BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi telah berkembang pesat dan memainkan peran penting dalam berbagai aspek kehidupan manusia. Ini mencakup penerapan pengetahuan dan keterampilan untuk mengatasi masalah serta meningkatkan kualitas kehidupan. Teknologi melibatkan penggunaan pengetahuan, keterampilan, alat, dan sistem untuk menciptakan solusi efisien bagi berbagai masalah.

Menurut Subitmele (2023), Teknologi sudah ada saat masa prasejarah, dimana manusia pertama menemukan batu dan kayu untuk kebutuhan sehari-harinya, seperti memotong, memalu, dan membuat api. Namun pada abad ke-20, teknologi komputer sudah mulai tercipta. Penemuan teknologi komputer inilah yang menciptakan kemajuan di dunia sampai sekarang.

Pada zaman sekarang, teknologi sudah menjadi kebutuhan utama yang harus dimiliki setiap manusia. Peran dari teknologi ini sudah dipergunakan di kegiatan sehari-hari manusia, seperti berbelanja, bepergian, belajar, dan lain-lain. Perkembangan teknologi ini membuat orang-orang mulai menggunakan setiap teknologi yang sesuai dengan kebutuhan mereka masing-masing.

Menurut penjelasan dari Salim (2022), ada berbagai manfaat yang dimiliki oleh teknologi, seperti mengakses informasi yang dibutuhkan para pelajar atau orang yang ingin mempelajari sesuatu, menciptakan jenis pekerjaan baru yang berhubungan dengan teknologi yang ada, menghemat waktu, menciptakan hiburan, menjadi alat komunikasi, globalisasi, dan menciptakan transaksi yang lebih mudah.

Salah satu manfaat teknologi yang sampai sekarang masih dirasakan oleh banyak orang adalah sebagai tempat penyimpanan data-data penting, dan mengembangkan kegiatan bisnis yang mudah dan nyaman. Penyimpanan data penting merupakan kegiatan yang dilakukan hampir di setiap perusahaan sebagai pengganti penyimpanan data secara konvensional. Data tersebut tidak hanya dokumen saja, melainkan semua yang berhubungan dengan kepentingan dari orang tersebut.

Dalam kegiatan bisnis, teknologi merupakan hal yang sampai sekarang masih dirasakan oleh banyak orang. Dimulai dari berbelanja sampai bepergian, banyak perusahaan menciptakan kegiatan bisnis dari hal tersebut, seperti Gojek, Astro, Grab, dan lain-lain. Di dunia luar, semua orang sudah menggunakan teknologi sebagai kebutuhannya, dari membayar belanjaan, membayar jalan tol, dan berbelanja barang-barang keperluan.

Meskipun membawa kemajuan besar di masa sekarang, teknologi juga memiliki masalah. Masalah ini tidak hanya menyerang teknologi, tetapi bisa mengganggu kegiatan orang-orang yang biasa menggunakan teknologi tersebut. Hal yang umum menjadi masalah dalam teknologi adalah kejahatan siber.

Kejahatan siber adalah sebuah kejahatan yang sering terjadi di dunia maya. Kejahatan ini biasanya melakukan sebuah pencurian data penting, memberikan virus, atau meneror seseorang untuk membayar uang agar data-data penting tidak dihapus oleh si penjahat. Kejahatan siber tersebut tidak hanya merugikan seseorang saja, perusahaan bisa menjadi korban dari kejahatan jika keamanan dari teknologi yang dimiliki perusahaan masih lemah.

Kejahatan siber ini tidak hanya terjadi sekarang. Pada tahun 1834, terjadi pencurian sistem telegram di Prancis. Hal tersebut membuat pelaku bisa mengakses market milik Prancis dan mencuri datanya. Kemudian pada tahun 1876, dimana telefon pertama kali diciptakan, sudah terkenal dengan hal yang bernama *phone hacking*.

Kejahatan siber ini bukanlah cuma kejahatan kecil, banyak kerugian yang terjadi akibat dari kejahatan siber tersebut. Salah satu yang cukup terkenal adalah kasusnya *ransomware*. *Ransomware* adalah sebuah serangan dimana pelaku kejahatan meneror pengguna dengan cara memasukkan virus atau melakukan *hacking* ke dalam teknologi pengguna. Setelah itu, pelaku akan meminta uang dari korban. Jika tidak diberikan uang sesuai dengan keinginan pelaku, pelaku dapat menghapus atau mencuri data penting milik pengguna.

Untuk perusahaan yang bekerja di bidang perbisnisan, kejahatan siber ini merupakan kejahatan yang sangat diperhatikan oleh mereka. Hal ini karena kejahatan tersebut dapat mengganggu kegiatan perbisnisan perusahaan, salah satunya adalah pencurian data pribadi milik orang yang bekerja sama dengan perusahaan tersebut. Ketika data tersebut sudah tercuri, data tersebut bisa diperjual-belikan. Hal tersebut akan membuat pengguna merasa tidak nyaman dengan perusahaan tersebut dan memutus mitra kerja dengannya.

Untuk menghindari kejahatan siber, beberapa perusahaan mulai mencari cara untuk menghindari kerugian tersebut. Namun pelaku masih bisa menyerang mereka. Hingga akhirnya muncullah ide untuk menciptakan sebuah keamanan yang berfungsi sebagai penangkal kejahatan-kejahatan siber. Hal itu mulai dikenal dengan keamanan siber.

Menurut Shea (2023), Keamanan siber adalah sebuah sistem pelindung yang terhubung ke internet yang berfungsi sebagai pelindung perangkat yang digunakan oleh pengguna dari serangan-serangan siber. Keamanan siber ini tidak hanya digunakan oleh perusahaan saja, semua orang yang memiliki perangkat juga menggunakan keamanan tersebut.

Keamanan siber adalah serangkaian tindakan untuk melindungi komputer, jaringan, dan data

dari akses ilegal. Ini sangat penting karena hampir semua aktivitas saat ini terhubung secara digital, termasuk berbelanja online, memesan makanan, dan menggunakan transportasi. Prinsip dasar dalam keamanan siber adalah Triad CIA: kerahasiaan, integritas, dan ketersediaan informasi. Kerahasiaan melibatkan pembatasan akses ke data sensitif, integritas menjaga keaslian data, dan ketersediaan memastikan akses sistem selalu tersedia.

Ada berbagai jenis keamanan siber, termasuk cloud security untuk melindungi data di cloud, network security untuk menjaga jaringan komputer, dan application security untuk mengamankan aplikasi. Ancaman utama dalam keamanan siber meliputi cyber crime, cyber attack, dan cyber terrorism. Cyber crime melibatkan tindakan ilegal dalam sistem komputer tanpa target tertentu, sementara cyber attack adalah serangan dengan tujuan politik tertentu. Ancaman terparah adalah cyber terrorism, yang bertujuan menciptakan ketakutan melalui sistem komputer.

Ancaman siber juga melibatkan berbagai jenis malware seperti virus, Trojan, spyware, ransomware, adware, dan botnet. Selain itu, ada injeksi SQL, phishing, rootkit, dan serangan Denial-of-Service (DoS). Memahami ancaman siber ini penting dan memerlukan praktik keamanan yang ketat untuk melindungi diri dari serangan cyber yang merugikan.

Ancaman siber ini juga bisa menyerang di institusi. Institusi juga bisa menjadi target untuk penyerangan di dunia maya. Hal ini karena ada beberapa institusi yang menggunakan *website* atau aplikasi khusus milik institusi. Jika di institusi terkena serangan siber, hal ini bisa mengganggu kegiatan perkuliahan dan bisa mengurangi kualitas institusi.

Sayangnya, banyak institusi yang kurang memahami betapa pentingnya keamanan siber tersebut terhadap keadaan sekarang, dimana serangan siber sudah berada di sekitar mereka.

Dari identifikasi masalah yang didapatkan, maka rumusan masalah yang akan dibahas pada skripsi ini yaitu: “Bagaimana Cara Penerapan *Framework NIST Cyber Security* di Institusi XYZ.”

1.2 Identifikasi dan Rumusan Masalah

Berdasarkan latar belakang yang sudah dijelaskan, peneliti bisa mengidentifikasikan masalah-masalah yang ada, yaitu:

a. Rendahnya kesadaran civitas akademika terkait bahaya ancaman siber dan pentingnya keamanan TI.
b. Belum adanya kebijakan yang tegas dan ketat terkait keamanan siber di Institusi XYZ.
c. Belum diterapkannya suatu *framework* keamanan siber di Institusi XYZ.
d. Penyebaran ancaman siber yang meliputi *malware* yang didalamnya ada virus,

trojan, spyware, ransomware, adware, botnet, rootkits masih menjadi ancaman serius yang dapat menginfeksi sistem, mengenkripsi data, dan mengganggu operasional Institusi XYZ.

e. Ancaman *spoofing* serta *phising* melalui email tetap menjadi masalah, dengan banyak pengguna yang dapat terjebak dalam skema penipuan ini sehingga perlu adanya perlindungan email yang ketat dan ampuh.

Masalah-masalah yang sudah diidentifikasi ini, peneliti dapat membuat rumusan masalah sebagai berikut:

a. Bagaimana cara meningkatkan kesadaran civitas akademika terkait dengan bahaya ancaman siber dan pentingnya keamanan TI?
b. Kebijakan apa saja yang diperlukan Institusi XYZ terkait keamanan siber?
c. Bagaimana cara menerapkan *framework* untuk keamanan siber di Institusi XYZ

1.3 Ruang Lingkup dan Batasan Masalah

Berdasarkan identifikasi masalah berikut adalah ruang lingkup dan batasan masalah yang dapat dirangkum:

1. Penelitian ini dilakukan pada Institusi XYZ.
2. Penelitian dilakukan dengan menggunakan metode Framework NIST Cyber Security.
3. Objek penelitian ini adalah kesadaran civitas akademika Institusi XYZ mengenai keamanan siber. Penelitian ini juga memetakan penggunaan tools keamanan siber, serta perlindungan dari berbagai jenis serangan siber. Secara spesifik, penelitian ini menganalisis:

Kesadaran mengenai keamanan siber, pemetaan tools keamanan siber, perlindungan dari serangan jaringan seperti botnet dan sniffing, perlindungan dari serangan endpoint seperti malware dan ransomware, perlindungan dari serangan aplikasi seperti SQL injection, backdoor, dan deface, perlindungan dari serangan email seperti spoofing dan phishing. Dengan demikian, penelitian ini mencakup aspek kesadaran, perencanaan, tools, dan perlindungan terhadap beragam jenis serangan siber di Institusi XYZ.

1.4 Tujuan Penelitian

Tujuan dari penelitian yang dilakukan Peneliti adalah:

a. Melakukan analisis terhadap keamanan siber menggunakan *Framework NIST Cyber Security.*
b. Dilakukannya penerapan *Framework NIST Cyber Security* pada Institusi XYZ.

Agar terwujudnya peningkatan kesadaran civitas akademika mengenai keamanan siber, pengoptimalan terhadap tools-tools keamanan siber yang digunakan keamanan siber dari hasil analisis sehingga keamanan siber di Institusi XYZ menjadi optimal.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat untuk penulis dan pihak-pihak terkait lainnya. Manfaat yang diharapkan yaitu :

A. Bagi Penulis

Sebagai sarana agar mampu menerapkan ilmu pengetahuan yang didapat selama studi. Terutama pada bidang keahlian dalam melakukan analisis, terutama pada keamanan siber.

B. Bagi Pembaca

1.4.1.1 Sebagai sarana referensi wawasan dalam melakukan analisa terutama di bidang keamanan siber dengan metode *Framework NIST Cyber Security.*

1.4.1.2 Dapat mengembangkan sebuah keamanan teknologi yang kuat dan bisa diimplementasikan ke teknologi lain.

C. Bagi Pihak Terkait

Dari solusi optimalisasi berdasarkan hasil analisa yang telah dilakukan di dapat membantu pihak institusi dalam melakukan optimalisasi keamanan siber sehingga keamanan siber menjadi optimal dan semakin aman.

1.6 Sistematika Penulisan

Susunan atau sistematika penulisan Skripsi ini terbagi menjadi 5 (lima) bab, berikut ini uraian pada setiap bab, diantaranya:

BAB I PENDAHULUAN

Pada bab ini terdapat beberapa pembahasan yaitu tentang, latar belakang, identifikasi dan rumusan masalah, lalu maksud dan tujuan penelitian, manfaat penelitian, dan juga susunan atau sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini terdapat beberapa pembahasan yaitu tentang tinjauan studi. Pada tinjauan studi berisikan tentang pengertian yang digunakan dan dikutip dari beberapa buku dan jurnal yang memiliki keterkaitan dengan penelititan tersebut.

BAB III METODE PENELITIAN

Pada bab ini pembahasan berisikan tentang analisa keamanan siber yang sedang berjalan. Hal yang dianalisa antara lain kesadaran civitas akademika mengenai keamanan siber, disaster recovery plan, pemetaan teerhadap tools-tools keamanan siber yang digunakan,

serangan malware dan serangan ransomware, dan serangan terhadap email Institusi XYZ.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini pembahasan berisikan tentang estimasi biaya yang digunakan dalam melakukan kegiatan penelitian serta jadwal kegiatan penelitian dalam bentuk bar chart.

BAB V KESIMPULAN DAN SARAN

Pada bab ini pembahasan berisikan tentang kesimpulan dan juga saran mengenai penelitian yang dilakukan dan untuk pengembangan lebih lanjut.

DAFTAR PUSTAKA

Pada bab ini pembahasan berisikan tentang referensi yang dikutip dan digunakan pada penelitian ini guna membantu pengembangan aplikasi dan penulisan Laporan Tugas Akhir.