CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 2, No. 2, November 2019, hlm. 69-76

PEMANFAATAN HASIL REPORT NEXT-GENERATION FIREWALL SEBAGAI SECURITY AWARENESS

Akhmad Muzakka[1], Bambang Sugiantoro[2], Yudi Prayudi[3]

[1]Magister Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
[2]Magister Teknik Informatika, UIN Sunan Kalijaga, Yogyakarta
[3]Magister Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
Email: [1]15917202@students.uii.ac.id, [2]bambang.sugiantoro@uin-suka.ac.id, [3]prayudi@uii.ac.id

Abstrak

Keamanan informasi merupakan ranah multidisiplin dalam konsentrasi pengembangan dan pelaksanaan dari berbagai mekanisme yang ada untuk menjaga informasi sesuai pada tempatnya. 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. 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 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. Tujuan dari penelitian tersebut adalah untuk mengetahui adakah perbedaan dan seberapa besar perbedaan jumlah nilai Indeks KAMI ketika Bidang LTI menggunakan NGFW sebagai acuan untuk *security awareness*. Dari hasil *pre-assesment* dan *post-assesment*, ditemukan perbedaan jumlah nilai indeks KAMI dari 403 menjadi 444. Perbedaan yang cukup signifikan berada pada 3 area, yaitu Tata Kelola, Pengelolaan Aset, dan Teknologi dan Keamanan Informasi. Namun, peningkatan tersebut belum cukup untuk menaikkan hasil evaluasi akhir yang masih berada pada "Pemenuhan Kerangka Kerja Dasar" dengan tingkat kematangan mengalami kenaikan dari I+ menjadi Tingkat II pada area "Pengelolaan Aset" dan pada area "Teknologi dan Keamanan Informasi". Pada kedua area yang mengalami kenaikan yang cukup signifikan dikarenakan responden merasa lebih aware terhadap keamanan yang diterapkan pada jaringan yang dikelola. Hal tersebut juga diterapkan melalui rekomendasi yang sudah diberikan sebelumnya dan dijalankan disesuaikan dengan SOP yang ada pada bidang kerjanya. Hasil dari penelitian tersebut adalah Bidang LTI mampu menggunakan NGFW yang dimiliki untuk pengamanan jaringan yang dikelola, serta ada peningkatan nilai Indeks KAMI setelah menggunakan report dari *Firewall Report Center* sebagai *security awareness.*

Kata kunci: *indeks KAMI, security awareness, NGFW report*

USING NEXT-GENERATION FIREWALL REPORT RESULT AS A SECURITY AWARENESS

Abstract

Information security is a multidisciplinary domain in the concentration of development and implementation of various mechanisms available to keep information in place. In general, the element of information security consists of the availability, integrity and confidentiality of that information. Information security is closely related to the concept of risk management because the potential threats posed will cause vulnerability to the assets of an organization. As one of the efforts to measure the level of maturity and readiness of an agency in the field of information security is to use an information security index assessment (Indeks Keamanan Informasi – KAMI). Indeks KAMI has 5 evaluation areas which are summarized from ISO / IEC 27001: 2013. The five areas are governance, risk management, frameworks, asset management, and technological aspects. The purpose of

this research is to find out whether there is a difference and how big is the difference in the value of the Indeks KAMI when the Bidang LTI uses ngfw as a reference for security awareness. From the results of the pre-assessment and post-assessment, found differences in the number of scores of the Indeks KAMI value from 403 to 444. Significant differences are in 3 areas, Governance, Asset Management, Technology and Information Security. However, this increase is not enough to raise the results of the final evaluation which is still in the "Fulfillment of the Basic Framework" with the level of maturity increasing from I + to Level II in the "Asset Management" area and in the "Information Technology and Security" area. In both areas that experienced a significant increase because respondents felt more aware of the security applied to the managed network. This is also applied through recommendations that have been given previously and carried out in accordance with existing SOPs in the field of work. The results of this research are Bidang LTI is able to use the ngfw to secure managed networks, and there is an increase in the value of the Indeks KAMI after using reports from the Firewall Report Center as security awareness..

Keywords: *indeks KAMI, security awareness, NGFW report*

1. PENDAHULUAN

Keamanan informasi merupakan ranah multidisiplin 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 dan 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, dkk, 2019). Manajemen resiko dalam ranah keamanan informasi adalah serangkaian proses yang dilakukan untuk mengelola resiko mulai dari proses identifikasi sampai penanganannya (Basyarahil, dkk, 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, dkk (2018) adalah SNI ISO/IEC 27001:2013. Dilanjutkan oleh Basyarahil, dkk (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, dan Tarigan, 2018).

Pratama, dkk (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 menggunakan kontrol dari ISO27001:2013 sebagai acuan.

Penelitian lain dilakukan oleh Citra Arfanudin (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.

Dari penjabaran permasalahan yang sedang dialami di latar belakang, dapat dirumuskan menjadi bagaimana menggunakan NGFW untuk dapat

memantau lalu lintas dan serangan pada jaringan Pemda DIY. Dari penggunaan NGFW tersebut diharapkan akan didapatkan informasi atau report yang detail untuk dapat meningkatkan *security awarenes* dan digunakan pihak pengelola dalam mengambil keputusan dan menjadikan SOP yang ada. Salah satu cara untuk dapat mengukur security awareness suatu instansi dapat dilakukan dengan menggunakan indeks KAMI, sehingga diharapkan akan ada perubahan dalam pengukuran indeks KAMI tersebut pada saat tidak menggunakan NGFW maupun ketika menggunakan NGFW.

2. PENELITIAN TERKAIT

Penelitian tentang keamanan informasi dalam lingkup pemerintahan yang pernah dilakukan oleh Pratama, Suprapto, Perdanakusuma (2018) dilakukan di Dinas Kominfo Provinsi Jawa Timur. Dalam penelitian tersebut menjelaskan bahwasannya Dinas Kominfo Jatim semakin berkembang mengurusi informasi dan data yang dianggap penting. Oleh karenanya perlu dilakukan pengujian tingkat kematangan dan kesiapan terhadap keamanan informasi menggunakan pengukuran Indeks KAMI. Peneliti menambahkan acuan ISO 27001:2013 sebagai kontrol dari pengujian Indeks KAMI. Hasil yang didapatkan berupa nilai dari Indeks KAMI yang menunjukkan tingkat kelengkapan dan kematangan keamanan informasi dari Dinas Kominfo Jatim masih rendah. Peneliti kemudian menambahkan rekomendasi berupa kontrol ISO yang menerapkan beberapa klausul untuk membantu Dinas Kominfo Jatim dapat dinyatakan layak melakukan sertifikasi ISO27001 dan mengelola informasi pada instansi tersebut.

Penelitian berikutnya terdapat institusi pendidikan atau kampus sebagai tempat melakukan penelitian. Dilakukan oleh Basyarahil, Astuti, Hidayanto (2017) pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS. Dalam penelitian tersebut mengevaluasi manajemen keamanan informasi dengan menggunakan Indeks KAMI dan ISO 27001:2013 sebagai kontrol. Masalah yang dialami oleh DPTSI ITS berdasarkan data yang diperoleh adalah banyak ditemukan celah keamanan pada jaringan komputer dan sistem informasi yang ada di kampus tersebut. Ditambah, beberapa kali terjadi serangan yang mengakibatkan gangguan terhadap kegiatan civitas akademika di ITS. Pengukuran dilakukan mengunakan Indeks KAMI dan ISO27001:2013 sebagai kontrol terhadap hasil yang didapatkan. Dari penelitian tersebut, dapat disimpulkan bahwa DPTSI ITS belum siap dan belum matang untuk mengikuti sertifikasi ISO 27001:2013. Hal yang menyebabkan adalah kurangnya nilai yang didapat pada area pengelolaan resiko keamanan informasi karena belum diterapkan secara maksimal.

Masih dalam ranah institusi pendidikan, terkait dengan Keamanan Informasi. Asriyanik, dan Prajoko (2018) melakukan penelitian tentang manajemen resiko keamanan informasi dengan menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI). Penelitian tersebut dirasa perlu dilakukan karena SIAK di UMMI sudah terintegrasi dengan jaringan dan dapat diakses secara daring melalui internet. Dengan pengembangan tersebut, dikhawatirkan terjadi serangan terhadap SIAK sehingga diharapkan dengan mempersiapkan manajemen resiko akan dapat mengurangi kemungkinan terjadinya serangan terhadap SIAK maupun meminimalkan dampak ketika terjadi serangan. Dalam penelitian tersebut menggunakan standar ISO 27005:2011 sebagai acuan proses manajemen resiko keamanan informasi, kemudian melakukan wawancara dan diskusi dari pengelola SIAK UMMI. Hasil yang didapatkan dari penilaian manajemen resiko keamanan informasi dengan kontrol ISO 27001:2011, pengelola harus dapat mempersiapkan terhadap 47 dari 73 skenario serangan karena belum bisa diselesaikan oleh pengendalian yang ada. Pemilihan pengendalian resiko juga terbagi menjadi 19 poin diharuskan melakukan modifikasi, 1 resiko ditransfer, dan 27 resiko dihindari.

Penelitian berikutnya tentang keamanan sistem informasi dilihat dari aspek manusia yang dilakukan oleh Shouran, Priyambodo, Ashari (2019). Dalam penelitian tersebut menjelaskan bahwa keamanan sistem informasi dipengaruhi oleh beberapa aspek, seperti aspek data itu sendiri, aspek kebijakan, aspek infrastruktur, aspek teknologi, dan aspek manusia. Dijabarkan juga aspek manusia arahnya adalah kurangnya kesadaran dan perilaku berbahaya dalam menggunakan sistem informasi itu sendiri, termasuk di dalamnya dalam membuat, menggunakan, hingga menghapus. Diskusi yang diberikan dalam penelitian tersebut mengarahkan penggunaan standart untuk keamanan sistem informasi, seperti ISO untuk mengenalkan kesadaran dalam keamanan sistem informasi. Sebagai penutup, peneliti menyimpulkan bahwa kesadaran keamanan informasi merupakan cara untuk mengurangi ancaman serangan yang mengarah ke kelemahan manusia itu sendiri.

Selanjutnya terdapat penelitian studi pustaka tentang konsep dan strategi evaluasi manajemen keamanan informasi menggunakan indeks KAMI dan evaluasi kesadaran keamanan informasi pada pengguna. Penelitian tersebut dilakukan oleh Budi, Tarigan (2018) guna merumuskan konsep strategi evaluasi manajemen keamanan informasi dan kesadaran keamanan informasi pada pengguna, berikut konsep yang mendukungnya. Dalam penelitian tersebut dijelaskan area dari Indeks Kami dan konsep evaluasi kesadaran keamanan informasi pada pengguna menggunakan metode evaluasi Human Aspects of Information Security Questionnaire (HAIS-Q). Hasil yang didapatkan adalah sebuah tahapan – tahapan dalam

melaksanakan evaluasi Indeks KAMI dan berbarengan dengan evaluasi HAIS-Q untuk menilai tingkat kesadaran keamanan pada pengguna.

Penelitian berikutnya adalah tentang pengukuran kesadaran keamanan informasi menggunakan metode Multiple Criteria Decision Analysis(MCDA) yang mengambil studi kasus pada pengguna perangkat maupun aplikasi yang menyangkut keamanan informasi di kantor pemerintahan. Penelitian yang dilakukan oleh Kusumawati (2018) banyak mengambil bahan dari sikap, perilaku, dan pengetahuan akan kesadaran keamanan informasi. Permodelan tersebut berasal dari penelitian terdahulu yang dilakukan oleh Kruger dan Kearney di tahun 2005 silam. Dari permodelan tersebut, peneliti mendapatkan area – area yang dapat dijadikan menjadi objek penelitian dan dapat dikembangkan menjadi pertanyaan di kuisioner. Hasil yang didapatkan kemudian dikalkulasi menggunakan MCDA supaya mendapatkan prosentase dari nilai kesadaran keamanan informasi di kantor pemerintahan tersebut. Hasil yang didapatkan yakni pengguna masih berada pada level menengah dan dengan acuan tersebut maka diharapkan dapat meningkatkan tingkat kesadaran keamanan informasi terutama pada area pengetahuan tentang best practice keamanan informasi.

Penelitian terakhir yang dijadikan acuan datang dari studi literatur milik Babtain, Halabi, Karrar (2019) yang membahas tentang kebijakan keamanan informasi yang berada pada suatu sistem atau organisasi. Kebijakan tersebut banyak digunakan sebagai asuransi terhadap data – data yang digunakan oleh pengguna. Kepercayaan pengguna sebagai objek penelitian dijadikan patokan dalam peneliti menilai dari setiap kebijakan yang ada. Seperti dalam penyusunan kebijakan, banyak dipengaruhi oleh aspek – aspek yang mengedepankan kepercayaan dari pengguna itu sendiri.

3. METODE PENELITIAN

Penelitian akan dilakukan dalam berbagai tahapan yakni:

3.1. Studi literatur

Studi literatur dengan mendalami penelitian dari Arfanudin, Sugiantoro, Prayudi (2017) sebagai acuan utama, tentang serangan dan implikasinya terhadap nilai Indeks KAMI, dilanjutkan dengan penelitian lainnya sebagai acuan tambahan dan pembanding, maka dilakukan alur penelitian dengan melakukan pengambilan nilai Indeks KAMI, kemudian melakukan pembuatan report dari NGFW supaya dapat dijadikan sebagai acuan untuk security awareness lalu kemudian dilakukan pengambilan nilai Indeks KAMI ulang setelah diadakan diskusi dan presentasi hasil report yang sudah dibuat.

3.2. *Pre-Assesment* Indeks KAMI di awal

Pre-Assesment indeks KAMI atau pengujian awal dilakukan untuk mengetahui bagaimana nilai atau kondisi sebelum memanfaatkan *report NGFW*. Bentuk evaluasi yang diterapkan dalam indeks KAMI dapat digunakan oleh suatu organisasi dari berbagai kepentingan penggunaan TIK. Hasil evaluasi ini nantinya akan memberikan snapshot indeks kesiapan - dari aspek kelengkapan maupun kematangan - kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Hasil evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan kepada pihak yang terkait (stakeholders). Dalam penelitian, pihak yang ikut andil dalam mengisi indeks KAMI dibagi berdasarkan area yang diampu tanggung jawabnya, diantaranya adalah Kepala Bidang LTI, Kepala Seksi Pengelolaan dan Pengembangan Infrastruktur, dan Staff dari Pengelolaan dan Pengembangan Infrastruktur.

3.3. Pembuatan Report NGFW

Pembuatan report, dilakukan dengan melakukan generate report dari Sangfor Firewall Report Center. Report yang dapat diambil berupa tren, rangking, dan detail berbagai macam serangan secara real-time dari kondisi jaringan Pemda DIY. Data traffic yang ditangkap pada lalu lintas jaringan pada bidang LTI meliputi jaringan pemda DIY, termasuk di dalamnya jaringan inbound maupun outbound. Hasil yang didapatkan dari report tersebut cukup tergantung dengan peletakan dan setup dari NGFW. Pada jaringan Pemda DIY, NGFW diletakkan di bawah router border sebelum router distribusi. Hal ini dimaksudkan supaya dapat memfilter traffic dari luar menuju jaringan lokal pemda DIY, dan arah sebaliknya.

3.4. Pemaparan hasil report NGFW

Hasil report NGFW pada lalu lintas jaringan Pemda DIY disampaikan, dan diadakan diskusi kepada responden sebagai pejabat berwenang dan staf pada Bidang LTI. Dalam kegiatan ini juga akan diberikan rekomendasi oleh peneliti terhadap hasil pre-assesment dan hasil report NGFW sesuai dengan poin – poin dari standardisasi yang diakui oleh BSN, yakni ISO/IEC 27001. Dari hasil presentasi dan rekomendasi, diharapkan dari Bidang LTI dapat menjalankan ataupun mempertahankan apa yang sudah baik dan meningkatkan apa yang perlu, terlebih dapat meningkatkan kesadaran terhadap keamanan jaringan komputer.

3.5. *Post-Assesment* Indeks KAMI di akhir

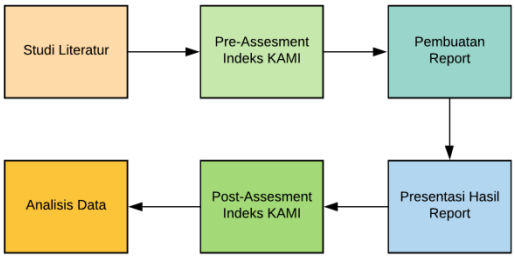
Setelah dilakukan kegiatan pemaparan hasil report NGFW, dilakukan kembali pengukuran indeks KAMI terhadap responden. Hasil tersebut akan dibandingkan dengan hasil dari pre-assesment yang dilakukan sebelumnya. Apakah ada perbedan atau tidak, perbedaan tersebut berupa penurunan

ataukah peningkatan terkait dengan presentasi dan diskusi hasil report NGFW.

3.6. Analisis Data

Data – data dari hasil pengujian indeks KAMI, wawancara, dan penelitian dikumpulkan lalu dianalisis supaya dapat mendapatkan kesimpulan dari penelitian yang dilakukan. Hasil yang diharapkan adalah dapat menampilkan korelasi antara hasil report NGFW dengan hasil pengujian Indeks KAMI, bahkan diharapkan akan meningkatan nilai Indeks KAMI pada pengujian post-assesment. Hasil tersebut kemudian akan memunculkan rekomendasi – rekomendasi yang dapat digunakan dan diterapkan di Bidang LTI.

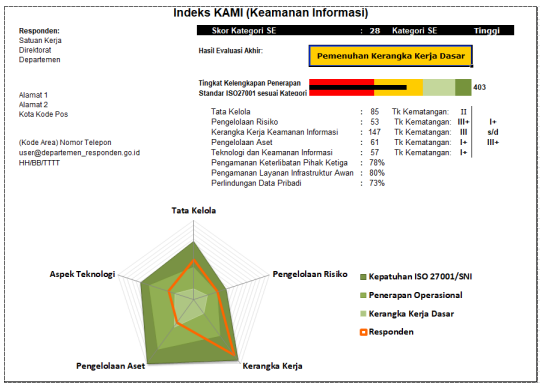
Secara umum, gambaran dari kegiatan penelitian dapat dijabarkan dalam gambar alur seperti berikut:



Gambar 1. Alur kegiatan penelitian

4. HASIL DAN PEMBAHASAN

4.1 *Pre-Assesment* Indeks KAMI



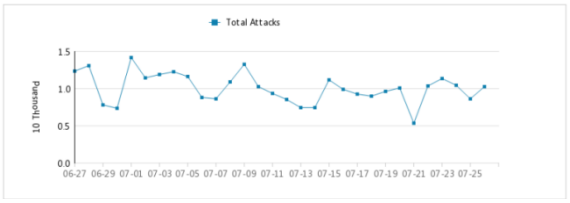
Gambar 2. Hasil *pre-assesment*

Pre-assesment Indeks KAMI diisi oleh pejabat berwenang, berdasarkan pada tanggungjawab yang diampu, seperti "Kategori Sistem Elektronik" yang bertindak sebagai responden adalah Kepala Bidang LTI (Kabid) karena poin – poin dari area kategorisasi sistem elektronik yang ada pada Bidang LTI banyak diprakarsai dan disusun oleh beliau. Sedangkan untuk tata kelola, Kabid LTI juga sebagai responden karena banyak kegiatan tata kelola masih diatur oleh beliau. Area Pengelolaan Risiko dan Kerangka Kerja diisi oleh Kepala Seksi Pengelolaan dan Pengembangan Infrastruktur (Kasi Infra) karena dalam Bidang LTI, KaSi Infra yang lebih banyak dalam mengampu tanggungjawab tersebut. Sedangkan untuk Pengelolaan Aset dan Teknologi dan Keamanan Informasi diberikan kepada Staff Pengelolaan dan Pengembangan Infrastruktur (Staff Infra) dikarenakan beliau lah yang setiap harinya mengurusi kegiatan di area tersebut.

Seperti ditampilkan dalam Gambar 2, Hasil yang didapatkan berada pada kategori SE Tinggi, sehingga membutuhkan nilai tingkat kematangan yang cukup tinggi dengan skor 28, maka dibutuhkan skor evaluasi akhir 456-583 untuk dinyatakan "Cukup Baik". Namun skor yang didapatkan adalah 403 dengan tingkat kelengkapan penerapan berupa "Pemenuhan Kerangka Kerja Dasar" dengan tingkat kematangan antara I+ hingga III+. Skor dari area paling rendah berada pada area "Pengelolaan Aset" dan "Teknologi dan Keamanan Informasi" yang diberikan oleh Staff infra sebagai penanggung jawab responden.

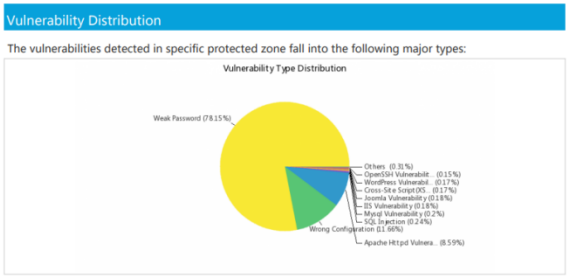
4.2 *Generate Report NGFW*

Menggunakan NGFW, Report yang dapat dibuat bermacam – macam. Seperti trend serangan yang ada, Vulnerability, Server Security, event serangan, hingga endpoint security. Report tersebut dapat dibuka sewaktu-waktu selama NGFW digunakan pada jaringan tersebut. Pada penelitian ini, digunakan data security report dengan range waktu dari 26 Juni 2019 hingga 26 Juli 2019.



Gambar 3. *Trend* tentang total serangan yang terjadi di jaringan Pemda DIY

Pada Gambar 3 di atas menunjukkan trend dari jumlah total serangan yang ada pada jaringan Pemda DIY, yang mana Bidang LTI dari Dinas Kominfo DIY sebagai pengelola jaringan tersebut. Range serangan yang ada pada waktu tersebut berkisar antara 5000 hingga 15000 serangan.



Gambar 4. *Vulnerability distribution* di dalam jaringan pemda DIY

Pada gambar 4 di atas, terdapat informasi kerentanan yang ada pada jaringan Pemda DIY. Prosentase paling tinggi adalah penggunaan *password* yang lemah, dilanjutkan oleh konfigurasi yang kurang

tepat dan kerentanan pada *httpd* yang tidak dilakukan *update* pada peringkat selanjutnya. Dari penjabaran gambar 4 sebelumnya, terdapat informasi lebih lengkap mengenai *server security* pada gambar 5 di bawah. Informasi tersebut berisi target serangan, jenis aplikasi, kerasnya serangan, ancaman terakhir, jumlah ancaman, dan jumlah yang berhasil diblok. Pada gambar 5 di bawah, juga dapat diamati terdapat catatan tentang *endpoint* yang sudah terinfeksi oleh *malware*. Dalam serangan tersebut disebutkan bahwa perangkat tersebut melakukan kontak dengan *CNC Server*.

Application Server Security

The following are the top attacked servers:

No.	Fixed	Target Server	Application Server	Severity (Level)	Latest Threat	Threat Count	Block Count	Block Percent
1	No	103.255.15.68	Web	Hacked(5)	2019-07-26 23:45:56	22548	7199	31.93%
2	No	103.255.15.33	-	Hacked(5)	2019-07-26 21:50:15	9203	3923	42.63%
3	No	103.255.15.66	-	Hacked(5)	2019-07-26 23:50:12	4488	1949	43.43%
4	No	103.255.15.57	-	Hacked(5)	2019-07-26 23:59:08	3672	502	13.67%
5	No	103.255.15.93	Web	Ever been attacked(4)	2019-07-26 23:32:26	20927	4904	23.43%
6	No	103.255.15.23	-	Ever been attacked(4)	2019-07-26 23:33:54	6270	1238	19.74%
7	No	103.255.15.84	-	Ever been attacked(4)	2019-07-26 21:16:15	4742	332	7%
8	No	103.255.15.97	Web	Ever been attacked(4)	2019-07-26 23:02:25	3402	1198	35.21%
9	No	103.255.15.29	-	Ever been attacked(4)	2019-07-26 19:37:20	2637	752	28.52%

Gambar 5. *Application Server Security*

Endpoint Security

103.255.15.49 Security Details (To be Fixed)

Overall security rating: Critical (Infected)

103.255.15.49 has undergone 35198 threat(s). It is at the stage of C&C Communication currently. At this attack stage, host is infected with malware and controlled by hacker.

Threat Details

Event Category	C&C Communication
Details	Host visited C&C communication domain or IP address proved by CNCERT.
Description	No data available

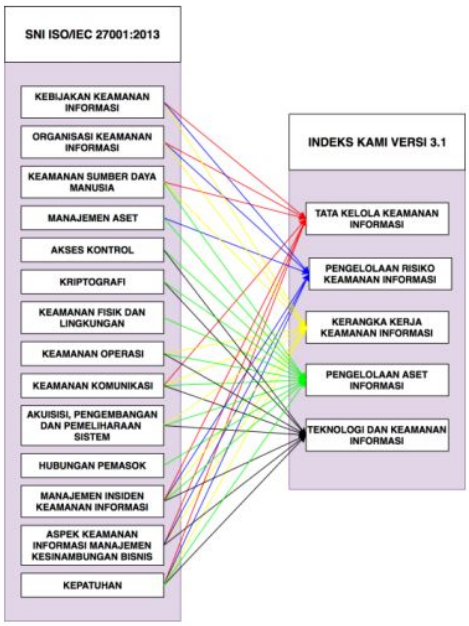
Event Category	C&C Communication
Details	Host visited a C&C Communication URL proved by CNCERT.
Description	2019-07-26 19:55:58 It is attempting to access the botnet C&C server (nxtfdata.xyz/cl.exe). (5 occurrence(s))

Gambar 6. *Endpoint Security*

Dari penggunaan NGFW, dapat dibuat sebuah *report* secara otomatis oleh sistem firewall tersebut. Pada gambar 3,4,5 dan 6 di atas adalah sebagian kecil informasi yang terdapat dalam *security report* hasil *generate* dari NGAF Sangfor. Dari *report* tersebut, dapat dijadikan pembelajaran mengenani apa yang harus dikerjakan selanjutnya.

4.3 Pemaparan hasil pembuatan report dari NGFW

Dari hasil pembuatan report yang sudah dikerjakan sebelumnya, maka berikutnya adalah dilakukan pemaparan hasil. Presentasi dilakukan dengan menghadirkan pada responden untuk mendengar, melihat, berdiskusi dan mengevaluasi bersama mengenai hasil *report* dan hasil Indeks KAMI yang diisi pada saat *pre assesment* dilakukan. Dibahas juga mengenai jenis serangan yang ada, serta korelasinya dengan Indeks KAMI sebelumnya. Pada tahapan ini juga diberikan rekomendasi – rekomendasi mengenai SOP atau hal yang dapat ditingkatan untuk keamanan informasi di lingkungan jaringan Pemda DIY.



Gambar 7. Hubungan antara ISO 27001 dengan Indeks Kami

Rekomendasi tersebut mengacu pada ISO 27001 dan hubungannya pada Indeks KAMI dapat ditinjau dari gambar 7 di atas. Berdasarkan skor nilai Indeks KAMI yang diambil sebelumnya, serta melihat dari kondisi jaringan Pemda DIY melalui report yang ada, maka dibuat rekomendasi sebagai berikut.

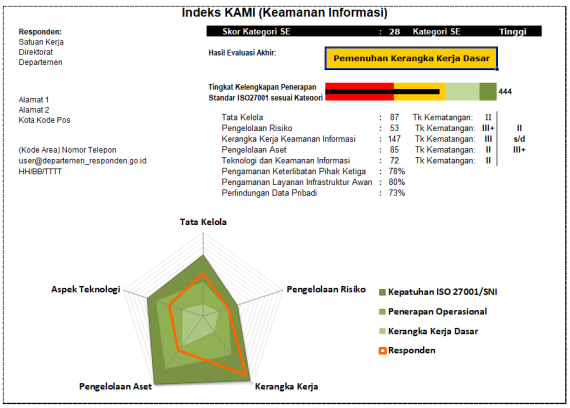
Tabel 1. Rekomendasi

Area Indeks Kami	Rekomendasi	Kontrol ISO
Tata Kelola	Mengatur Kebijakan dengan seksama	A5.1
	Mengatur pengelolaan data sesuai dengan SDM	A6.1
	Melakukan pendalaman tentang ISMS kepada SDM yang bertugas, serta mengikuti training yang ada	A7.2
Risiko	Mengatur kebijakan terkait penanganan risiko yang ada	A5.1, A16,
	Mengatur tanggung jawab terhadap keamanan informasi sesuai dengan SDM	A17.1, A17.2
Kerangka Kerja	Melengkapi dokumen – dokumen terkait kerangka kerja, SOP serta menjalankannya secara disiplin	A9, A10, A11, A12, A13
Pengelolaan Aset	Pendataan asset secara detail dan	A5.1, A8, A15

	dapat dimonitor dengan baik	
Teknologi & Keamanan Informasi	Meningkatkan kepekaan terhadap keamanan informasi, sehingga dapat mengikuti perkembangan teknologi yang ada	A7.2.2

4.4 *Post Assesment* Indeks KAMI

Setelah dilakukan pemaparan hasil pembuatan report dan rekomendasi yang dapat dilakukan oleh tim, maka berikutnya adalah dilakukan pengukuran ulang Indeks KAMI oleh responden yang sama. Berikut adalah hasil dashboard Indeks KAMI pada tahap post assesment pada Gambar 8 di bawah ini.



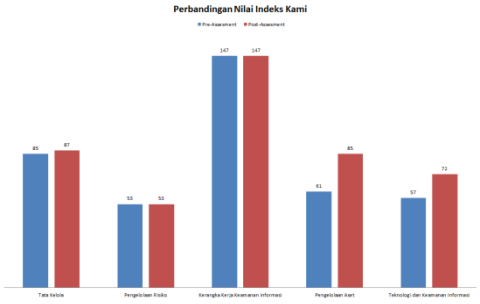
Gambar 8. Hasil *post assessment* dari Indeks KAMI

Ada kenaikan dari nilai Indeks KAMI antara pre-assesment dan post-assesment.Kenaikan tersebut terjadi pada area Tata Kelola, Pengelolaan Aset, Teknologi dan Keamanan Informasi. Pejabat sebagai responden tetap sama seperti sebelumnya, supaya data tetap dapat dipertahankan arahnya.

Hasil yang didapatkan berada pada kategori SE cukup tinggi dengan skor 28, maka dibutuhkan jumlah skor evaluasi akhir antara 456 hingga 583 untuk dinyatakan "Cukup Baik". Namun skor yang didapatkan adalah 444 dengan tingkat kelengkapan penerapan berupa "Pemenuhan Kerangka Kerja Dasar" dengan tingkat kematangan antara II hingga III+. Jumlah Skor dari area paling rendah berada pada area "Pengelolaan Aset" dan "Teknologi dan Keamanan Informasi" yang diberikan oleh Staff infra sebagai penanggung jawab responden seperti assesment sebelumnya

4.5 Analisis Data

Dari hasil pre-assesment dan post-assesment, ditemukan perbedaan jumlah skor nilai indeks KAMI dari 403 menjadi 444. Perbedaan yang cukup signifikan berada pada 3 area, yaitu Tata Kelola, Pengelolaan Aset, dan Teknologi dan Keamanan Informasi. Namun, peningkatan tersebut belum cukup untuk menaikkan hasil evaluasi akhir yang masih berada pada "Pemenuhan Kerangka Kerja Dasar" dengan tingkat kematangan mengalami kenaikan dari I+ menjadi Tingkat II pada area "Pengelolaan Aset" dan pada area "Teknologi dan Keamanan Informasi". Sedangkan Pada area "Tata Kelola" terdapat kenaikan pada poin 2.9 tentang peningkatan kompetensi pegawai. Pada area "Pengelolaan Resiko" dan "Kerangka Kerja" tidak terdapat peningkatan jumlah skor.



Gambar 9. Perbandingan Jumlah Skor Nilai Indeks KAMI

Pada area "Pengelolaan Aset" dan "Teknologi dan Keamanan Informasi" mengalami kenaikan yang cukup signifikan dikarenakan responden merasa lebih aware terhadap keamanan yang diterapkan pada jaringan yang dikelola. Hal tersebut juga diterapkan melalui rekomendasi yang sudah diberikan sebelumnya dan dijalankan disesuaikan dengan SOP yang ada pada bidang kerja.

Dari data – data yang sudah disajikan di atas, rekomendasi yang diberikan kepada Bidang LTI dapat ditingkatkan dan atau minimal dipertahankan supaya kedepan dapat meningkatkan skor ketika dilakukan pengetesan Indeks KAMI lanjutan, atau ketika dirasa cukup dapat mengikuti assessment untuk ISO 27001. Kendala yang dialami adalah pembacaan alamat ip user/host pada jaringan pemda DIY masih berupa ip publik, belum terlihat secara lokal, dikarenakan jaringan tersebut berada di balik NAT. Kedepan, akan dirubah skema jaringan menerapkan routing pada sisi lokal antar bagian supaya dapat lebih transparan, dan digunakan single sign on pada jaringan pemda sehingga dapat terdeteksi hingga ke level identitas pengguna/user.

5. Kesimpulan dan Saran

Dengan menggunakan report dari NGFW, dapat membantu meningkatkan *security awareness* bagi para pemangku kebijakan yang dinilai menggunakan Indeks KAMI. Terbukti dengan naiknya jumlah skor indeks KAMI dari 403 menjadi 444. Meskipun belum dapat dinyatakan dengan "cukup baik", akan tetapi ada peningkatan juga pada tingkat kematangan dari Bidang tersebut.

Menggunakan hasil report dari Firewall Report Center, Bidang LTI dapat mengetahui kondisi keamanan Jaringan Pemda DIY seperti bahaya yang ada pada sisi *core* hingga *endpoint* dan maupun serangan yang muncul sehingga dapat lebih *aware* terhadap setiap langkah yang harus dilakukan.

Untuk penelitian berikutnya, supaya dapat menilai perkembangan dari kegiatan yang dilakukan dari setiap rekomendasi.

6. DAFTAR PUSTAKA

CHERDANTSEVA, Y., dan HILTON, J. 2015. Understanding Information Assurance and Security. International Journal, [online] Tersedia di: < https://www.researchgate.net/publication/283569185> [Diakses 1 Mei 2019]

SHOURAN, Z., PRIYAMBODO, T.K., dan ASHARI, A., 2019. Information System Security: Human Aspects. International journal of scientific & technology research. 8(03), p.111-115

PRAJOKO, A., ASRIYANIK. 2018. Jurnal Teknik Informatika dan Sistem Informasi: Manajemen Risiko Keamanan Informasi Menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI). 4(2), p.315-325

PRATAMA, E.R., SUPRAPTO, DAN PERDANAKUSUMA, A.R., 2018. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer: Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur). 2(11). p.5911-5920

BASYARAHIL. F.A., ASTUTI, H.M., dan HIDAYANTO, B.C., Jurnal Teknik ITS: Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS. 6(1). P. A122 – A128

BUDI, D.S., TARIGAN, A., 2018. METIK Journal : Konsep dan strategi evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (kami) dan evaluasi kesadaran keamanan informasi pada pengguna. 2(1). P.53-64

ALEXANDROS, I.Z., 2018. Information security organizational change assessment. International Hellenic University. Greece

TORTEN, R.T., dan REACHIE, C., 2018. The Impact Of Security Awarness On Information Technology Professionals' Behavior. [Online] Tersedia di <https://doi.org/10.1016/j.cose.2018.08.007 > [Diakses pada 1 Mei 2019]

KUSUMAWATI, A., 2018. Information Security Awareness: Study on a Government Agency. International Conference on Sustainable Information Engineering and Technology (SIET), [e-journal] Tersedia di < http://dx.doi.org/10.1109/SIET.2018.8693168> [Diakses pada 1 Mei 2019]

BABTAIN, F., HALABI, Z., dan KARRAR, A., 2019. International Journal of Computer Science and Software Engineering (IJCSSE) : Enhancing the Trust of Users Based on Information Security Policy Compliance. 8(3). P.69-71