PENGELOLAAN KEAMANAN INFORMASI DAN PERSANDIAN DI DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI KALIMANTAN TIMUR

ALDI DINATA SAPUTRA

NPP. 30.0981

Asdaf Kabupaten Kutai Kartanegara, Provinsi Kalimantan Timur

Program Studi Teknologi Rekayasa Informasi Pemerintahan

Email: saputraaldi480@gmail.com

ABSTRACT

Problem Statement/Background: *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.* ***Purpose:*** *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.* ***Method:*** *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.* ***Results:*** *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+.* ***Conclusion:*** *Office of Communication and Informatics, East Kalimantan Province are not reaching the minimum requirement for basic information security standard.*

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

Abstrak

Permasalahan/Latar Belakang: 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. **Tujuan:** 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. **Metode:** 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/Temuan:** 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+. **Kesimpulan:** Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur belum mencapai ketentuan minimal standar keamanan informasi.

Kata-kata Kunci: Informasi, Kejahatan Siber, Keamanan Informasi, Persandian

I. PENDAHULUAN

1.1 Latar Belakang

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[1].

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. Oleh karena itu, pemerintah telah mengambil langkah-langkah strategis untuk memenuhi harapan pelayanan publik yang berkualitas dengan mengesahkan Undang-Undang Nomor 25 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.

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[2].

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.

---

[1] Sari, W. P. (2019). FUNGSI DAN PERAN HUMAS DI LEMBAGA PENDIDIKAN. *Communicology: Jurnal Ilmu Komunikasi*. Hal. 49

[2] 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

Penggunaan teknologi informasi juga membutuhkan manajemen keamanan informasi untuk melindungi aset institusi, informasi dianggap aset yang sangat berharga dan perlu untuk dilindungi[3].

1.2 Kesenjangan Masalah yang Diambil

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[4].

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 mengakses, mengubah, ataupun menghapus data, sehingga dari gambar diatas menunjukkan bahwa besarnya tingkat kerentanan yang terjadi pada sistem keamanan informasi dan keamanan[5].

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.

---

[3]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

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

[5]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

Pengaruh serangan siber pada tingkat pusat tentu saja menjadi tolak ukur bagi organisasi pengelola keamanan informasi dan persandian di tingkat daerah. seperti yang disampaikan 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.

Kesadaran keamanan 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, peneliti tertarik untuk memfokuskan penelitian pada Bagaimana Pengelolaan Keamanan Informasi dan Persandian di Diskominfo Provinsi Kalimantan Timur dan Bagaimana Tingkat Keamanan Informasi di Diskominfo Provinsi Kalimantan Timur.

1.3 Penelitian Terdahulu

1. Sayyid Muhammad Thalha Ibrahim (Skripsi, 2020) dari Prodi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" tentang "Evaluasi Keamanan Informasi Pada Diskominfo Kota Depok Menggunakan Indeks KAMI 4.0". Dalam penelitian tersebut bertujuan untuk melakukan evaluasi keamanan informasi menggunakan Indeks KAMI 4.0. Pemberian rekomendasi oleh peneliti didasari dari hasil evaluasi menggunakan Indeks KAMI yang sesuai dengan kelengkapan standar ISO/IEC 27001:2013 dan ISO/IEC 27002:2013 dalam peraktiknya untuk dapat menunjang proses peningkatan keamanan informasi.
2. Aryani C.D Tinungki (Skripsi, 2021) dari Prodi Teknik Informatika, Fakultas Teknik, Universitas Sam Ratulangi tentang "Analisa Tingkat Kematangan Penerapan Keamanan Informasi Pemerintah Kota Bitung Menggunakan Indeks KAMI (Studi Kasus : Diskominfo Kota Bitung). Indeks KAMI 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. Alat evaluasi ini sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi pada pimpinan instansi Terkait.

3. Ilham Bintang, Catur Eri Gunawanm dan Freddy Kurnia Wijaya (Vol. 12 No. 2, tahun 2020) dari Prodi Sistem Informasi, Universitas Islam Negeri Raden Fatah Palembang tentang “Evaluasi Internal Keamanan Informasi Pada Diskominfo Kota Palembang” Dalam penelitian tersebut bertujuan untuk mendeskripsikan kondisi kematangan dalam keamanan informasi pada Diskominfo Palembang secara internal. Instrumen penelitian yang digunakan adalah panduan yang diberikan oleh BSSN yaitu Indeks KAMI versi 3.1. metode yang digunakan pada penelitian ini adalah deskriptif kuantitatif.
4. Hadiati Agus Pratiwi dan Lily Wulandari (Vol. 2 No. 5, tahun 2021) dari Prodi Magister Manajemen Sistem Informasi, Universitas Gunadarma tentang “Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI Versi 4.0 pada Diskominfo Kota Bogor”. Dalam penelitian ini, peneliti membahas tentang tingkat kesiapan keamanan pada Diskominfo Kota Bogor dalam melakukan keamanan informasi dengan menggunakan Indeks KAMI Versi 4.0 yang telah terstandar oleh ISO/IEC 27001:2013 yang dibuat oleh Badan Siber dan Sandi Negara (BSSN).

1.4 Pernyataan Kebaruan Ilmiah

Hubungan penelitian di atas dengan penulis yaitu membahas mengenai evaluasi keamanan dan persandian informasi di instansi daerah dengan menggunakan Indeks KAMI, namun pada penelitian terdahulu menggunakan versi Indeks KAMI 4.0 sebagai alat untuk melakukan penilaian dan evaluasi tingkat kesiapan penerapan keamanan informasi di pemerintah daerah.

Aryani C.D Tinungki meneliti mengenai keamanan dan persandian dalam menjaga kerahasiaan informasi penting negara pada instansi pemerintahan Diskominfo, hal ini menjadi persamaan dalam penulisan yang penulis lakukan dalam penelitian ini yang kemudian menjadi inspirasi dalam penulisan penelitian ini.

Perbedaan yang ada pada 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.

1.5 Tujuan

Menjelaskan dan memahami bagaimana pengelolaan keamanan dan persandian di Diskominfo Provinsi Kalimantan Timur dan Menjelaskan dan memahami tingkat keamanan informasi Diskominfo Provinsi Kalimantan Timur dengan menggunakan Indeks KAMI 4.2 yang diterbitkan oleh BSSN.

II. METODE

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[6] 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).

Teknik analisis data yang penulis terapkan adalah teknik analisis triangulasi yang menggunakan metode induktif, yaitu mencari pemahaman umum tentang masalah utama yang muncul di lapangan. Kegiatan analisis data secara simultan dibagi menjadi tiga alur kegiatan, yaitu reduksi data, penyajian data, dan penarikan kesimpulan/verifikasi.

[6] Amir Hamzah, M. (2019). *Metode Penelitian Kualitatif, Konstruksi Pemikiran Dasar serta Contoh Penerapan Pada Ilmu Pendidikan, Sosial & Humaniora.* Batu: Literasi Nusantara. Hal. 1

III. HASIL DAN PEMBAHASAN

Informasi dan Data yang diperoleh dari wawancara, dokumentasi pendukung berupa Hasil Evaluasi Indeks Keamanan Informasi (KAMI 4.2) serta pengamatan secara langsung pada lokasi penelitian di Diskominfo Provinsi Kalimantan Timur. Untuk mengetahui Pengelolaan Keamanan Informasi dan Persandian di Diskominfo Provinsi Kalimantan Timur dan dari hasil serta teknik yang digunakan oleh penulis dapat diuraikan dalam hasil dan pembahasan sebagai berikut:

3.1 Informan

Penulis dalam penelitian ini menggunakan teknik penentuan informan secara *purposive sampling* dalam teknik wawancara, Sehingga peneliti dapat mempertimbangkan informan mana yang cocok untuk menambahkan data pada fenomena yang sedang diteliti. Berikut daftar infoman dalam penelitian ini:

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

Sumber : Diolah oleh Penulis, 2022

Informan yang dipilih adalah pihak-pihak yang memiliki kaitan langsung serta terlibat pada bidang Pengelolaan Keamanan Informasi dan Persandian, sehingga dipercaya dapat memberikan informasi yang diperlukan kepada peneliti terkait dengan Keamanan Informasi dan Persandian pada Diskominfo Prov. Kaltim.

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

Pada penelitian ini akan dilakukan analisis pengumpulan data menggunakan wawancara yang didasari teori *CIA TRIAD* oleh Whitman[7] 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.

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.

B. Penerapan Enkripsi.

Keterangan yang diberikan oleh Diskomindo 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

[7] M. E. Whitman, H. J. (2018). *Principles of Information Security 6th Edition.* Atlanta: Cengange Learning. Hal. 92

Diskominfo telah menerapkan enkripsi dalam penyimpanan dan pengarsipan data dan informasi sedangkan untuk transfer file antar dinas, enkripsi tidak diperlukan.

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.

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.

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.

H. Perangkat Lunak *Anti-Virus.*

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*).

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

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**. 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*. 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+.

3.4 Kurangnya Tingkat Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika

Berdasarkan ISO/IEC 27001: 2013 sebagai pedoman standar dasar keamanan secara internasional bahwa dari hasil ini menemukan kurangnya tingkat keamanan dasar informasi dan persandian hal ini dengan dibuktikannya hasil evaluasi serta dari kurangnya pemenuhan aspek-aspek pada teori dasar keamanan *CIA TRIAD*. Penelitian ini baru dilakukan tepat pada lokasi penelitian ini dan belum ada penelitian sebelumnya sehingga penelitian ini menjadi dasar pertama sebagai temuan hasil evaluasi kemanan informasi dan persandian di Dinas Komunikasi dan Persandian Provinsi Kalimantan Timur.

IV. KESIMPULAN

Setelah dilakukan tinjauan Dasar Keamanan Informasi dan Persandian serta dengan didukung dengan penilaian dari pihak Badan Siber dan Sandi Negara dapat disimpulkan bahwa Pengelolaan Keamanan Informasi dan Persandian di ruang lingkup Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur masih kurang maksimal, hal ini karena Pengelolaan Keamanan Informasi dan Persandian belum memenuhi semua aspek dari Dasar Keamanan *CIA TRIAD*. Kemudian hal ini juga didukung oleh penilaian oleh BSSN menggunakan alat ukur Indeks KAMI 4.2 yang terstandar ISO/IEC 27001: 2013 dengan hasil Tidak Layak yang berarti masih jauh dari standar internasional dasar manajemen pengelolaan keamanan informasi. **Keterbatasan Penelitian:** Keterbatasan pada penelitian ini adalah kurangnya durasi untuk menggali lebih dalam keadaan di lapangan. **Arah Masa Depan Penelitian *(Future Work)*:** Peneliti menyadari dalam penelitian ini merupakan temuan awal yang dilakukan oelh peneliti sehingga masih perlu diteliti lebih lanjut mengenai keamanan informasi serta kemajuan setelah dilakukan evaluasi oleh karena itu peneliti penyarankan agar dapat dilakukan penelitian lanjutan pada lokasi serupa berkaitan dengan pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur.

V. UCAPAN TERIMAKASIH

Ucapan terima kasih saya sampaikan kepada dosen pembimbing saya Dr. Frans Dione., S.IP, M.SI serta dosen penguji saya yang telah membantu dalam menyempurnakan tulisan saya dan segenap Aparatur Sipil Negara pada Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur yang telah membantu peneliti dalam menyelesaikan skripsi penelitian ini

serta menjadi narasumber dalam yang sangat penting dalam kelanjutan penelitian skripsi ini, Terima Kasih saya ucapkan dan hasil dari penelitian ini merupakan kontribusi saya terhadap lokasi penelitian saya dengan harapan dapat menjadi lebih baik dari sebelumnya.

VI. DAFTAR PUSTAKA

Sari, W. P. (2019). FUNGSI DAN PERAN HUMAS DI LEMBAGA PENDIDIKAN. *Communicology: Jurnal Ilmu Komunikasi*. Hal. 49

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

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

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

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

Amir Hamzah, M. (2019). *Metode Penelitian Kualitatif, Konstruksi Pemikiran Dasar serta Contoh Penerapan Pada Ilmu Pendidikan, Sosial & Humaniora.* Batu: Literasi Nusantara. Hal. 1

M. E. *Whitman*, H. J. (2018). *Principles of Information Security 6th Edition.* Atlanta: Cengange Learning. Hal. 92