Jurnal Teknologi dan Komunikasi Pemerintahan Vol 5, No. 2, 2023, pp. 159-187
Website:http://ejournal.ipdn.ac.id/JTKP, **p-ISSN 2722-1717**

Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur

Author:
Aldi Dinata Saputra[1*], Frans Dione[2], Irfan Uluputty[3]

Affiiation:
Sekretariat Daerah Kutai Kartanegara, Jl. Wolter Mongonsidi, Tenggarong 75123, Indonesia[1]
Institut Pemerintahan Dalam Negeri, Jl. Ir. Soekarno Km. 20, Jatinangor 45363, Indonesia[2,3]

e-Mail: saputraaldi480@gmail.com[1], fransdionesa@gmail.com[2] , irfan_uluputty@ipdn.ac.id[3]
*Correspondence Author

Receieved, 4 Oktober 2023
Revised, 15 Desember 2023
Accepted, 20 Desember 2023
Available Online, 21 Desember 2023

Abstrak

Informasi dan data merupakan aset yang sangat penting untuk dilindungi karena saat ini informasi dan data merupakan aset yang berharga karena berisikan segala keterangan mengenai sebuah organisasi. Karena anggapan demikian maka hal ini menyebabkan timbulnya kejahatan di dunia digital yang disebut kejahatan siber. Maraknya kejahatan siber yang terjadi maka diperlukan Keamanan Informasi dan Persandian yang mahir pula untuk mencegah pencurian data dan informasi. Penelitian ini bertujuan untuk mengetahui bagaimana pengelolaan keamanan informasi dan persandian dan tingkat kematangan dalam pengamanan informasi di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur. model penelitian yang digunakan adalah penelitian kualitatif dengan metode deskriptif dengan pendekatan induktif. Peneliti melakukan wawancara, observasi dan dokumentasi pada lokasi penelitian sebagai teknik pengumpulan data. Pada penelitian ini, peneliti menggunakan teori CIA TRIAD oleh Michael E. Whitman dengan dimensi Confidentiality, Integrity dan Avalaibility. Penelitian ini juga menggunakan alat evaluasi Indeks Keamanan Informasi (KAMI 4.2) dengan standar ISO/IEC 27001: 2013 yang menentukan aspek-aspek yang perlu dipenuhi untuk mencapai keamanan informasi. Hasil dari penelitian ini adalah bahwa pengelolaan keamanan informasi dan persandian di Dinas Komunikasi dan Informatika masih kurang dan rentan terhadap serangan siber karena beberapa fasilitas yang belum memadai dan regulasi yang belum mengatur penuh mengenai keamanan informasi, hal ini juga dibuktikan dari hasil evaluasi Indeks Keamanan Informasi yang menunjukkan tingkat kematangan keamanan informasi yang masih berada pada Tingkat I+ - Tingkat II+, dimana seharusnya dalam standar ISO/IEC 27001: 2013 bahwa ambang batas minimum kesiapan sertifikasi adalah Tingkat III+.

Kata Kunci: Informasi, Kejahatan Siber, Keamanan Informasi, Persandian.

Abstract

Information and data are assets that are very important to protect because currently information and data are valuable assets because they contain all information about an organization. Because of this assumption, this has led to crimes in the digital world which are called cybercrimes. The rise of cybercrime that occurs, requires advanced Information and

Encryption Security to prevent data and information theft. This study aims to find out how information and encryption security is managed and the level of maturity in information security at the Office of Communication and Informatics, East Kalimantan Province. the research model used is qualitative research with descriptive methods with an inductive approach. Researchers conducted interviews, observation and documentation at the research location as a data collection technique. In this study, researchers used the CIA TRIAD theory by Michael E. Whitman with the dimensions of Confidentiality, Integrity and Avalaibility. This study also uses the Information Security Index evaluation tool (KAMI 4.2) with the ISO/IEC 27001: 2013 standard which determines the aspects that need to be met to achieve information security. The results of this study are that the management of information security and encryption at the Office of Communication and Informatics is still lacking and vulnerable to cyber attacks because several facilities are inadequate and regulations do not fully regulate information security, this is also evidenced from the results of the Information Security Index evaluation which indicates the maturity level of information security which is still at Level I+ - Level II+, where it should be in the ISO/IEC 27001: 2013 standard that the minimum threshold for certification readiness is Level III+.

Keywords: *Cyber Crime, Encryption, Information, Information Security.*

1. Pendahuluan

Teknologi informasi dan komunikasi yang berkembang di era industri 4.0 yang pesat membuka banyak fasilitas yang tersedia. Masyarakat merasakan dampak yang sangat signifikan dari perkembangan teknologi karena manfaat teknologi begitu besar. Semua kebutuhan masyarakat dapat dipenuhi dari satu tangan. Hal ini membuat orang tergantung pada kebutuhan mereka untuk setiap aspek teknologi.

Tidak hanya dalam hal pemenuhan kebutuhan informasi dan pemenuhan kebutuhan, bahkan pemerintah saat ini telah memanfaatkan momentum tersebut untuk memaksimalkan kualitas pelayanan terhadap publik kepada masyarakat. Pelayanan terhadap publik yang memenuhi kebutuhan dan hak setiap warga negara berupa barang, jasa, dan pelayanan administrasi merupakan kewajiban pemerintah. Hal ini pun merupakan suatu tuntutan yang dilakukan oleh masyarakat dalam pelayanan kepada publik sehingga hampir semua pelayanan publik yang dilakukan oleh pemerintah saat ini telah menerapkan pelaksanaan *e-Government* walaupun dalam penerapannya masih banyak terdapat kekurangan [1]. Oleh karena itu, pemerintah telah mengambil langkah-langkah strategis untuk memenuhi harapan pelayanan publik yang berkualitas dengan mengesahkan Undang-Undang Nomor 25

[1] Agung Nurrahman, dkk. (2021). Pemanfaatan Website Sebagai Bentuk Digitalisasi Pelayanan Publik di Kabupaten Garut. JTKP (Jurnal Teknologi dan Komunikasi Pemerintahan). Hal 78.

Tahun 2009 tentang Pelayanan Publik. Pelayanan Publik pada era saat ini telah terintegrasi dengan teknologi informasi dimana hampir semuanya telah menggunakan aplikasi berbasis website, hal ini seperti yang tercantum dalam Peraturan Presiden No. 95 Tahun 2018 Tentang SPBE. Oleh karena itu segala informasi yang diarsipkan demi kepentingan administrasi masyarakat dalam urusan pelayanan publik disimpan di dalam database, disimpan, dan terhubung secara daring pada internet.

Digitalisasi Pelayanan Publik di Pemerintahan indonesia sendiri sudah mulai meluas. Saat ini, hingga pemerintahan yang paling melekat dengan masyarakat sudah memiliki pelayanan online yang terintegrasi. Pelayanan publik berbasis online di desa sendiri telah mendorong kemajuan di desa[2]. hal ini membuktikan bahwa penerapan sistem online telah diterapkan hampir di semua instansi pemerintahan. Data dan Informasi yang disimpan pun semakin banyak, oleh karena itu data yang tersimpan perlu diamankan dengan hati-hati. Data yang disimpan juga butuh perhatian khusus dengan pengelolaan data yang baik serta keamanan yang tinggi karena semakin banyak data yang disimpan semakin tinggi resiko kehilangan serta kebocoran data.

Meskipun dalam penerapannya, informasi yang digunakan tidak semua adalah bersifat rahasia. adapun informasi yang menjadi hak untuk diketahui masyarakat, oleh karena itu beberapa informasi dapat di *expose* ke masyarakat sebagai bentuk transparansi dalam pelayanan publik. salah satu metode penyebaran informasi yang umum dipakai adalah dengan sosial media, dengan sosial media, penyebaran informasi dapat menjangkau masyarakat dengan mudah. Penyebaran informasi ini dapat dibenarkan karena menjadi sarana pemerintah dalam menjaga citra dan kualitas pelayanan dalam penyelenggaraan pemerintahan[3]. walaupun begitu, tetap terdapat data yang bersifat penting dan rahasia. Data ini perlu disimpan baik-baik

[2] Ikhbaluddin, (2021). Pelayanan Publik Berbasis Online di Desa (Studi pada empat desa di Kecamatan Jatinangor). JTKP (Jurnal Teknologi dan Komunikasi Pemerintahan). Hal 16.
[3] Lisdawati, Yuni, (2022) Penggunaan Media Sosial dalam Penyebarluasan Informasi Program Pemerintah di Dinas Komunikasi Informatika Statistik dan Persandian Kabupaten Rokan Hilir Provinsi Riau. JTKP (Jurnal Teknologi dan Komunikasi Pemerintahan) Vol 4. No. 2. Hal 73.

dan tidak boleh diketahui oleh siapapun kecuali internal instansi atau organisasi terkait.

Informasi yang disimpan sangat penting sifatnya bagi organisasi yang terkait. Data dan informasi merupakan aset bagi perusahaan, keamanan dalam data atau informasi secara tidak langsung dapat meningkatkan kelangsungan bisnis, mengurangi risiko, memaksimalkan pengembalian investasi, dan mengejar peluang baru. Semakin banyak data yang disimpan, dikelola, dan dikomunikasikan oleh perusahaan, semakin besar potensi kerusakan, kehilangan, atau pencurian data oleh pihak ketiga[4]. Bahkan sekarang, aset organisasi meningkat, tidak hanya pada peralatan kantor dan dokumen kelembagaan, tetapi juga dengan informasi dari berbagai sumber Perangkat lunak yang digunakan oleh institusi untuk memfasilitasi penyampaian layanan kepada masyarakat. Penggunaan teknologi informasi juga membutuhkan manajemen keamanan informasi untuk melindungi aset institusi, informasi dianggap aset yang sangat berharga dan perlu untuk dilindungi[5].

Serangan yang sering terjadi dalam menginvasi data di sebuah organisasi dimulai dari bermunculannya aktivitas pada sistem yang mencurigakan berupa Anomali. Anomali adalah titik, objek, peristiwa, pola, vektor, sampel dan lain-lain di dalam data yang tidak sesuai dengan perilaku normal yang dapat diterima sistem. Anomali pada jaringan dapat menyebabkan operasi jaringan menyimpang dari perilaku normal. Anomali dapat terjadi karena kapasitas jaringan yang penuh, malfungsi pada perangkat, kesalahan konfigurasi pada jaringan, serta perilaku kejahatan atau invasi pada jaringan[6].

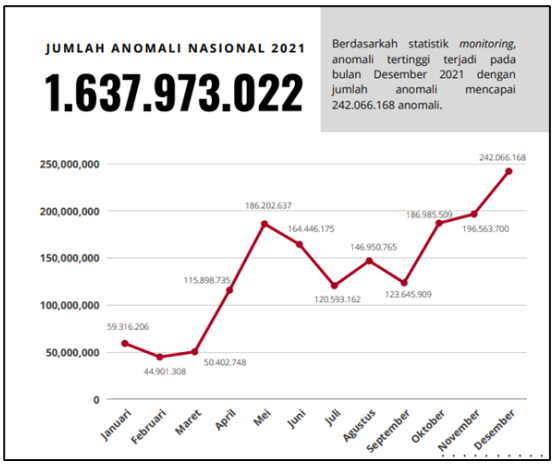
Deteksi anomali bertujuan untuk mendeteksi lalu lintas data yang tidak normal yang kemudian dapat menimbulkan masalah keamanan jaringan dan sebagai tanda adanya akses dari orang yang tidak memiliki kewenangan dalam

[4] Halilul Khairi, M. (2017). Dinamika Pelaksanaan Urusan Di Bidang Persandian Pemerintah Daerah. In A. A. Prayudi, *Dinamika Pelaksanaan Urusan Di Bidang Persandian Pemerintah Daerah.* Jakarta: Yayasan Pustaka Obor Indonesia. Hal. 1

[5] Gunawan, C. E. (2018). Pengukuran Keamanan Informasi Menggunakan Keamanan Informasi (KAMI) Studi Kasusu di PUSTIPD UIN Raden Fatah Palembang. *JUSIFO (Jurnal Sistem Informasi)*. Hal 122-123

[6] Dhruba Kumar Bhattacharyya, J. K. (2014). *Network Anomaly Detection A Machine Learning Perspective.* London: CRC Press. Hal 45-46

mengakses, mengubah, ataupun menghapus data, sehingga dari gambar diatas menunjukkan bahwa besarnya tingkat kerentanan yang terjadi pada sistem keamanan informasi dan keamanan[7].

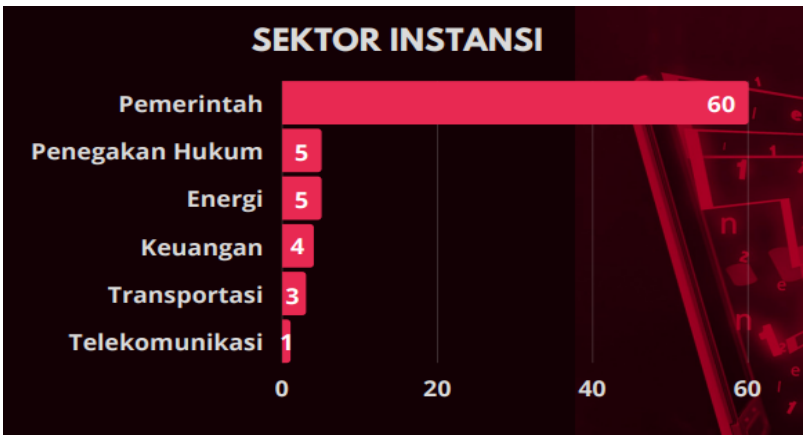


Gambar 1. Jumlah Deteksi Anomali pada Tahun 2021

Pada tahun 2021 silam telah dilakukan deteksi anomali oleh Badan Siber dan Sandi Negara (BSSN) dengan hasil terdapat peningkatan jumlah anomali mulai dari awal tahun. Peningkatan ini membuktikan bahwa kerentanan dari sistem informasi pada jaringan di indonesia semakin tinggi karena meningkatnya jumlah anomali menandakan banyaknya akses yang masuk ke dalam sebuah sistem sehingga informasi yang terdapat di dalam sistem tersebut terekspos. Menurut Badan Siber dan Sandi Negara (BSSN), 700 juta serangan siber akan terjadi di Indonesia pada tahun 2022. Serangan dunia maya yang dominan adalah *ransomware*, atau *malware* dengan permintaan uang tebusan. Menurut data BSSN, terdapat 714.170.967 serangan pada bulan Januari dengan 272.962.734 serangan, lebih dari sepertiga jumlah serangan pada paruh pertama tahun 2022.

[7] Setiawan, M. R. (2021). Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII. *AUTOMATA, Diseminasi Tugas Akhir Mahasiswa*. Hal 1-2

Baru-baru ini sedang marak sebuah serangan dari peretas dengan inisial "bjorka" yang telah berhasil menyerang dan membocorkan hingga menjual informasi yang terdapat pada Kementerian Komunikasi dan Informatika (Kominfo). Dia telah menjual sebanyak 105 juta rekaman warga negara Indonesia (WNI) dari Komisi Pemilihan Umum (KPU), 1,3 miliar rekaman registrasi kartu SIM prabayar Indonesia, termasuk NIK, nomor telepon, operator seluler, hingga saat ini.



Gambar 2. Sektor Rentan Serangan Data Breach

Dilihat dari data laporan tahunan monitoring keamanan siber, sektor instansi yang paling sering terkena serangan siber adalah sektor pemerintah. Hal ini tentu terjadi, karena sektor pemerintah sendiri menyimpan dan mengelola informasi yang penting dan data yang berkaitan dengan data pribadi masyarakat secara lengkap. Data pribadi sendiri bersifat sensitif dan rentan untuk disalahgunakan hal ini juga sesuai dengan penyampaian oleh Analis Sistem Informasi dan Jaringan Diskominfo Kaltim kepada penulis pada pukul **11.52 WIB hari senin tanggal 17 Oktober 2022** melalui **Whatsapp**, bahwa hampir setiap harinya ditemukan anomali, sehingga terjadi pencurian data dan terganggunya operasional organisasi. Hal ini menjadi permasalahan utama pada tingkat daerah dimana serangan siber dengan frekuensi yang sangat tinggi.

Gambar 3. Jumlah Data yang Terekspos Berdasarkan Sektor

Data yang disimpan dan dikelola oleh pemerintah merupakan data dengan resiko tinggi untuk dicuri atau diserang, karena sektor yang strategis dengan informasi yang sangat sensitif menjadi sasaran untuk disalahgunakan oleh peretas. Sehingga sektor Pemerintahan menjadi sasaran utama bagi peretas untuk melakukan Serangan Siber. Atas dasar ini sangat penting untuk memerhatikan dan meninjau Pengelolaan Keamanan Informasi dan Persandian di sektor Pemerintahan.

Kesadaran keamanan informasi dan risiko kebocoran informasi, terutama informasi rahasia dan strategis, menjadi perhatian utama saat menggunakan teknologi informasi. Persandian adalah upaya untuk melindungi dan menjamin keaslian berita atau dokumen pemerintah. Dalam konteks ini, penelitian ini berfokus kepada Pengelolaan Keamanan Informasi dan Persandian di Diskominfo Provinsi Kalimantan Timur dan Tingkat Keamanan Informasi di Diskominfo Provinsi Kalimantan Timur.

Penelitian ini bertujuan untuk mengetahui dan mengevaluasi kelebihan dan kelemahan dari Pengelolaan keamanan dan persandian yang dilaksanakan oleh Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur, hal ini berkaitan dengan upaya yang dilakukan untuk mencegah serta mengatasi peristiwa serangan siber yang terjadi serta untuk mengetahui tingkat keamanan berdasarkan standar Internasional ISO/IEC 27001: 2013 dengan alat evaluasi Indeks Keamanan Informasi (KAMI) versi 4.2 yang diterbitkan oleh Badan Siber dan Sandi Negara.

Manfaat dari penelitian ini mampu menambah pengetahuan, sebagai landasan teoritis pada penelitian selanjutnya ataupun sebagai bahan bacaan untuk menambah wawasan mengenai keamanan informasi dan persandian yang cukup rumit untuk dipahami. Selanjutnya dapat sebagai data studi kasus untuk meneliti fenomena kejahatan siber yang kerap menyerang sistem informasi pemerintahan negara kita. Kemudian juga diharapkan dapat menjadi bahan bacaan dan sumber ilmu dalam meningkatkan pengetahuan dan kompetensi serta sebagai modal dalam pengelolaan keamanan informasi dan persandian di daerah.

Hasil pada penelitian ini juga dapat dijadikan masukan serta referensi untuk Diskominfo Provinsi Kaltim dalam pengelolaan Keamanan Informasi dan Persandian sebagai dasar dalam pengambilan keputusan atau kebijakan agar lebih mampu untuk meningkatkan kapabilitas dari organisasi dalam urusan menjaga informasi dan data masyarakat yang bersifat privasi di Provinsi Kalimantan Timur. Serta menjadi saran dalam perbaikan kemanan informasi yang dapat dilihat dari hasil pengukuran Indeks KAMI. Selain itu juga, dapat dijadikan sebagai kontribusi dalam hal akademis yang berkaitan dengan Keamanan informasi dan Persandian di pemerintah daerah serta dapat dijadikan sebagai bahan penelitian selanjutnya khususnya mengenai Keamanan Informasi dan Persandian.

Penelitian sebelumnya mengenai topik yang sama telah melakukan Evaluasi Tingkat Keamanan Siber Pengelolaan Keamanan Informasi menggunakan Indeks KAMI Versi sebelumnya. Pada versi ini adalah untuk menilai kesiapan Instansi dallam mengelola risiko di 3 (tiga) area baru ini, pada revisi 4.2 disediakan modul suplemen yang membahsa aspek kesiapan pengamanan untuk ketiga aspek tersebut. Penggunaan modul sulemen untuk evaluasi kesiapan Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastruktur Awan dan Perlindungan Data Pribadi digunakan sesuai konteks atau cakupan yang ada. Responden hanya perlu menjawab area evaluasi yang berlaku.

Perbedaan antara penelitian yang telah dilakukan dengan penelitian saat ini adalah versi Indeks KAMI yang akan digunakan pada penelitian ini yaitu Indeks KAMI 4.2 karena peneliti sebelumnya telah menggunakan Indeks KAMI versi

sebelumnya yaitu versi 4.0, sehingga penulis menggunakan versi Indeks KAMI yang lebih terbaru dan menggunakan dimensi dari *CIA TRIAD* pengelolaan persandian pada Diskominfo.

Informasi merupakan aset yang harus dilindungi agar terhindar dari serangan yang dapat merugikan sebuah perusahaan atau organisasi. Keamanan Secara umum didefinisikan sebagai kualitas atau keadaan aman - tidak tunduk ataupun memiliki kedudukan yang terbuka kepada Bahaya". Keamanan adalah menjauhkan diri dari musuh dan Bahaya[8].

Keamanan informasi terdiri dari perlindungan terhadap aspek *Confidentiality, Integrity* dan *Availability*.

Gambar 4. Dasar Keamanan Informasi (CIA Triad)

Confidentiality (Kerahasiaan)

Aspek yang menjaga kerahasiaan data atau informasi, menjamin bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjaga kerahasiaan data yang dikirim, diterima dan disimpan [9]. Terdapat beberapa mekanisme yang digunakan untuk mendukung konsep confidentiality meliputi:

[8] M. E. Whitman, H. J. (2018). *Principles of Information Security 6th Edition.* Atlanta: Cengange Learning. Hal 92
[9] Osborne, M. (2006). *How to Cheat at Managing Information Security.* Florida: Syngress. Hal 51-56

Klasifikasi Data

Merupakan Proses pemberian label tingkat kerahasiaan informasi sehingga individu mengetahui siapa yang diizinkan untuk melihatnya dan siapa yang tidak. Klasifikasi data memiliki tiga kategori yaitu data biasa (*Ordinary Data),* Data Penting *(Critical Data),* dan Data Rahasia *(Confidential Data)*.

Enkripsi

Merupakan mekanisme teknis yang digunakan untuk menjaga kerahasiaan (confidentiality).

Penghapusan Data Rahasia (*Equipment Disposal*)

Merupakan bentuk usaha atau aktivitas yang ditujukan untuk melindungi kerahasiaan informasi ketika tidak digunakan lagi pada media penyimpanan. Sebagai contoh, proses format pada penyimpanan Tujuh Kali, penyobekan kertas dengan mesin shredder dan sebagainya.

Integrity (Integritas)

Aspek yang menjaga agar data atau informasi tidak dirubah tanpa ijin pihak yang berwenang (authorized), menjamin keakuratan dan keutuhan informasi serta prosesnya demi aspek integrity[10]. Adapun tujuan dari integrity adalah Mencegah modifikasi informasi yang dilakukan oleh user atau pengguna yang tidak berhak, Mencegah akses yang bersifat merusak dan tidak sah dari pengguna yang tidak berhak. Pemeliharaan terhadap konsistensi internal dan eksternal. Konsistensi internal menjamin bahwa data internal tetap konsisten. Jumlah item yang dimiliki oleh organisasi harus sama dengan yang ditampilkan pada database. Konsistensi eksternal menjamin bahwa data yang disimpan database konsisten dengan data fisik. jumlah item secara fisik harus sama dengan jumlah yang terdapat di dalam database.

[10] Ibid

Availability (Ketersediaan)

Aspek yang menyediakan data ketika dibutuhkan, memastikan perangkat atau pengguna memiliki akses untuk dapat memperoleh dan menggunakan informasi terkait. Bentuk-bentuk usaha yang dapat dilakukan untuk menjaga ketersediaan data yaitu: (1) Redundant Systems atau implementasi sistem berganda ke dalam suatu infrastruktur (seperti disk array atau mesin-mesin yang di-cluster). (2) Perangkat Lunak Anti-Virus untuk menghentikan worm atau program berbahaya lainnya yang mengganggu kondisi jaringan. (3) Penerapan perangkat *Intrusion Prevention System* (IPS) adalah sebuah perangkat lunak atau perangkat keras yang bekerja untuk monitoring trafik jaringan, mendeteksi aktivitas yang mencurigakan dan melakukan pencegahan dini terhadap penyusupan atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya.

Dengan dasar konsep ini, aspek-aspek keamanan informasi memiliki keterkaitan dengan pengamanan pada alur jaringan tidak hanya dari segi fisik yang dalam pengamanannya pula perlu pengaman dari segi fisik misalnya pengamanan perangkat dari terkena ancaman kebakaran, penyalahgunaan, ataupun bencana alam. Namun upaya pengamanan informasi meliputi juga Operation security dan Network security, dari sinilah kejahatan siber muncul tanpa adanya interaksi fisik dengan perangkat, pelaku kejahatan siber mampu melakukan tindakan pencurian data melalui jaringan yang terhubung ke perangkat yang dituju.

Konsep Persandian

Persandian adalah kegiatan di bidang pengamanan sistem informasi yang dilaksanakan dengan menerapkan konsep, teori dan seni dari ilmu kripto beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terikat pada etika profesi sandi sesuai dengan Peraturan Menteri Pertahanan Republik Indonesia Nomor 21 Tahun 2011 Tentang Pembinaan dan Penyelenggaraan Persandian pada pasal 1 ayat 3.

Persandian memiliki nilai strategis dan terkait dengan keamanan atau kerahasiaan data dan informasi, dapat dilindungi, namun tetap harus diperhatikan keterbukaan informasi yang telah mencakup seluruh aspek kehidupan masyarakat. Persandian juga harus membahas keyakinan publik tentang operasi pemerintah daerah yang bersih dan terbuka. Undang-undang Nomor 23 Tahun 2014 juga mengatur bahwa sub-masalah keamanan informasi dan persandian di tingkat pusat, provinsi, dan kabupaten/kota juga disebutkan[11].

Indeks Keamanan Informasi (KAMI 4.2)

Indeks KAMI adalah alat penilaian yang digunakan untuk menganalisis kesiapan suatu organisasi untuk keamanan informasi. Tujuan dari alat penilaian ini bukan untuk menganalisis kelayakan atau efektivitas formulir keamanan yang ada, melainkan sebagai alat untuk menunjukkan gambaran kesiapan (*completeness and maturity*) untuk memberikan gambaran kesiapan informasi kepada IAEA. memimpin kerangka keamanan. Penilaian dilakukan di berbagai bidang untuk menerapkan keamanan informasi, dan kerangka diskusi juga mematuhi semua aspek keamanan standar ISO/IEC 27001:2013.

Pada penelitian ini, penggunaan alat evaluasi ini adalah untuk menilai Tingkat Kesiapan Keamanan Informasi yang diterapkan di Instansi Pemerintah. Indeks KAMI memiliki standar Internasional ISO/IEC 27001: 2013 sebagai tolak ukur dalam pengelolaan Keamanan Informasi dan Persandian yang diterapkan di Instansi Pemerintah. Dengan standar Internasional dan diterbitkan oleh Badan Siber dan Sandi Negara, Indeks KAMI adalah tolak ukur yang memadai untuk meninjau secara kuantitatif pengelolaan Keamanan Informasi.

Penggunaan Indeks KAMI pada penelitian ini hanya sebagai perbandingan dengan hasil tinjauan oleh peneliti dengan menggunakan teori Dasar Keamanan, sehingga dalam hal ini, Peneliti bukanlah pihak yang berwenang untuk melakukan evaluasi menggunakan alat ukur Indeks KAMI, melainkan penelitian ini hanya

[11] Budiman, A. (2016, Mei). Urgensi Pengaturan Persandian Di Pemerintah Daerah. *Info Singkat*. . Hal 17-19

menggunakan data dari hasil evaluasi yang dilakukan oleh Badan Siber dan Sandi Negara kepada instansi Terkait.

2. Metode Penelitian

Objek pada penelitian ini adalah Pengelolaan Keamanan Informasi dan Persandian atau sistem manajemen keamanan informasi serta Tingkat Kematangan keamanan ditinjau dari evaluasi keamanan informasi. Penelitian ini menggunakan metode Deskriptif dengan pendekatan Kualitatif di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur sebagai metode untuk menguraikan Pengelolaan yang dilakukan dengan ini pembaca akan memahami kekurangan serta kelebihan dari pengelolaan keamanan informasi dan persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur. Teknik pengumpulan data dengan melakukan Wawancara terhadap Informan yang terlibat dalam kegiatan pengamanan Informasi dan Persandian di Diskominfo Kaltim. Kemudian untuk meninjau kegiatan dan fasilitas yang tersedia, peneliti juga melakukan observasi terhadap lokasi penelitian yang bertempat di kantor Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur dan mengumpulkan sumber data yang relevan dengan kegiatan Pengelolaan Keamanan Informasi dan Persandian seperti Rencana Strategi Diskominfo Kaltim Tahun 2019-2023, Ketersediaan sarana dan prasarana, legalitas pelaksanaan kegiatan keamanan informasi dan persandian serta hasil evaluasi keamanan informasi yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN) di Diskominfo Kaltim menggunakan alat evaluasi Indeks Keamanan Informasi versi 4.2 (Indeks KAMI 4.2).

Tabel 1. Data Informan

NO.	INFORMAN
1	Kepala Dinas Komunikasi dan Informatika
2	Kepala Bidang TIK dan Persandian
3	Kepala Seksi Keamanan Informasi dan Persandian
4	Kepala Seksi Infrastruktur Teknologi Informasi Komunikasi
5	Kepala Seksi Pengelolaan Data dan Integrasi Sistem Informasi
6	Analis Sistem Informasi dan Jaringan

Informan pada penelitian ini merupakan informan yang terlibat didalam proses Pengamanan Informasi. Informan ini merupakan Pegawai Diskominfo Kaltim dari Bidang Keamanan Informasi dan Persandian dengan tugas dan fungsi pembangunan infrastruktur dan Pengamanan Informasi dan Persandian. Setelah dilakukan pengumpulan data dengan wawancara kepada informan dan observasi oleh peneliti, Peneliti akan meganalisis data yang diperoleh dengan membandingkan kesesuaian data dengan Teknik analisis data yang penulis terapkan, yaitu dengan teknik analisis triangulasi dengan melakukan wawancara dengan informan di intansi terkait, observasi yang dilakukan oleh peneliti di lingkungan kerja, kemudian mengumpulkan data pendukung yang relevan dengan penelitian ini. Didukung dengan data dari hasil evaluasi dari Indeks KAMI 4.2. kemudian data ditarik kesimpulan dengan menggunakan metode induktif. Kegiatan analisis data secara simultan dibagi menjadi tiga alur kegiatan, yaitu reduksi data, penyajian data, dan penarikan kesimpulan/verifikasi.

3. Hasil Dan Pembahasan

Setelah dilakukan penelitian di lapangan, pada bagian ini akan dibahas mengenai Bagaimana Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informasi Provinsi Kalimantan Timur dengan meninjau kelemahan dan kelebihan, upaya yang dilakukan, serta fasilitas yang menyangkut kelengkapan dalam pengamanan informasi sesuai dengan konsep CIA TRIAD, didukung juga dengan data evaluasi hasil tingkat Keamanan Informasi dan Persandian dengan alat Indeks KAMI 4.2 yang telah dievaluasi oleh Badan Siber dan Sandi Negara di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur.

Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur

Pelaksanaan Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur berdasarkan landasan Peraturan Gubernur Kalimantan Timur Nomor 41 Tahun 2020 tentang Susunan

Organisasi, Tugas, Fungsi, Dan Tata Kerja Dinas Komunikasi Dan Informatika, Provinsi Kalimantan Timur khususnya pada bidang TIK dan Persandian. Dengan begitu pengelolaan Keamanan Informasi dan Persandian telah menjadi agenda bagi Diskominfo Provinsi Kalimantan Timur dalam Penanganan Insiden Keamanan Informasi dan Pengawasan dan pengendalian pengamanan informasi, persandian, pos dan telekomunikasi. Hal ini berdasarkan pada Rencana Strategis Diskominfo Provinsi Kalimantan Timur Tahun 2019 – 2023.

Tanggung jawab Diskominfo dalam Keamanan Informasi dan Persandian adalah Dokumen yang diarsipkan berupa fisik maupun digital yang tersimpan di dalam kantor Diskominfo Kalitm dan tersimpan secara digital dalam penyimpanan awan atau *cloud* termasuk *Website* yang dikelola oleh Diskominfo Kaltim. Kemudian juga Diskominfo Kaltim memiliki tanggung jawab untuk mengatasi masalah Keamanan yang terjadi pada *Website* Dinas lainnya di ruang lingkup Provinsi Kalimantan Timur, sehingga ketika Diskominfo menerima laporan dari dinas lain bahwa terdapat masalah atau ancaman keamanan informasi dan kerentanan persandian, tim khusus pengamanan informasi dan persandian dari Diskominfo Kaltim bersedia untuk ikut serta menyelesaikan permasalahan yang terjadi pada dinas lainnya pada provinsi Kalimantan Timur. Bantuan yang dilakukan oleh Diskominfo Kaltim pada dinas lainnya hanya dalam penyelesaian masalah keamanan informasi dan persandian yang dilaporkan dari dinas lain kepada Diskominfo, penyimpanan data dan pengarsipan dari dinas lain di Kantor Diskominfo Kaltim tidak menjadi tugas dan tanggung jawab Diskominfo Kaltim.

Kemudian ditinjau Berdasarkan Teori CIA TRIAD (*Confidentiality, Integrity, Availability*), dalam Sistem Manajemen Keamanan Informasi yang menggunakan standar ISO/IEC 27001: 2013 bahwa keamanan informasi dapat diukur tingkat keamanannya dari dimensi yang disebutkan untuk mengetahui tingkat persiapan organisasi dalam mengamankan informasi dan data yang dianggap rahasia. Tingkat Kesiapan keamanan informasi dan persandian menjadi sangat penting karena mencakup hal yang mendasari untuk menjalankan tahapan-tahapan selanjutnya dalam mengamankan informasi seperti fasilitas dan keahlian, sehingga tingkat

kesiapan keamanan informasi dan persandian tidak hanya dilihat sebagai sistem tetapi kompetensi karyawan atau pegawai menjadi hal yang krusial dalam memutuskan strategi dalam pengamanan informasi dan menerapkan persandian.

Pada penelitian ini akan dilakukan analisis pengumpulan data menggunakan wawancara yang didasari teori *CIA TRIAD* oleh Whitman dan dengan didukung oleh hasil evaluasi keamanan informasi dan persandian dengan alat evaluasi bernama Indeks KAMI Versi 4.2 yang diterbitkan oleh Badan Siber dan Sandi Negara dengan standar ISO/IEC 27001: 2013. Landasan Teoritis serta hasil evaluasi tersebut mampu menggambarkan kesiapan Diskominfo Provinsi Kalimantan Timur dalam mengamankan Informasi serta menerapkan Persandian dalam mengamankan informasi dan data yang dianggap penting serta menjadi aset bagi organisasi. Berikut Hasil dan Pembahasan menggunakan Indikator dari masing-masing Dimensi pada teori *CIA Triad*:

a) Klasifikasi Data

Sesuai dengan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik dan pelaksanaan UU No. 14 Tahun 2008 tercantum pada Peraturan Daerah Nomor 15 Tahun 2012 tentang Layanan Informasi Publik Di Lingkungan Pemerintah Provinsi Kalimantan Timur menerangkan bahwa dalam pengelolaan data yang pada hal ini dilaksanakan oleh Organisasi Perangkat Daerah Dinas Komunikasi dan Informatika dan Pejabat Pengelola Informasi dan Dokumentasi (PPID) yang menjadi bagian dari Diskominfo, bahwa terdapat Informasi yang wajib disediakan dan diumumkan dan informasi yang dikecualikan yang bersifat rahasia dan tidak dipublikasikan. Dapat disimpulkan bahwa Dinas Komunikasi dan Informatika Kaltim seharusnya menerapkan Klasifikasi data dalam artian mengkategorikan Informasi yang bersifat umum atau dapat dipublikasikan dan Informasi Rahasia yang tidak dapat dipublikasikan.

Dalam Indikator Klasifikasi Data terdapat tingkat kelompok pengklasifikasian data, sedangkan dari pengklasifikasian Data yang dilakukan oleh Diskominfo Provinsi Kaltim seperti yang disampaikan oleh informan dalam wawancara yang

dilakukan peneliti adalah dengan mengklasifikasikan informasi berdasarkan kepentingannya. Kepentingan seperti informasi untuk masyarakat tentu informasi yang tidak bersifat rahasia dan dapat diakses oleh khalayak umum, namun untuk kepentingan antar dinas seperti surat ataupun undangan bersifat terbatas. Maka dari itu klasifikasi data pada Diskominfo Provinsi Kaltim bersifat *Critical Data* atau Data Penting, dan *Ordinary Data* Atau Data Biasa, Sedangkan Untuk *Confidential Data* atau Data Rahasia masih belum secara khusus diklasifikasikan oleh Diskominfo Provinsi Kaltim.

Pada dasarnya sesuai dengan Perda Provinsi Kalimantan Timur Nomor 15 Tahun 2012 terdapat Informasi yang wajib disediakan dan diumumkan dan Informasi yang dikecualikan. Informasi yang wajib disediakan dan diumumkan secara berkala terdapat pada pasal 18 sampai pasal 23, sedangkan Informasi yang dikecualikan terdapat pada pasal 24 sampai pasal 27 Perda Provinsi Kalimantan Timur Nomor 15 Tahun 2012. Dalam penerapan pada klasifikasi data, Informasi yang wajib disediakan merupakan *Ordinary Data* atau data biasa yang tidak memiliki kerahasiaan untuk dipublikasikan kepada masyarakat, sedangkan Informasi yang dikecualikan merupakan *Critical* hingga *Confidential Data* atau Data Penting hingga Rahasia yang tidak untuk dipublikasikan ke publik karena dapat menghambat, merugikan, hingga membahayakan organisasi sesuai dengan yang disebutkan pada Perda Provinsi Kalimantan Timur Nomor 15 Tahun 2012.

b) Penerapan Enkripsi

Berdasarkan hasil wawancara yang dilakukan peneliti kepada 2 responden, terdapat perbedaan pendapat. Perbedaan ini dikarenakan perbedaan tugas dalam penggunaan data di jabatan tertentu. Kepala Seksi Keamanan Informasi dan Persandian berfokus kepada penerapan enkripsi dalam transfer informasi antar dinas dimana dalam penjelasannya bahwa dalam transfer file antar dinas tidak memerlukan penerapan enkripsi, sedangkan Kepala seksi Pengelolaan Data dan Integrasi Sistem Informasi berfokus kepada penerapan enkripsi pada penyimpanan dan pengarsipan data. Keterangan yang diberikan oleh Kepala Seksi Pengelolaan

Data dan Integrasi Sistem bahwa data telah dicadangkan ke Synology Drive. Synology NAS Rackstation merupakan salah satu produk solusi penyimpanan pada jaringan komputer server untuk skala perusahaan menengah sampai enterprise dan data center yang menggunakan teknologi *Btrfs* yang tentunya sudah terenkripsi yang menjamin keamanan dalam penyimpanan data secara awan (*Cloud*) sehingga dari keterangan ini Diskominfo telah menerapkan enkripsi dalam penyimpanan dan pengarsipan data dan informasi sedangkan untuk transfer file antar dinas, enkripsi tidak diperlukan.

Berdasarkan Rencana Strategis (RENSTRA) Diskominfo Tahun 2019-2023, Diskominfo memiliki Rencana Program dan Kegiatan yang berhubungan dengan penerapan enkripsi, yaitu pada Program Pembinaan dan Pengembangan Sumber Daya Kominfo dengan Indikator Kinerja Program yaitu Meningkatnya sistem pemerintahan berbasis elektronik serta tersedianya data dan Informasi KPU/USO, Telekomunikasi dan Penyiaran, Informasi sandi yang ter-enkripsi, Dalam kegiatan Pengawasan dan pengendalian pengamanan informasi, persandian, pos dan telekomunikasi dengan harapan Tersedianya data dan informasi yang ter-enkripsi. Hal ini menjelaskan bahwa Diskominfo dalam Rencana Program dan Kegiatan pada RENSTRA Tahun 2019-2023 untuk mencapai visi dan misinya, telah melaksanakan penerapan dan penyediaan data dan informasi yang telah ter-enkripsi. Sehingga penerapan enkripsi di Diskominfo telah terprogram dan diterapkan dalam penyimpanan informasi pada arsip.

c) Penghapusan data secara berkala *(Equipment Disposal).*

Diskominfo Provinsi Kalimantan Timur belum memiliki program khusus untuk penghapusan data yang tidak digunakan secara berkala tetapi untuk selalu mengarsipkan data yang tersedia. Hal ini disebabkan karena belum adanya kebijakan dan prosedur dalam rutinitas penghapusan data dari Diskominfo Kaltim. Namun pada RENSTRA Diskominfo tahun 2019-2023 bahwa dalam aset dan modal terdapat 5 buah mesin penghancur kertas, hal ini termasuk kedalam ketersediaan penerapan penghapusan data.

Berdasarkan ISO/IEC 27001:2013 mengenai Sistem Manajemen Keamanan Informasi, *Equipment disposal* dengan kontrol bahwa Semua item peralatan yang mengandung media penyimpanan harus diverifikasi untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa dengan aman sebelum dibuang atau digunakan kembali. Hal ini dilakukan untuk mencegah kehilangan, kerusakan, pencurian dan gangguan pada operasi organisasi.

d) Pencegahan Modifikasi

Diskominfo Provinsi Kalimantan Timur pada dasarnya telah melakukan berbagai macam upaya dalam mencegah adanya serangan siber yang terjadi dimulai dari sisi internal organisasi, dengan meningkatkan kompetensi pegawai dengan melakukan pelatihan yang diberikan oleh Badan Siber dan Sandi Negara (BSSN) sehingga diberi kepercayaan untuk membentuk team bersertifikasi *Computer Security Incident Response Team (*CSIRT*). CSIRT* merupakan sebuah satuan organisasi yang mempunyai fungsi utama mengkoordinir pelaksanaan kegiatan tanggap insiden siber. Keberadaannya sangat dibutuhkan oleh setiap organisasi untuk meminimalisir dampak dari risiko yang disebabkan oleh insiden siber. Kemudian juga Diskominfo Kaltim telah melengkapi perlengkapan Anti serangan siber dengan alat monitoring seperti Wazuh yang membantu untuk mendeteksi anomali pada jaringan serta *Firewall* untuk mencegah serangan siber.

Kemudian upaya yang dilakukan dari sisi eksternal meliputi sosialisasi kepada pegawai dan masyarakat untuk menggunakan internet dengan bijaksana, sehingga keamanan data dan informasi yang bersifat pribadi dan penting bisa terjaga dari pencurian data seperti *Phising* yang bisa disalahgunakan oleh pihak yang tidak bertanggungjawab. Keterangan yang diberikan informan mengenai upaya yang dilakukan Diskominfo Kaltim dalam mencegah anomali dan serangan siber adalah bahwa Diskominfo telah berupaya besar untuk mencegah serangan siber terjadi dengan tindakan dan persiapan perangkat yang sangat lengkap dari sisi internal maupun eksternal.

e) Pencegahan Akses Ilegal.

Upaya dari pencegahan akses ilegal yang dilakukan Diskominfo Kaltim berawal dari pencegahan ancaman akses ilegal yang berasal dari internal organisasi, yaitu dengan memberi akses kepada pihak yang kompeten dan terpercaya untuk mengamankan data yang disimpan. Kemudian untuk mencegah adanya akses ilegal yang berasal dari eksternal dengan upaya yaitu melindungi aset data kependudukan. Upaya tersebut juga dapat ditinjau pada Indikator upaya pencegahan anomali dan penerapan *Intrusion Prevention System* (IPS). Anomali merupakan langkah pertama dari peretas untuk dapat menyusup kedalam sistem hingga akhirnya terjadi pencurian data hingga akses ilegal, Sehingga akses ilegal yang terjadi merupakan lolosnya peretas dari alat deteksi anomali dan dari keterangan yang diberikan informan melalui wawancara, akses ilegal terbesar merupakan penggantian halaman depan atau *Defacement*. Hal ini termasuk ke dalam akses ilegal karena hanya administrator yang dapat mengubah tampilan yang ada dan upaya yang dilakukan Diskominfo Kaltim yaitu mengubah tampilan kembali ke keadaan semula kemudian selalu memonitor akses ilegal yang terjadi, dan bagi Diskominfo kejahatan tersebut tidak terlalu merugikan karena tidak berkaitan dengan pencurian data melainkan hanya mengubah tampilan depan pada *website*.

f) Pemeliharaan Konsistensi.

Konsistensi data antara data yang berupa fisik dengan data yang ada pada digital atau data yang diunggah pada penyimpanan awan (*cloud)* sudah konsisten dan selalu diupayakan untuk selalu konsisten walaupun terdapat serangan-serangan siber yang mengakibatkan kerusakan data ataupun perubahan data yang terjadi pada *website* ataupun database dari Diskominfo sendiri, namun hal tersebut dapat cepat diatasi dengan upaya pemulihan data yang dilakukan oleh Diskominfo. Dengan alat deteksi serangan siber yang mampu mendeteksi serangan yang terjadi, Diskominfo mampu mencegah adanya ketidaksamaan data fisik dengan data digital.

g) *Redundant System.*

Fasilitas yang tersedia, khususnya komputer tidak menerapkan sistem berganda bahkan kurang. Observasi yang dilakukan peneliti di ruangan kantor Bidang TIK dan Keamanan Informasi, peneliti mengamati bahwa pada meja kerja pegawai terdapat masing-masing komputer kerja dengan jumlah yang sesuai dengan jumlah pegawai. Dengan artian bahwa keterangan yang diberikan informan kepada peneliti sudah sesuai dengan keadaan yang sebenarnya.

Tabel 2. Aset dan Modal Dinas Kominfo Prov. Kaltim (Nomor 1 sampai 5)

No.	Jenis Barang	Jumlah Unit	Keterangan
1	Komputer	24	Kondisi baik/Masih digunakan
2	Air Conditioner/AC	55	Kondisi baik/Masih digunakan
3	Printer	40	Kondisi baik/Masih digunakan
4	Kursi Kayu / Busa	13	Kondisi baik/Masih digunakan
5	Kursi Kerja	20	Kondisi baik/Masih digunakan

Aset dan modal Dinas pada gambar diatas menunjukkan jumlah unit komputer pada Diskominfo secara keseluruhan yang dibagikan kepada seluruh bidang di Diskominfo, observasi yang peneliti lakukan dalam ruangan Bidang TIK dan Persandian Diskominfo Kaltim, bahwa setiap pegawai tercukupi masing-masing memiliki setidaknya 1 perangkat komputer yang berarti Redundansi belum diterapkan karena pada dasarnya redudansi berarti menyiapkan perangkat cadangan yang akan digunakan ketika terdapat gangguan atau kerusakan, sehingga tidak mengganggu operasi pada kantor terutama dalam mendeteksi dan mencegah adanya serangan siber.

h) Perangkat Lunak *Anti-Virus.*

Anti-virus adalah alat yang sangat penting dalam melakukan upaya pengamanan informasi, karena *virus* merupakan sebuah serangan siber yang digunakan untuk merusak sistem dari internal, sehingga sistem dapat menjadi rentan hingga rusak kemudian peretas akan sangat mudah mengambil informasi atau merusak bahkan menghapus semua informasi yang tersedia untuk kepentingan pribadi. Penerapan dan pemasangan *Anti-virus* di Diskominfo Kaltim sudah diterapkan, hal ini dijelaskan oleh informan terkait jenis anti-virus yang dipasang. *Anti-virus* yang dipasang pada perangkat komputer di Diskominfo Kaltim menggunakan *anti-virus* bawaan dari *Microsoft Windows 10* yaitu *Windows Defender*. Diskominfo Kaltim telah menerapkan pemasangan anti-virus berbayar untuk menjaga keamanan informasi dan data untuk mencegah adanya serangan dari virus yang membuat kerusakan secara internal sehingga rentan terjadi serangan siber.

i) Perangkat *IPS.*

Penerapan *Intrusion Prevention System* sudah diterapkan dan dikelola langsung oleh Diskominfo Kaltim dan jenis dari alat *IPS* yang diterapkan adalah BitNinja. BitNinja merupakan alat pendeteksi alamat *IP* (*Internet Protocol*) yang memiliki aktivitas yang mencurigakan dan langsung menghapuskan IP tersebut dari akses yang diberikan, sebagai contoh akses *website* dan sebagainya. Berbeda dengan *Intrusion Detection System (*IDS*)* yang hanya mendeteksi dan mengirimkan peringatan saja. Namun kedua hal tersebut telah diterapkan pada Diskominfo menjadikan pertahanan yang ganda untuk mencegah adanya peretasan berupa akses ilegal, pembajakan dan aktivitas yang mencurigakan (anomali). Adapun aplikasi yang digunakan yaitu BitNinja (*IPS*) dan Wazuh (*IDS*).

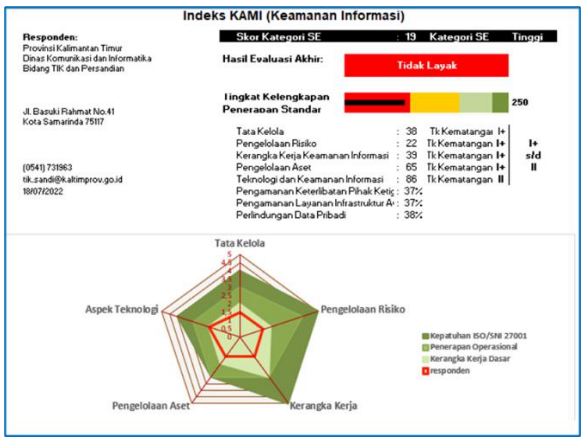
Pengamanan Sistem Elektronik di Provinsi Kalimantan Timur telah tertuang dalam Peraturan Gubernur Kalimantan Timur Nomor 20 Tahun 2022 tentang Pedoman Penyelenggaraan Persandian Untuk Pengamanan Informasi Pemerintahan Daerah. Dalam melaksanakan Pengamanan, Dinas Kominfo

melakukan identifikasi, deteksi, proteksi dan penanggulangan dan pemulihan. Deteksi dilakukan melalui kegiatan analisis untuk menentukan adanya ancaman atau kejadian insiden pada Sistem Elektronik. Berdasarkan hal ini sudah menjadi keharusan bagi Diskominfo untuk melakukan upaya dalam pencegahan adanya serangan siber dengan menerapkan alat deteksi *Intrusion Prevention System* (IPS) dan keadaan dilapangan sudah menunjukkan bahwa penerapan telah dilakukan dari hasil observasi penulis dan juga didukung dari hasil evaluasi Indeks Keamanan Informasi (KAMI 4.2).

Tingkat Keamanan Informasi di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur.

Indeks KAMI merupakan aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001. Peninjauan Indeks KAMI 4.2 dilaksanakan oleh Badan Siber dan Sandi negara kepada Instansi terkait dengan Aspek Kategori Sistem Elektronik, Tata Kelola, Risiko, Kerangka Kerja, Pengelolaan Aset, Teknologi dan Sumplemen. Sehingga, peneliti menggunakan hasil evaluasi sebagai data pendukung antara observasi yang dilakukan oleh peneliti, dengan hasil evaluasi yang dilakukan oleh Badan Siber dan Sandi Negara.

Berikut Hasil Kekuatan/Kematangan dan Kelemahan/Kekurangan dari masing-masing aspek Berdasarkan Laporan INDEKS KAMI 4.2 yang dilaksanakan oleh Badan Siber dan Sandi Negara di Diskominfo Provinsi Kalimantan Timur, Samarinda 21 Juli 2022:



Gambar 5. Evaluasi Indeks KAMI (Keamanan Informasi)

Penilaian Mandiri Indeks KAMI dilakukan di tahun 2022 ini dengan ruang lingkup Diskominfo Pemerintah Provinsi Kalimantan Timur, Ruang Server dan Sistem Informasi yang dikelola dan dilakukan verifikasi oleh Tim BSSN. Dari ketiga kategori sistem elektronik, Tim BSSN mengkategorikan Diskominfo Kaltim dengan kategori **Tinggi** dengan hasil **Tidak Layak** dengan total nilai **250**.

Pada tahun 2022 ini merupakan periode kali pertama bagi lingkup Diskominfo Pemerintah Provinsi Kalimantan Timur dilakukan verifikasi oleh Tim BSSN dalam penilaian mandiri Indeks KAMI, sehingga sesuai mekanisme kebijakan yang ada untuk pelaksanaan kegiatan verifikasi adalah dengan melakukan pengecekan keseluruhan kelengkapan kebijakan dan/atau prosedur dan penerapan dokumen kebijakan dan/atau prosedur pada area Kategori, Tata Kelola, Pengelolaan Risiko, Aset, Teknologi dan Keamanan Informasi serta Suplemen. Pada pelaksanaan verifikasi, Tim Asesor berupaya untuk membantu dan mengarahkan lingkup Diskominfo Pemerintah Provinsi Kalimantan Timur untuk dapat memperbaiki dan meningkatkan implementasi Keamanan Informasi sesuai ruang lingkup Diskominfo melalui penyiapan data dukung/ *evidence*.

Diskominfo Provinsi Kalimantan Timur telah melakukan evaluasi Menggunakan Indeks KAMI dengan Hasil Evaluasi Akhir yaitu **Tidak Layak**, dengan tingkat keamanan I+ sampai dengan II+. Tingkat Kematangan penerapan pengamanan dengan kategorisasi mengacu kepada tingkatan kematangan

berdasarkan kerangka kerja COBIT atau CMMI. Tingkat kematangan didefinisikan sebagai:

a) Tingkat I – Kondisi Awal
b) Tingkat II – Penerapan Kerangka Kerja Dasar
c) Tingkat III – Terdefinisi dan Konsisten
d) Tingkat IV – Terkelola dan Terukur
e) Tingkat V - Optimal

Untuk membantu memberikan uraian yang lebih detail, kemudian tingkatan ini ditambahkan dengan tingkatan antara – I+, II+, III+, dan IV+, sehingga total terdapat 9 tingkatan kematangan. Berdasarkan standar ISO/IEC 27001: 2013, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+. Mengacu kepada hasil evaluasi di Diskominfo Kaltim dengan Tingkat Keamanan I+ - II+, yang berarti tingkat keamanan berdasarkan ISO/IEC 27001: 2013 masih jauh dari ambang batas minimum yaitu pada Tingkat III+. Diskominfo Provinsi Kalimantan Timur tidak hanya menganggap keberatan memenuhi standar dari alat evaluasi Indeks KAMI, hal ini dikarenakan standar dari Indeks KAMI yang terlalu tinggi yaitu menggunakan standar internasional ISO/IEC 27001: 2013, yang berarti standar yang digunakan sangat tinggi sehingga Diskominfo Keberatan untuk memenuhi kebutuhan standarisasi keamanan informasi tingkat tinggi. Diskominfo juga melakukan evaluasi menggunakan alat evaluasi lainnya yaitu menggunakan *CSN*. Walaupun begitu, Diskominfo Kaltim tetap menggunakan semua jenis alat evaluasi dari BSSN untuk meninjau tingkat keamanan siber dan persandian di Diskominfo Kaltim.

Cyber Security Network atau CSN adalah asosiasi mandiri untuk mengevaluasi keamanan sistem informasi, CSN sendiri memiliki standar yang berbeda dari ISO 27001: 2013. Walaupun Diskominfo mengakui bahwa telah mendapatkan level yang cukup pada alat evaluasi lainnya, namun standarisasi ISO/IEC 27001: 2013 yang bersifat dan diakui secara internasional masih menempati tingkat terendah dan

masih dalam proses untuk mengupayakan pengelolaan keamanan informasi dan persandian yang layak serta aman dari ancaman serangan siber.

4. Kesimpulan

Setelah dilakukan penelitian dilapangan oleh peneliti menggunakan teknik wawancara, observasi dan dokumentasi, ditarik kesimpulan dari masing-masing dimensi pada teori yang digunakan pada penelitian ini. Pengelolaan Keamanan Informasi dan Persandian di Dinas Kominfo Provinsi Kalimantan Timur setelah ditinjau menggunakan teori *CIA Triad* yang terdiri atas 3 dimensi yang ada pada penelitian yaitu Kerahasiaan, Integritas dan Ketersediaan dapat disimpulkan sebagai berikut:

Pertama, Kerahasiaan pada Diskominfo Kaltim ditinjau dari klasifikasi yang ada terdapat 2 jenis klasifikasi data yaitu *Critical Data* dan *Ordinary* Data. Penggunaan Enkripsi diterapkan pada penyimpanan dan pengarsipan dokumen. Dan kemudian Penghapusan Data Berkala belum dilaksanakan melainkan segala dokumen disimpan dan diarsipkan.

Kedua, Integritas pada Diskominfo Kaltim, upaya dalam pencegahan modifikasi yang dilakukan secara internal dan eksternal, secara internal yaitu dengan memberikan pelatihan kepada pegawai dan membentuk tim cepat tanggap serangan siber *Computer Security Incident Response Team (*CSIRT*)* serta membekali kantor dengan alat monitoring Wazuh untuk mendeteksi adanya anomali sebagai sinyal adanya aktivitas yang mencurigakan. Secara eksternal pencegahan dilakukan dengan memberikan himbauan kepada pegawai dan masyarakat agar menggunakan internet dengan bijaksana agar tidak terjadi pencurian data ataupun jenis peretasan lainnya. Kemudian pencegahan akses ilegal di Diskominfo Kaltim yaitu dengan memberikan akses kepada pegawai yang kompeten dan terpercaya dan juga dengan membekali kantor dengan alat *Intrusion Detection System* BitNinja yaitu alat yang mampu mendeteksi serangan yang terjadi kemudian secara otomatis mengatasi serangan yang terjadi. Pemeliharaan Konsistensi yang dilakukan adalah dengan

menjaga dokumen yang diarsipkan dan mengunggah dokumen fisik ke penyimpanan awan (*cloud*) dan memastikan data yang diunggah dan fisik tetap sama serta mengupayakan untuk mencegah serangan serta modifikasi yang terjadi.

Ketiga, yaitu Ketersediaan peralatan Keamanan di Diskominfo Kaltim. Diskominfo Kaltim tidak memiliki perangkat cadangan atau redudansi pada perangkat sehingga sangat rentan jika suatu saat terjadi serangan. Kemudian Diskominfo Kaltim menggunakan *Anti-Virus* bawaan dari *Windows 10 yaitu Windows Defender*. Untuk mencegah adanya serangan, Diskominfo Kaltim telah membekali kantor dengan *Intrusion Prevention System* yaitu BitNinja yang mampu mendeteksi dan secara otomatis mencegah serangan yang terjadi.

Meski serangan siber yang terjadi tidak terlalu beresiko tinggi bagi organisasi seperti serangan *defacement* dan modifikasi data, namun jika terjadi serangan yang lebih besar maka Diskominfo Kaltim belum siap dalam menghadapi serangan tersebut ditinjau dari fasilitas yang masih kurang dan belum menerapkan *Redundant System* yang menjadi *Backup plan* dalam mengatasi berhentinya operasi dalam organisasi dalam kasus ini pemantauan dan pencegahan serangan siber. Hal ini juga didukung dari hasil evaluasi menggunakan Indeks KAMI yang menunjukkan tingkat kesiapan Diskominfo Kaltim berdasarkan standar ISO/IEC 27001: 2013 yang masih sangat rendah yaitu masih pada **Tingkat I+ - II+.** Hal tersebut masih jauh dari tingkat kesiapan sesuai standar yang ditetapkan oleh karena itu kerentanan dalam pengamanan informasi masih sangat tinggi.

Pada dasarnya Diskominfo Kaltim telah berupaya untuk meningkatkan Keamanan Informasi dan Persandian seperti menerapkan Enkripsi dalam pengarsipan informasi pada *Synology,* pencegahan adanya Modifikasi data menggunakan alat monitoring Wazuh dan BitNinja, dan penggunaan *Anti-Virus* dan penerapan *Intrusion Prevention System*. Diskominfo Kaltim Dalam evaluasi menggunakan alat evaluasi berupa *Cyber Security Network* telah mendapatkan skor yang cukup tinggi namun alat evaluasi ini belum terstandar secara internasional sehingga belum cukup akurat dalam mengukur tingkat keamanan yang tersedia.

5. Daftar Pustaka

Amir Hamzah, M. (2019). Metode Penelitian Kualitatif, Konstruksi Pemikiran Dasar serta Contoh Penerapan Pada Ilmu Pendidikan, Sosial & Humaniora. Batu: Literasi Nusantara.

Budiman, A. (2016, Mei). Urgensi Pengaturan Persandian Di Pemerintah Daerah. Info Singkat.

Dhruba Kumar Bhattacharyya, J. K. (2014). Network Anomaly Detection A Machine Learning Perspective. London: CRC Press.

Dowling, D. M. (2013). Cyber crime: A review of the evidence. Home Office Research Report 75.

Gunawan, C. E. (2018). Pengukuran Keamanan Informasi Menggunakan Keamanan Informasi (KAMI) Studi Kasusu di PUSTIPD UIN Raden Fatah Palembang. JUSIFO (Jurnal Sistem Informasi).

Halilul Khairi, M. (2017). Dinamika Pelaksanaan Urusan Di Bidang Persandian Pemerintah Daerah. In A. A. Prayudi, Dinamika Pelaksanaan Urusan Di Bidang Persandian Pemerintah Daerah. Jakarta: Yayasan Pustaka Obor Indonesia.

Ikhbaluddin, (2021). Pelayanan Publik Berbasis Online di Desa (Studi pada empat desa di Kecamatan Jatinangor). *Jurnal Teknologi dan Komunikasi Pemerintahan, 3(2).*

Lisdawati, Yuni, (2022) Penggunaan Media Sosial dalam Penyebarluasan Informasi Program Pemerintah di Dinas Komunikasi Informatika Statistik dan Persandian Kabupaten Rokan Hilir Provinsi Riau. *Jurnal Teknologi dan Komunikasi Pemerintahan*, *4(2).*

M. E. Whitman, H. J. (2018). Principles of Information Security 6th Edition. Atlanta: Cengange Learning.

Merrill Warkentin, C. o. (2020). Using the security triad to assess blockchain technology in public sector applications. International Journal of Information Management, 2-3.

Miles, M. B. (1992). Analisis data Kualitatif : buku sumber tentang metode baru. Jakarta: UI Press.

Nurrahman, A., Dimas, M., Ma'sum, M. F., & Ino, M. F. (2021). Pemanfaatan Website Sebagai Bentuk Digitalisasi Pelayanan Publik di Kabupaten Garut. *Jurnal Teknologi dan Komunikasi Pemerintahan*, *3(1)*.

Osborne, M. (2006). How to Cheat at Managing Information Security. Florida: Syngress.

Kosasi, S. (2002). Peran Teknologi Informasi dalam Pengembangan Organisasi. *Jurnal Teknologi Informasi,* Edisi Januari, Volume VII.

Sari, W. P., & Soegiarto, A. (2019). FUNGSI DAN PERAN HUMAS DI LEMBAGA PENDIDIKAN. *Communicology: Jurnal Ilmu Komunikasi*, *7*(1). https://doi.org/10.21009/COMMUNICOLOGY.14.03

Setiawan, M. R. (2021). Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII. AUTOMATA, Diseminasi Tugas Akhir Mahasiswa.

Sugiyono. (2016). Metode Penelitian Kuantitatif, Kualitatif, R&D. Bandung: IKAPI.

Tehubijuluw Zacharias, S. M. (2019). Metode Penelitian Sosial Teori dan Aplikasi. Ponorogo: Uwais Inspirasi Indonesia.

Yudi Herdiana, Z. M. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. Jurnal ICT: Information Communication & Technology.