BAB I PENDAHULUAN

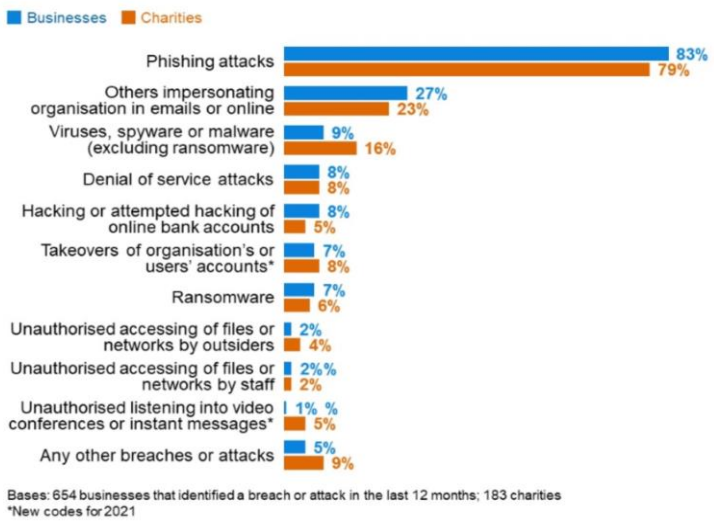
1.1 Latar Belakang

Revolusi Industri 4.0 merupakan suatu era yang mana hampir semua aspek kehidupan memerlukan teknologi dan informasi dalam implementasinya. Menurut (Haag dan Keen,1996) [1] Manusia dalam melakukan pekerjaan dan tugas-tugasnya yang berhubungan dengan informasi atau pesan harus bisa menggunakan teknologi informasi sebagai sarana untuk menunjang pekerjaannya. Oleh sebab itu, teknologi informasi merupakan suatu hal mutlak yang diperlukan dalam menunjang kehidupan manusia di era revolusi industri 4.0 salah satunya berpengaruh di bidang pemerintahan contohnya seperti E-Government (Pemerintahan Elektronik) yang didasarkan pada dasar hukum Perpres No 95 Tahun 2018.

Selain itu juga, ada beberapa peraturan perundang-undangan yang dibuat berkaitan dengan keamanan informasi. contohnya seperti Perpres No 95 Tahun 2018 yang mengatur tentang SPBE (Sistem Pemerintahan Berbasis Elektronik),Peraturan Menteri Komunikasi dan Informatika No 4 Tahun 2016 Pasal 1 Ayat 5 dan 6 yang mana pasal 5 mengatur tentang sistem manajemen pengamanan informasi, dan pasal 6 yang mengatur tentang aspek-aspek keamanan informasi (CIA) dan Peraturan Menteri Komunikasi dan Informatika No 4 Tahun 2016 Pasal 4 tentang Kategorisasi Sistem Elektronik berdasarkan asas risiko. beberapa peraturan ini dikeluarkan untuk mengatur keamanan informasi pada bidang pemerintahan.

Menurut G.J.Sismsons, Keamanan Informasi adalah bagaimana kita dapat mencegah penipuan (cheating) atau paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi,di mana informasinya itu sendiri tidak memiliki arti fisik sehingga rentan terhadap penipuan yang terjadi pada sistem berbasis informasi itu sendiri, sehingga diperlukan manajemen keamanan informasi yang baik untuk mencegah adanya ancaman yang terjadi pada informasi yang dimiliki.

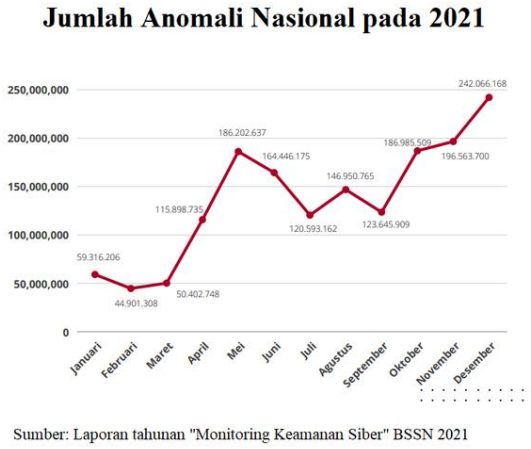
Ancaman Keamanan informasi merupakan suatu kejadian yang bisa merugikan suatu pihak dikarenakan adanya kehilangan data dan informasi yang berharga.ancaman keamanan informasi ini sendiri bisa terjadi di mana saja dan kapan saja baik secara nasional maupun internasional.berikut ini merupakan contoh kasus keamanan informasi yang terjadi di dunia (internasional) dan Indonesia (Nasional).



Gambar 1 Survey Tipe Ancaman Keamanan Informasi Tahun 2021 di Dunia

Sumber : Cyber Security Breaches (2021)

Berdasarkan hasil survei di atas maka bisa dilihat bahwa terjadi banyak serangan yang menyerang keamanan informasi.*Phising attacks* merupakan tipe ancaman yang paling besar persentasenya. selain itu ada juga tipe ancaman seperti *other impersonating organization, virus or malware, hacking, ransomware,* dan lain-lain. tipe ancaman ini bisa terjadi dikarenakan faktor manajemen keamanan informasi yang diterapkan belum berdasarkan dengan standar yang berlaku, sehingga informasi yang dimiliki belum terjamin keamanannya dan bisa mendapatkan ancaman keamanan informasi.



Gambar 2 Hasil Survey Ancaman Keamanan Informasi di Indonesia tahun 2021

Sumber : *Badan Siber dan Sandi Negara (bssn.go.id)*

Selain ancaman yang terjadi di seluruh dunia, Indonesia juga menjadi salah satu Negara

yang tidak terlepas dari ancaman keamanan informasi itu sendiri. oleh sebab itu Pemerintah membentuk sebuah badan yang disebut dengan BSSN (*Badan Siber dan Sandi Negara)* yang merupakan sebuah lembaga yang bergerak di bidang keamanan informasi tentang siber dan persandiaan yang mempunyai tugas pokok untuk mengatur, mengkoordinasikan dan menyelenggarakan pengamanan berita rahasia negara yang dikirim melalui sarana komunikasi antara aparatur negara di seluruh Indonesia. berdasarkan data laporan Tahunan "Monitoring Keamanan Siber" BSSN 2021 di atas bisa dilihat bahwa ancaman keamanan informasi yang terjadi pada bulan Januari – Desember 2021berjumlah 1,6 miliar atau tepatnya 1.637.973.022 anomali trafik atau serangan siber (cyber attack) yang terjadi di seluruh wilayah Indonesia sepanjang tahun 2021.jika dilihat berdasarkan data di atas maka ancaman serangan siber terendah terjadi pada bulan Februari tahun 2021 dengan jumlah 45 juta anomali dan penyimpangan atau ancaman serangan siber terbesar terjadi pada bulan Desember 2021 dengan jumlah lebih dari 242 juta anomali atau penyimpangan dengan jumlah rata-rata ada sekitar 136 juta serangan yang terjadi setiap bulannya.selain menghitung nilai serangan siber, BSSN juga mengonfirmasi bahwa jenis anomali yang menjadi ancaman yakni MyloBot Botnet dengan Jumlah anomali terbanyak yaitu 44,62 persen atau lebih dari 730 juta, selain itu juga ada Protocol-Scada Moxa, MiningPool Win, Trojan, ZeroAccess, dan lain-lain. adapun beberapa kasus serangan siber yang terjadi di Indonesia pada tahun 2021 dan 2022 yakni adanya kebocoran informasi dari data BPJS Kesehatan dan bocornya data Presiden yang diretas oleh pihak yang tidak bertanggung jawab merupakan salah satu bukti bahwa pentingnya membangun sistem keamanan informasi yang baik dan akurat sehingga tidak terjadi insiden keamanan informasi yang dapat merugikan instansi.

Selain itu, ancaman keamanan informasi juga pernah terjadi di Dinas Komunikasi dan Informatika Pemerintah Kota Ambon. dan berdasarkan hasil wawancara yang telah dilakukan, didapatkan bahwa objek penelitian juga pernah mengalami ancaman keamanan informasi seperti *hacking, serverdown* yang terjadi hampir di setiap tahun, upaya pembobolan data instansi oleh pihak yang tidak bertanggung jawab pada tahun 2020 hal ini terjadi karena keamanan fisik yang dimiliki oleh objek penelitian belum optimal.

Berdasarkan data yang ada maka analisis keamanan informasi akan dilakukan untuk mengatasi permasalahan yang terjadi di Dinas Komunikasi dan Informatika Pemerintah Kota

Ambon untuk mengetahui bukti apa saja yang dimiliki oleh objek penelitian serta menganalisis sistem manajemen keamanan informasi menggunakan *gap analysis* dan menentukan *Maturity Level* dari keamanan informasi yang dimiliki untuk digunakan sebagai acuan informasi pada Dinas Komunikasi dan Informatika Kota Ambon sebagai tujuan utama.

1.2 Perumusan Masalah

Berdasarkan Latar Belakang yang ada, maka terdapat beberapa rumusan masalah yang muncul yakni :

1. Dinas Komunikasi dan Informatika Pemerintah Kota Ambon perlu mengetahui temuan atau bukti berdasarkan ISO 27002:2013
2. Dinas Komunikasi dan Informatika Pemerintah Kota Ambon perlu mengetahui *gap dan Maturity Level* agar bisa membuat keamanan informasi sesuai dengan standar ISO 27002:2013
3. Dinas Komunikasi dan Informatika sebagai institusi pelayanan publik perlu diberikan Rekomendasi untuk melindungi keamanan informasi yang dimiliki

1.3 Pertanyaan Penelitian

Sesuai dengan latar belakang dan rumusan masalah yang ada, yang mana berfokus pada keamanan informasi di lingkup Pemerintah Kota Ambon khususnya Dinas Komunikasi dan Informatika, muncul beberapa pertanyaan penelitian , yakni :

1. Apa saja temuan berdasarkan ISO 27002:2013 yang dimiliki oleh Dinas Komunikasi dan Informatika Pemerintah Kota Ambon?
2. Bagaimana *Gap Analisis dan Maturity Level* keamanan informasi yang diterapkan oleh Dinas Komunikasi dan Informatika Pemerintah Kota Ambon?
3. Bagaimana Rekomendasi yang bisa diberikan kepada Dinas Komunikasi dan Informatika Pemerintah Kota Ambon agar bisa melindungi informasi yang dimiliki ?

1.4 Tujuan Penelitian

Beberapa penelitian tujuan, antara lain:

1. Mengetahui temuan penelitan berdasarkan ISO 27002:2013 pada Dinas Komunikasi dan Informatika Pemerintah Kota Ambon

2. Mengetahui *Gap Analisis dan Maturity Level* keamanan informasi yang diterapkan oleh Dinas Komunikasi dan Informatika Pemerintah Kota Ambon
3. Memberikan Rekomendasi yang bisa diberikan kepada Dinas Komunikasi dan Informatika Pemerintah Kota Ambon agar bisa melindungi informasi yang dimiliki.

1.5 Manfaat Penelitian

1.5.1 Aspek Teoritis

Melalui Penelitian ini, diharapkan bisa menjadi bahan pertimbangan dan masukan tentang bagaimana cara untuk menganalisis keamanan informasi pada institusi penyelenggaraan pelayanan publik berdasarkan ISO 27002:2013 selain itu penelitian ini juga bisa melengkapi penelitian-penelitian sebelumnya yang mempunyai rumpun ilmu yang sama yakni mengenai Analisis Manajemen Keamanan Informasi pada Institusi penyelenggara pelayanan publik.

1.5.2 Aspek Praktis

Penelitian ini diharapkan mampu menjadi sumber informasi dan referensi terhadap penerapan Manajemen Keamanan Informasi menggunakan ISO 27002:2013 pada institusi penyelenggara pelayanan publik agar bisa melindungi informasi yang dimiliki dari ancaman serta menjaga informasi yang dimiliki sesuai dengan aspek-aspek keamanan informasi yaitu Kerahasiaan, Ketersediaan dan Integritas**.** Penelitian ini menggambarkan sejauh mana tingkat Keamanan Informasi yang dimiliki oleh Dinas Komunikasi dan Informatika Pemerintah Kota Ambon serta memberikan Rekomendasi keamanan informasi yang bisa dijadikan sebagai referensi.