BAB V
PENUTUP

5.1 Kesimpulan

Rendahnya kesadaran civitas akademika universitas terhadap serangan siber merupakan isu yang perlu mendapatkan perhatian serius. Fenomena ini dapat menimbulkan risiko yang signifikan terhadap integritas dan keamanan sistem informasi di lingkungan akademis. Hasil penelitian menunjukkan bahwa mahasiswa, dosen, dan staf administrasi masih memiliki tingkat pemahaman yang terbatas mengenai serangan siber dan dampaknya. Untuk mengatasi permasalahan ini, implementasi strategi keamanan siber yang terpadu dan terfokus pada edukasi menjadi krusial. Pelatihan rutin, workshop, dan seminar yang diselenggarakan oleh pusat keamanan siber di universitas dapat menjadi langkah efektif untuk meningkatkan pemahaman civitas akademika. Melibatkan mereka dalam program-program ini dapat membentuk kebiasaan proaktif dalam menjaga keamanan informasi.

Selain itu, kampanye informasi yang intensif perlu dilakukan untuk meningkatkan kesadaran civitas akademika. Penggunaan berbagai saluran komunikasi dan bahasa yang mudah dipahami dapat membantu menyampaikan pesan-pesan keamanan siber dengan lebih efektif. Langkah-langkah konkret, seperti penerapan kebijakan keamanan siber yang ketat, juga perlu diambil untuk menciptakan lingkungan yang lebih terlindungi. Kerjasama antaruniversitas, industri keamanan siber, dan pemerintah dapat memberikan dukungan yang signifikan dalam upaya meningkatkan keamanan siber di lingkungan akademis. Pertukaran informasi dan pengetahuan mengenai ancaman terkini dapat meningkatkan kapasitas universitas dalam menghadapi serangan siber yang semakin canggih. Penting untuk mencatat bahwa kesadaran terhadap serangan siber bukan hanya tanggung jawab individu, tetapi juga merupakan komitmen bersama untuk menjaga keamanan informasi universitas. Dengan mengimplementasikan strategi keamanan siber yang holistik dan melibatkan seluruh komunitas akademika, diharapkan dapat menciptakan lingkungan yang lebih aman dan sadar akan ancaman siber.

Institusi XYZ belum memiliki kebijakan dan strategi keamanan siber yang memadai untuk melindungi sistem teknologi informasi dan data institusi dari ancaman serangan siber. Hal ini berpotensi mengganggu operasional, kehilangan data penting, serta menurunkan kepercayaan pemangku kepentingan terhadap institusi. Beberapa strategi keamanan siber yang dapat direkomendasikan antara lain pembentukan tim khusus keamanan TI, penyusunan

kebijakan dan prosedur keamanan siber, sosialisasi dan pelatihan budaya keamanan data, hingga pengadaan solusi keamanan TI terkini. Implementasi strategi tersebut memerlukan komitmen dan dukungan penuh dari pimpinan dan seluruh anggota Institusi XYZ. Dengan penerapan strategi keamanan siber yang komprehensif, diharapkan Institusi XYZ mampu meningkatkan ketahanan sistem TI dan melindungi kerahasiaan, integritas, serta ketersediaan data institusi dari segala bentuk serangan siber. Sehingga, fungsi edukasi, penelitian, dan pengabdian kepada masyarakat XYZ tetap dapat berjalan secara optimal.

Sebagai penelitian awal, Disarankan untuk meneruskan studi lebih lanjut guna memperoleh pemahaman yang lebih mendalam mengenai faktor-faktor yang mempengaruhi tingkat kesadaran terhadap serangan siber di lingkungan akademis. Hal ini dapat memberikan kontribusi yang lebih signifikan dalam merancang kebijakan dan strategi yang lebih tepat guna menghadapi tantangan keamanan siber yang terus berkembang di era digital ini.

5.2 Saran

Berikut adalah rekomendasi yang dapat Peneliti berikan untuk mengembangkan sistem keamanan tersebut.

1. Keamanan siber di Institusi XYZ sudah cukup kuat tetapi belum maksimal, sehingga masih bisa dikembangkan lagi agar perlindungan terhadap keamanan siber nya menjadi maksimal. Misalnya dengan berinvestasi pada solusi keamanan TI terkini seperti antivirus, firewall, intrusion detection system, enkripsi data, dan data backup guna memperkuat sistem pertahanan institusi dari serangan dunia maya.
2. Mengusulkan pelaksanaan kampanye informasi yang intensif menggunakan berbagai saluran komunikasi, seperti media sosial, email, dan papan

pengumuman digital. Kampanye tersebut harus memberikan informasi yang mudah dipahami dan relevan mengenai risiko serangan siber, serta tindakan yang dapat diambil untuk melindungi diri. Melaksanakan program rutin sosialisasi dan pelatihan keamanan siber bagi dosen, karyawan, dan mahasiswa agar tercipta budaya keamanan data dan kesadaran mengenai ancaman siber.

3. Mengingatkan pentingnya merancang dan mengimplementasikan kebijakan keamanan siber yang jelas dan tegas. Kebijakan ini harus mencakup aspek-aspek seperti pengelolaan kata sandi, pemantauan aktivitas jaringan, dan tindakan respons cepat terhadap insiden keamanan. Keterlibatan seluruh civitas akademika dalam pengembangan kebijakan ini juga perlu ditekankan.
4. *Framework NIST Cyber Security* yang sudah peneliti buat dapat dikembangkan lebih jauh lagi dikemudian hari atau dikombinasikan dengan framework keamanan siber lain agar keamanan siber di Institusi XYZ menjadi super aman dan sangat sulit untuk diserang.