BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini telah melakukan penilaian risiko keamanan siber di Universitas Muhammadiyah Lamongan menggunakan *NIST Cybersecurity Framework 2.0*, khususnya pada kategori *Risk Assessment* (*RA1-10*). Berdasarkan hasil pengumpulan data melalui observasi, wawancara, serta kuesioner yang diadaptasi dari CSF Tools dan disesuaikan dengan konteks kampus, dapat disimpulkan bahwa tingkat kematangan keamanan siber di lingkungan kampus berada pada kategori "cukup baik" tetapi perlu peningkatan pada aspek tertentu.

Secara umum, kampus telah menunjukkan implementasi tata kelola keamanan siber yang positif, ditandai dengan adanya mekanisme identifikasi aset, penilaian risiko, pemantauan kerentanan, dan proses respons insiden yang relatif terstruktur. Hal ini terlihat dari beberapa skor yang tinggi pada kategori seperti penilaian risiko (RA-3), respon risiko (RA-7), dan perburuan ancaman (RA-10). Namun, masih ditemukan kekurangan pada aspek kebijakan tertulis, dokumentasi change log, dan sistem backup yang belum terotomasi serta terdokumentasi secara rutin.

Nilai rata-rata skor penilaian dari seluruh kategori NIST Risk Assessment (RA1-10) yang tersedia dalam penelitian ini adalah **4,01**dari skala 1-5. Hasil Skor ini menggambarkan tingkat kematangan keamanan siber pada aspek Risk Assessment di kampus telah berada pada level cukup baik dan stabil, namun tetap memiliki ruang untuk perbaikan di beberapa aspek tertentu.

5.2 Saran

1. Penyusunan Kebijakan Formal

Diperlukan adanya SOP dan kebijakan tertulis yang lengkap mengenai tata kelola keamanan informasi, pencegahan insiden, serta proses pemulihan bencana agar pengelolaan risiko lebih terdokumentasi dan mudah dievaluasi.

2. Penguatan Sistem Backup

Implementasi backup data secara otomatis dan terjadwal, beserta audit berkala pada sistem backup, sangat penting untuk meminimalisir risiko kehilangan data akibat serangan seperti ransomware.

3. Peningkatan Kesadaran dan Pelatihan

Pelatihan rutin bagi seluruh civitas akademika tentang praktik keamanan siber harus terus ditingkatkan. Pendekatan proaktif mengenai social engineering, penggunaan password yang kuat, dan pelaporan insiden perlu menjadi agenda utama.

4. Automasi dan Monitoring Berkelanjutan

Penguatan infrastruktur TI melalui monitoring kerentanan secara real-time dan automasi pada proses identifikasi serta pemulihan risiko agar ketahanan siber lebih terjamin.

5. Perluasan Kolaborasi Eksternal

Melanjutkan penyerapan informasi dari sumber eksternal seperti vendor keamanan sebagai sumber pembelajaran dan validasi terhadap standar keamanan yang diterapkan.

Dengan pelaksanaan saran di atas, diharapkan Universitas Muhammadiyah Lamongan dapat meningkatkan kematangan keamanan siber, memperkecil celah risiko, serta menciptakan lingkungan digital yang aman bagi seluruh civitas kampus.