BAB I
PENDAHULUAN

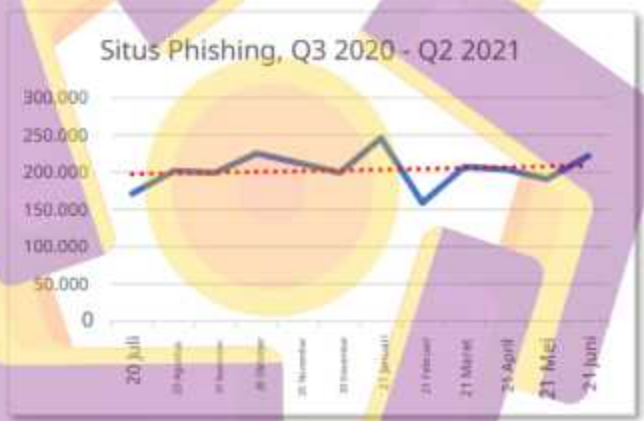
1.1 Latar Belakang

Perkembangan teknologi informasi saat ini mengalami kemajuan yang sangat pesat. Sehingga sangat berdampak terhadap kehidupan manusia. Hampir semua aktivitas yang manusia lakukan berkaitan dengan teknologi. Baik dari kalangan anak – anak hingga orang tua. Tentunya hal ini akan membawa dampak bagi pengguna baik itu negatif maupun positif. Karena semakin canggihnya teknologi maka akan semakin tinggi tingkat resiko kejahatan yang akan diterima. Istilah kejahatan pada dunia maya yang biasa disebut dengan *Cybercrime* ialah salah satu dampak negatif dari kemajuan teknologi. *Cybercrime* merupakan tindak kejahatan pada dunia maya yang memanfaatkan teknologi komputer dan jaringan internet sebagai sarana untuk melakukan aksi kejahatan.

Terdapat tiga hal yang menjadi komponen utama dalam keamanan informasi yaitu : manusia, proses dan teknologi. Ketiga aspek tersebut merupakan satu kesatuan dalam membangun sebuah sistem keamanan jaringan informasi [1]. Seringkali kita hanya memikirkan bahwa *hacker* dapat melakukan tindak kejahatan pada teknologi saja, namun kenyataannya ancaman yang sering diabaikan namun dapat dieksploitasi setiap saat untuk mengambil kesempatan dari adannya kelemahan didalam sebuah jaringan keamanan yaitu pada sisi manusia atau pengguna dari sistem itu sendiri. Serangan tersebut disebut dengan *Social Engineering* atau Rekayasa Sosial. Seperti yang dikemukakan oleh Prof. Richardus Eko Indrajit pada ID-SIRTI dalam keamanan jaringan ada prinsip yang berbunyi "kekuatan sebuah rantai tergantung dari atau terletak pada sambungan yang terlemah" atau dalam bahasa latin yaitu *"the strength of a chain depends on the weakest link"*. Yang menjelaskan bahwa komponen terlemah dalam sebuah sistem jaringan komputer adalah manusia *People is the weakest link* [2]. Teknik dalam melakukan *social engineering* dibagi menjadi dua kategori utama yaitu : teknik berbasis manusia dan teknik berbasis computer [3]. Terdapat beberapa cara untuk dapat mengantisipasi terkena serangan rekayasa sosial salah satunya dapat

memahami setiap serangan yang terjadi dengan memperhatikan keadaan dan pengetahuan terhadap serangan tersebut. Kesadaran keamanan merupakan hal yang penting bagi setiap individu, organisasi, ataupun perusahaan. Dengan menerapkan kesadaran keamanan informasi dapat mengurangi dan mencegah tingkat resiko kegagalan sistem maupun pencurian data yang diakibatkan karena kecerobohan pengguna.

Menurut hasil laporan dari *APWG (Phishing Activity Trends Report Analisys)* melaporkan bahwa setelah kenaikan dua kali lipat pada tahun 2020, jumlah *phishing* tetap berada pada level yang tinggi. Jumlah *phishing* pada Juni 2021 sebanyak 222.127 serangan yang merupakan bulan terburuk ketika dalam sejarah pelaporan APWG [4].



Gambar 1 1 Data jumlah phishing menurut laporan dari APWG

Oleh karena itu pentingnya kesadaran mengenai keamanan informasi bagi individu dalam melindungi data milik pribadi maupun data milik orang lain. Kesadaran keamanan informasi sangat diperlukan bagi petugas vaksin yang biasa bekerja dengan beberapa data penting milik orang lain. Seperti petugas admin pada pelaksanaan vaksin masal yang saat ini sedang banyak diselenggarakan diberbagai daerah. Karena salah satu syarat untuk proses pendaftaran vaksin yaitu dengan melampirkan foto copy kartu tanda penduduk (KTP) atau kartu keluarga (KK). Yang sudah kita ketahui bahwa semba informasi didalam KTP merupakan data-

data pribadi yang sangat penting. Selain itu banyak hal hal teknis yang diperlukan sebagai penunjang untuk dapat melindungi data pasien.

Atas dasar-dasar masalah diatas maka peneliti akan melakukan penelitian yang berjudul ***"Analisa kesadaran keamanan informasi pada petugas vaksin menggunakan metode OCTAVE-S dan FMEA berdasarkan standar ISO 27001:2013".*** Yang bertujuan untuk mengidentifikasi risiko khususnya pada serangan *social engineering* dengan menggunakan metode OCTAVE-S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) serta mengukur tingkat kesadaran keamanan informasi petugas vaksin dalam menjaga keamanan data pasien. Yang menerapkan metode *Failure Mode and Effect Analysis (FMEA)* sesuai standar keamanan ISO/IEC 27001:2013. Standar ISO/IEC 27001:2013 merupakan standar keamanan internasional dalam menetapkan persyaratan untuk penetapan, penerapan, pemeliharaan, dan perbaikan sistem manajemen keamanan informasi [5].

1.2 Perumusan masalah

Berdasarkan latar belakang masalah diatas, dapat dirumuskan sebuah permasalahan yaitu, bagaimana analisa kesadaran keamanan informasi pada petugas vaksin menggunakan metode OCTAVE-S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) dan FMEA *(Failure Mode and Effect Analysis)* berdasarkan standar ISO 27001:2013.

1.3 Tujuan Penelitian

Tujuan dilakukannya penelitian ini yaitu :

1. Untuk mengidentifikasi risiko menggunakan metode OCTAVE-S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) pada pelaksanaan vaksin massal.
2. Untuk menganalisa tingkat kesadaran keamanan informasi pada petugas vaksin dengan menggunakan metode *Failure Mode and Effect Analysis* (FMEA).
3. Untuk mengetahui mitigasi risiko berdasarkan standar ISO/IEC 27001:2013.

1.4 Batasan Masalah

1. Dalam penelitian ini melakukan analisa tingkat kesadaran keamanan informasi pada petugas vaksin massal
2. Dalam melakukan penilaian tingkat kesadaran keamanan informasi pada petugas vaksin massal menggunakan metode *Failure Mode and Effect Analysis* (FMEA)
3. Untuk mengidentifikasi risiko pada pelaksanaan vaksin massal menggunakan metode OCTAVE-S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*)
4. Objek penelitian meliputi petugas vaksin pada bagian admin pemrosesan data pasien, petugas dari Dinas Kesehatan dan petugas dari Dinas Komunikasi dan Informatika Kabupaten Sleman
5. Pada penelitian ini menggunakan metode kualitatif dengan mengajukan wawancara dan kuesioner
6. Dalam proses pengumpulan data menggunakan metode kuesioner terhadap 33 responden, melakukan wawancara dengan pihak Dinas Kesehatan dan Dinas Komunikasi dan Informatika Kabupaten Sleman serta melakukan observasi secara langsung pada proses pelaksanaan vaksin massal.
7. ISO/IEC 27001:2013 digunakan untuk memberikan langkah mitigasi pada risiko yang ada saat proses pelaksanaan vaksin massal

1.5 Manfaat Penelitian

Terselesainya laporan ini maka diharapkan dapat bermanfaat sebagai berikut :

1. Dapat memberikan gambaran apa itu *social engineering* dan beberapa jenis ancamannya, *security awareness*, metode OCTAVE-S, FMEA, ISO/IEC 27001:2013 bagi pembaca yang belum mengetahui akan hal tersebut.
2. Dapat mengetahui kemungkinan risiko yang akan terjadi pada proses pelaksanaan vaksin massal.
3. Memberikan gambaran bagi peneliti selanjutnya dalam penggunaan metode OCTAVE-S, FMEA dan gambaran mitigasi berdasarkan ISO/IEC 27001:2013.