BAB 1
PENDAHULUAN

1.1. Latar Belakang

Pada era digital ini pertukaran informasi merupakan proses utama dalam penggunaan teknologi setiap harinya [1]. Hal ini sejalan dengan peningkatan produksi informasi yang mengharuskan adanya komunikasi aman dan perlindungan data, seiring dengan perkembangan itu tingkat ancaman digital juga semakin canggih dan berisiko kerentanan pada data. Jika keamanan sistem informasi tidak terjaga dengan baik, beberapa risiko akan muncul dan menjadi penghalang pada organisasi dalam mencapai tujuannya, hal itu juga dapat menyebabkan beberapa masalah muncul seperti kerugian materil, pelanggaran hukum, dan rusaknya integritas yang sudah terbangun dengan baik [2]. Oleh karena itu, perlindungan keamanan informasi merupakan suatu hal mutlak yang harus dihadapi serius oleh seluruh anggota pada organisasi tersebut. Dengan adanya keselamatan dan keamanan pada lingkungan di mana informasi tersebut berada, integritas, ketersediaan, dan kerahasiaan informasi di perusahaan pasti akan terjamin [3].

Kasus yang berkaitan dengan efek negatif dari kurangnya kesadaran akan keamanan dan privasi sudah marak terjadi, termasuk di Indonesia. Hal ini disebabkan oleh fakta bahwa orang tidak sadar akan keamanan dan privasi mereka saat mendapatkan pesan dari orang yang tidak dikenal dan menerima tautan palsu yang mengarah ke situs web yang dibuat dengan tujuan membuat perangkat korban terkena serangan malware, yang mengambil data secara ilegal dan menyebabkan kerusakan internal pada perangkat korban [4]. Serangan siber tidak hanya terjadi pada masyarakat awam. Pada 20 Juni 2024, masyarakat Indonesia digegerkan mengenai insiden Pusat Data Nasional (PDN) mengalami serangan siber yang mengakibatkan kebocoran data**,** dan 282 layanan yang dijalankan instansi pemerintahan, baik untuk urusan internal ataupun layanan masyarakat tidak dapat digunakan [5]. Faktor yang memengaruhi terjadinya insiden ini adalah infeksi ransomware yang terjadi di pusat data nasional, ketika perangkat telah terinfeksi ransomware *hacker* sebagai pelaku utama pada kasus ini "menyandera" data-data penting negara dengan tebusan sebesar 8 juta dollar Amerika atau sekitar 131 milliar rupiah untuk memberikan akses kembali kepada data-data yang telah diambil. Pada kasus ini perangkat dapat terinfeksi ransomware tentu diakibatkan karena kelalaian oknum, kelalaian tersebut dapat terjadi diantaranya dengan cara membuka link yang mencurigakan, membuka *website* yang tidak terpercaya, jarang melakukan backup data-data. Hal ini merupakan salah satu contoh dari dampak rendahnya tingkat kesadaran keamanan informasi pada anggota organisasi, terlebih

instansi ini seharusnya memiliki kesadaran keamanan informasi yang tinggi karena menyangkut data-data penting dan sangat rahasia yang dimiliki oleh negara.

Universitas Telkom mengakui pentingnya keamanan data dalam era digital yang semakin kompleks dan rentan terhadap berbagai ancaman keamanan informasi. Dalam upaya untuk memastikan perlindungan data yang efektif dan aman, Universitas Telkom telah menerapkan berbagai kebijakan keamanan informasi sebagai contoh penggunaan autentikasi 2 faktor dalam proses login aplikasi, penggunaan *email Single Signed On* (SSO), penggunaan *ID card* yang terintegrasi dengan *RFID*, dan mengingatkan para mahasiswa mengenai keamanan informasi melalui email. Pada Universitas Telkom Bandung seluruh data mengenai sistem informasi dan keamanannya berpusat di Direktorat Pusat Teknologi Informasi (PUTI). PUTI adalah departemen yang bertanggung jawab untuk mengembangankan sistem dan teknologi informasi, mengelola serta mengembangkan infrastruktur dan keamanan teknologi informasi, serta mengorganisir dan memeriksa proses pengelolaan standar mutu teknologi informasi bagi mahasiswa Universitas Telkom.

Direktorat PUTI Universitas Telkom memiliki permasalahan mengenai tingkat kesadaran para mahasiswa terhadap manajemen keamanan informasi, menurut PUTI tingkat kesadaran mahasiswa terhadap manajemen keamanan informasi masih rendah. PUTI memiliki sistem yang dapat mendeteksi perangkat mahasiswa yang sedang menggunakan akun SSO Universitas Telkom, pada sistem tersebut terdeteksi bahwa sebagian besar perangkat pernah, dan sedang terjangkit *malware*. Hal tersebut diduga karena mahasiwa mengakses dan mengunduh file atau aplikasi yang berbahaya dari sumber asing dan tidak tepercaya. Selain itu PUTI selama ini sering berfokus dalam kesadaran keamanan informasi pada karyawannya, hal itu dilakukan untuk memastikan bahwa staff yang menjaga keamanan informasi mahasiswa dan civitas akademik di Telkom memiliki pemahaman yang tinggi dan mendetail mengenai pekerjaannya. Selama ini PUTI belum melaksanakan pengukuran tingkat kesadaran keamanan informasi pada Mahasiswa di Universitas Telkom, hal ini juga yang mendasari penulis untuk melaksanakan penelitian tentang pengukuran tingkat kesadaran keamanan informasi mahasiswa di Universitas Telkom. Harapannya penelitian ini akan membantu PUTI dalam mengetahui seberapa besar atau rendahnya tingkat kesadaran keamanan informasi pada mahasiswa di Universitas Telkom. Mahasiswa di Universitas Telkom, memiliki peran penting dalam menjaga keamanan informasi di lingkungan kampus. Sangat penting bagi mahasiswa untuk memahami keamanan informasi mereka karena kesadaran yang tinggi dapat membantu mencegah ancaman keamanan seperti kebocoran data dan serangan siber yang digunakan untuk melaporkan.Oleh karena itu, untuk menghadapi permasalahan tersebut, pada penelitian ini akan dilakukan pengukuran tingkat kesadaran keamanan informasi pada mahasiswa Universitas Telkom menggunakan instrumen Human Aspect of

Information Security Questionnaire (HAIS-Q). Tujuannya untuk mengevaluasi sejauh mana pemahaman dan kesadaran mahasiswa terhadap risiko keamanan informasi, dengan harapan dapat mengidentifikasi area yang perlu mendapat perbaikan. Dengan demikian, hasil dari penelitian ini diharapkan dapat memberikan wawasan yang lebih mendalam tentang aspek-aspek kritis yang mempengaruhi kesadaran keamanan informasi, sehingga langkah-langkah strategis dan efektif dapat diambil untuk meningkatkan keamanan informasi di Universitas Telkom.

Penelitian ini dilaksanakan di Universitas Telkom tepatnya pada Fakultas Informatika, karena Universitas Telkom merupakan perguruan tinggi swasta terbaik pertama menurut Webometrics perbulan Juli tahun 2024 [6], Universitas Telkom juga memiliki infrastruktur teknologi yang modern dan mumpuni untuk mendukung proses pembelajaran di lingkungan kampus [7]. Fakultas Informatika dipilih menjadi tempat penelitian, karena fakultas ini memiliki fokus yang kuat pada bidang teknologi informasi. Mahasiswa Fakultas Informatika terlibat langsung dengan teknologi serta memiliki mata kuliah yang berisiko mengalami serangan siber. Sangat penting bagi mahasiswa di fakultas informatika untuk memiliki kesadaran keamanan informasi yang kuat agar dapat melindungi data pribadi, maka dari itu diperlukan adanya pengukuran tingkat kesadaran terhadap keamanan informasi.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang disajikan, terdapat permasalahan utama yang perlu diidentifikasi dan diselesaikan dalam proses penelitian ini. Permasalahan yang harus diidentifikasi yaitu:

1. Bagaimana tingkat kesadaran keamanan informasi pada mahasiswa berdasarkan pengukuran menggunakan *HAIS-Q* di Universitas Telkom Bandung?
2. Bagaimana cara untuk mengukur tingkat kesadaran keamanan informasi mahasiswa fakultas informatika di Universitas Telkom Bandung.
3. Bagaimana cara untuk meningkatkan kesadaran keamanan informasi para mahasiswa di Universitas Telkom Bandung berdasarkan pendapat ahli?

1.3. Tujuan

Berdasarkan rumusan masalah diatas, penelitian ini memiliki tujuan yaitu:

1. Mengukur tingkat kesadaran keamanan informasi para mahasiswa di Universitas Telkom Bandung menggunakan *HAIS-Q*.
2. Memahami tingkat kesadaran keamanan informasi di kalangan mahasiswa.
3. Mengembangkan instrumen penelitian yang valid dan reliabel.
4. Mengumpulkan data yang akurat dan komprehensif berdasarkan kuisioner dan wawancara terhadap mahasiswa dan ahli.
5. Menganalisis data untuk mendapatkan temuan pada tingkat kesadaran keamanan informasi yang rendah.
6. Menjabarkan saran dan pendapat dari ahli yang bermanfaat untuk peningkatan kesadaran keamanan informasi mahasiswa di Universitas Telkom.

1.4. Batasan Masalah

Dari masalah yang telah diidentifikasi dalam penelitian ini, penulis memutuskan untuk membatasi responden dalam proses pengumpulan data hanya kepada mahasiswa/i S1 Fakultas Informatika Universitas Telkom. Fakultas Informatika dipilih menjadi tempat penelitian, karena fakultas ini memiliki fokus yang kuat pada bidang teknologi informasi. Mahasiswa Fakultas Informatika terlibat langsung dengan teknologi serta memiliki mata kuliah yang berisiko mengalami serangan siber seperti keamanan sistem, jaringan komputer, forensik komputer dll. Sangat penting bagi mahasiswa di fakultas informatika untuk memiliki kesadaran keamanan informasi yang kuat agar dapat melindungi data pribadi, dan menghindari resiko-resiko IT yang dapat mengancam dirinya maka dari itu diperlukan adanya pengukuran tingkat kesadaran terhadap keamanan informasi.

1.5. Rencana Kegiatan

Pada tahapan awal adalah melakukan studi literatur terhadap jurnal-jurnal yang berkaitan dengan topik penelitian ini, tujuannya untuk membantu mengetahui teori-teori dan teknis pada penelitian sebelumnya. Setelah memahami dasar, teori dan teknis dalam melakukan penelitian, selanjutnya menentukan ruang lingkup dan batasan masalah dalam penelitian ini. Selanjutnya memahami dan merumuskan pertanyaan kuisioner/wawancara, teknik pengumpulan data, dan responden yang akan digunakan saat melaksanakan proses pengumpulan data. Ketika pertanyaan kuisioner telah dirumuskan maka penulis akan melakukan *Pilot Study* dengan menyebar kuisioner dan melakukan uji reliabilitas dan validitas dari kuisioner untuk mengetahui apakah instrumen penelitian yang berupa kuisioner memiliki tingkat reliabilitas dan validitas yang cukup sebelum disebarkan ke sampel sesungguhnya. Setelah merencanakan instrumen penelitian dan melaksanakan *pilot study,* barulah dilakukan pengumpulan data kuantitatif dan kualitatif sesuai dengan metode *Human Aspect of Information Security Questionaire (HAIS-Q)*. Setelah terkumpul, data diolah untuk mendapatkan hasil akhir dari penelitian. Setelah mendapatkan hasil dari penelitian kuantitatif, selanjutnya dilaksanakan penelitian kualitatif dengan cara wawancara kepada mahasiswa untuk mengetahui lebih dalam tingkat pemahamannya, kemudian dilanjut dengan wawancara dengan ahli untuk mendapatkan saran dan rekomendasi untuk peningkatan kesadaran keamanan informasinya. Setelah itu langkah terakhir adalah memberikan rekomendasi dan saran kepada Direktorat Pusat Teknologi Informasi (PUTI), sesuai dengan hasil yang diperoleh untuk pengembangan dalam meningkatkan tingkat kesadaran tentang keamanan informasi di lingkungan Universitas Telkom.