BAB I
PENDAHULUAN

1.1 Latar Belakang

Perubahan lanskap teknologi informasi mengacu pada perkembangan dan transformasi yang sangat cepat dalam teknologi digital, terutama di bidang informasi dan komunikasi. Perubahan ini melibatkan kemajuan teknologi seperti internet, komputasi awan, big data, serta perangkat lunak dan perangkat keras yang semakin canggih. Dampak dari perubahan ini tidak hanya dirasakan oleh sektor bisnis atau industri, tetapi juga merambah ke berbagai organisasi. (Smith & Johnson, 2022)

Teknologi informasi yang berkembang dengan dinamis kini mencakup berbagai aspek kehidupan manusia, termasuk bidang pendidikan tinggi. Dalam dunia pendidikan yang semakin berkembang, teknologi informasi memegang peran krusial, khususnya di lingkungan kampus atau perguruan tinggi. Perguruan tinggi menggunakan teknologi informasi sebagai sarana penunjang demi tercapainya berbagai tujuan institusi. Namun, pemanfaatan teknologi informasi hanya akan optimal jika didukung oleh tata kelola yang efektif. Tata kelola tersebut memungkinkan institusi pendidikan tinggi untuk mengurangi risiko terkait ancaman keamanan siber maupun potensi kehilangan data yang dapat mengganggu kelancaran operasional sistem informasi kampus.(Handoyo, 2020).

Mengurangi resiko ancaman siber perlu tata kelola yang baik, ancaman siber juga telah menjadi perhatian utama bagi berbagai sektor. Pada satu tahun terakhir tepatnya di bulan Juni 2024 terjadi insiden peretasan yang menimpa Pusat Data Nasional (PDN) yang mengakibatkan lumpuhnya layanan publik dan terekspos nya data sensitif. Kasus tersebut menjadi urgensi untuk menanggulangi serangan siber yang dapat berakibat fatal (Tempo.co, 2024). Peretasan tersebut merupakan ransomware jenis *"Brain Chiper"*. Pelaku menuntut tebusan sebesar USD 8 juta atau sekitar 131 miliar rupiah untuk memulihkannya. Penyebab terjadinya peretasan tersebut adalah Fitur Windows Defender pada data center yang dinonaktifkan, Keamanan sistem yang sangat rentan terhadap serangan siber, serta kelemahan sistem keamanan yang digunakan oleh kominfo atau pihak ketiga yang mengolah data.(Wahyu dkk, 2024).

Beberapa tahun terakhir, sektor pendidikan tinggi menjadi salah satu target utama serangan siber, terutama ransomware. Berdasarkan laporan Malwarebytes yang dirilis pada awal 2024, tercatat bahwa sepanjang tahun 2023 terjadi peningkatan sebesar *70%* dalam jumlah serangan ransomware yang menarget institusi pendidikan tinggi dibandingkan tahun sebelumnya. Lebih jauh, jika mencakup seluruh sektor pendidikan, termasuk pendidikan dasar dan menengah, peningkatannya mencapai *105%,* dari 129 insiden pada 2022 menjadi 265 insiden pada 2023 (Kuykendall, 2024). Laporan tersebut menunjukkan bahwa sektor pendidikan menjadi sasaran empuk karena kombinasi antara lemahnya sistem pertahanan siber, banyaknya perangkat yang terhubung dalam jaringan kampus, dan keterbatasan sumber daya TI untuk mendeteksi serta merespons ancaman secara cepat. Hal ini menjadi peringatan penting bagi institusi pendidikan tinggi, termasuk di Indonesia, untuk meningkatkan kesiapan menghadapi ancaman siber yang semakin kompleks (Kuykendall, 2024).

Keamanan siber menjadi isu yang sangat penting karena ancaman terhadap sistem informasi semakin kompleks dan beragam. Ancaman siber bisa melalui seperti peretasan, malware, dan serangan phishing Jika tidak ditangani dengan baik, ancaman tersebut dapat mengakibatkan kebocoran data pribadi mahasiswa dan dosen, gangguan pada sistem akademik, hingga kerugian finansial. Universitas Muhammadiyah Lamongan, sebagai salah satu institusi pendidikan tinggi yang memanfaatkan teknologi informasi dalam operasionalnya, tidak terlepas dari risiko-risiko tersebut. Oleh karena itu, diperlukan langkah-langkah strategis untuk mengidentifikasi dan mengelola risiko keamanan siber guna melindungi data dan sistem informasi kampus.(Mahendra & Pinatih, 2021).

Perguruan tinggi Universitas Muhammadiyah Lamonagan, salah satu Universitas yang berada di Kabupaten Lamongan tentunya mempunyai ribuan data penting, dengan begitu tentunya keamanan data dan sistem informasi menjadi prioritas utama untuk memastikan keberlangsungan operasional serta menjaga kepercayaan civitas akademika.(Hendra & Budhy, 2021). Data yang dikelola oleh Universitas Muhammadiyah Lamongan meliputi data mahasiswa, dosen, staf, keuangan, akademik, hingga penelitian. Jika data ini jatuh ke tangan yang tidak bertanggung jawab atau sistem informasi terganggu, dampaknya tidak hanya

merugikan kampus tetapi juga individu terkait.(Intan Mafiana dkk, 2023). Universitas Muhammadiyah Lamongan sebagai studi kasus dalam penelitian ini didasarkan pada urgensi dan pentingnya pengelolaan keamanan siber di lingkungan pendidikan tinggi.

Kerangka kerja yang diakui secara luas untuk penilaian risiko keamanan siber adalah *NIST Cybersecurity Framework (CSF)* yang dikembangkan oleh *National Institute of Standards and Technology (NIST)*. *NIST Cybersecurity Framework (CSF)* menyediakan pendekatan berbasis risiko yang membantu organisasi dalam mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan diri dari insiden keamanan siber. Implementasi *NIST CSF* memungkinkan institusi pendidikan tinggi untuk melakukan penilaian risiko secara komprehensif dan sistematis. Sebagai contoh, penelitian yang dilakukan oleh Handoyo dan Nigrum (2024) di sebuah universitas menunjukkan bahwa penerapan *NIST CSF* membantu dalam mengidentifikasi kelemahan keamanan dan memberikan rekomendasi perbaikan yang spesifik (Handoyo & Nigrum, 2024).

Penelitian ini bertujuan untuk melakukan penilaian risiko keamanan siber di Universitas Muhammadiyah Lamongan dengan menggunakan *NIST Cybersecurity Framework* (CSF) versi 2.0 sebagai panduan utama. Penilaian risiko yang dimaksud dalam penelitian ini mencakup proses identifikasi, analisis, dan evaluasi terhadap potensi ancaman dan kerentanan yang dapat memengaruhi sistem informasi kampus. Melalui pendekatan ini, penelitian menilai sejauh mana kapabilitas keamanan siber saat ini telah memenuhi praktik terbaik yang direkomendasikan oleh *NIST*. Framework *NIST CSF* 2.0 menawarkan pendekatan sistematis dan terstruktur melalui enam fungsi inti: *Identify, Protect, Detect, Respond, Recover,* dan *Govern,* yang masing-masing membantu organisasi dalam memahami risiko, membangun kontrol perlindungan, mendeteksi insiden, merespons kejadian, memulihkan layanan, serta memastikan tata kelola yang baik. Versi terbaru ini lebih fleksibel untuk diterapkan di berbagai sektor, termasuk institusi pendidikan tinggi, dan menekankan pentingnya tata kelola serta pengukuran kinerja keamanan siber secara berkelanjutan (NIST, 2024).

1.2 Rumusan Masalah

1. Bagaimana mengimplementasikan *NIST Cybersecurity Framework 2.0* di Universitas Muhammadiyah Lamongan ?
2. Bagaimana menilai tingkat risiko keamanan siber Universitas Muhammadiyah Lamongan dengan standart *NIST Cybersecurity Framework 2.0* ?
3. Apa saja rekomendasi yang diberikan terkait keamanan siber kampus menggunakan *NIST Cybersecurity Framework 2.0* ?

1.3 Batasan Masalah

1. Fokus penelitian ini menggunakan *NIST Cyber Security Framework 2.0*
2. Fokus pada sistem informasi kampus universiytas muhammadiyah Lamongan yang mencakup layanan akademik, yaitu *sistem informasi akademik* (SIAK).

1.4 Tujuan Penelitian

1. Meningkatkan keamanan sistem informasi kampus Universitas Muhammadiyah Lamongan menggunakan *NIST Cyber Security Framework 2.0.*
2. Implementasi risiko keamanan siber di kampus Universitas Muhammadiyah Lamongan menggunakan pendekatan *NIST Cyber Security Framework 2.0* guna meningkatkan keamanan sistem informasi.
3. Memberikan rekomendasi peningkatan keamanan siber kampus menggunakan NIST Cyber Security Framework 2.0.

1.5 Manfaat Penelitian

1. Bagi Tim IT Universitas Muhammadiyah Lamongan: Menyediakan pemahaman yang lebih baik mengenai risiko keamanan siber dan langkah-langkah mitigasi yang perlu dilakukan.
2. Bagi Peneliti: Menjadi referensi bagi penelitian selanjutnya terkait keamanan siber di lingkungan pendidikan.
3. Bagi Tenaga Pendidik (TENDIK) Universitas Muhammadiyah Lamongan: Memberikan wawasan bagi pihak-pihak terkait dalam pengambilan keputusan mengenai kebijakan keamanan informasi.