BAB 5 KESIMPULAN

Dalam penutup penelitian Analisis Risiko dalam mengatasi serangan siber pada Perusahaan Teknologi Informasi, kami menyimpulkan bahwa pengelolaan risiko serangan siber adalah aspek yang sangat penting dalam menjaga keberlanjutan operasi perusahaan. Temuan utama penelitian ini mencakup identifikasi risiko utama, seperti serangan phishing, malware, dan ransomware, serta strategi mitigasi yang direkomendasikan untuk mengurangi risiko tersebut. Implikasi dari risiko serangan siber terhadap perusahaan adalah signifikan, termasuk potensi kerugian finansial, reputasi yang rusak, dan gangguan operasional. Oleh karena itu, kami merekomendasikan bahwa perusahaan harus mengadopsi pendekatan proaktif dalam melindungi aset dan operasi mereka dari serangan siber. Rekomendasi kami mencakup implementasi kontrol keamanan yang tepat, peningkatan kesadaran keamanan karyawan, serta pengembangan rencana tanggapan terhadap insiden yang efektif. Langkah-langkah ini akan membantu perusahaan untuk mengurangi risiko serangan siber dan meningkatkan kesiapan dalam menghadapi ancaman tersebut. Kami berharap bahwa hasil penelitian ini dapat memberikan kontribusi positif dalam meningkatkan kesadaran tentang pentingnya keamanan siber di kalangan perusahaan teknologi informasi. Dengan menerapkan strategi mitigasi yang tepat, kami yakin bahwa perusahaan dapat mengurangi risiko serangan siber dan melindungi aset mereka dengan lebih efektif di masa mendatang. Cybercrime terus berkembang seiring dengan perkembangan pesat teknologi informasi dan komunikasi, jadi cybersecurity yang handal dan efektif diperlukan untuk menanggulanginya. [16] Metode OCTAVE memberikan pedoman sistematis dan menyeluruh untuk manajemen risiko keamanan informasi. Metode ini lebih menekankan pengelolaan risiko berbasis ancaman (bahaya) dan kelemahan (kelemahan) terhadap aset informasi organisasi, yang mencakup perangkat keras, lunak, sistem, informasi, dan manusia. [24]