematangan keamanan informasi pada STMIK Rosma masih rendah. penyebab rendahnya tingkat kelengkapan dan kematangan keamanan informasi ini belum menerapkan semua syarat keamanan informasi atau masih dalam perencanaan. Rendahnya tingkat kelengkapan ini ditunjukan oleh bar chart yang menunjukan warna merah dengan total nilai 291, yang artinya keamanan informasi pada STMIK Rosma butuh perbaikan kembali. Sedangkan tingkat kematangan setiap area keamanan informasi berada pada I+.

Daftar Pustaka

Darmawan, B. S., & Tarigan, A. (2018). KONSEP DAN STRATEGI EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) DAN EVALUASI KESADARAN KEAMANAN INFORMASI PADA PENGGUNA. *METIK Jurnal*, *2*(1), 53–64.

Heryana, A., & Putra, Y. M. (2018). Perancangan Dan Implementasi Infrastruktur Jaringan Komputer Serta Cloud Strorage Server Berbasis Kendali Jarak Jauh (Studi Kasus Di Pt. Lapi Itb). *Teknologi Informasi Dan Komunikasi*, *IX*(Cloud Storage).

Jabez, J., & Muthukumar, B. (2015). Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach. *Procedia Computer Science*, *48*(C), 338–346. https://doi.org/10.1016/J.PROCS.2015.04.191

Pratama, E. R., Suprapto, & Perdanakusuma, A. R. (2018). Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001: Studi Kasus KOMINFO Provinsi Jawa Timur. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *2*(11), 5911–5920. http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3465

Setiawan, A. B. (2013). Kajian Kesiapan Keamanan Informasi Instansi Pemerintah Dalam Penerapan E-Government. *Jurnal Masyarakat Telematika Dan Informasi*, *4*(2).

Slamet, M. R., Wulandari, F., & Amalia, D. (2019). Penilaian Pengamanan Teknologi Pada Sistem Pembelajaran Elektronik Menggunakan Indeks Keamanan Informasi Di Politeknik Negeri Batam. *Journal of Applied Business Administration*, *3*(1), 162–171. https://doi.org/10.30871/jaba.v3i1.1305

Wowor, N. E., Sentinuwo, S. R., Karouw, S. D. S., Elektro, T., Sam, U., Manado, R., Kampus, J., & Bahu, U. (2018). Analisa Keamanan Informasi Pemerintah Kota Manado Menggunakan Indeks Kami. *Jurnal Teknik Informatika*, *13*(3), 1–10.

https://doi.org/10.35793/jti.13.3.2018.28081