BAB IV

KESIMPULAN DAN SARAN

1.1 Kesimpulan

Analisis menunjukkan bahwa kerja sama ASEAN melalui ACCP memainkan peran strategis dalam menghadapi ancaman siber LockBit melalui tiga mekanisme utama: Institusionalisme ACCP memperkuat kepercayaan, mengurangi ketidakpastian, dan menyediakan platform koordinasi dalam respons regional terhadap ransomware LockBit yang bersifat *borderless*. *Mutual Understanding* menciptakan persepsi ancaman bersama dan standar respons yang seragam, memungkinkan penanganan lebih cepat dan terkoordinasi. Kolektivisme dan Harmonisasi Regulasi memperkuat kohesi regional serta menyatukan kebijakan, kapasitas teknis, dan prosedur investigasi lintas negara untuk menghadapi ancaman siber yang bersifat transnasional. Secara keseluruhan, ACCP menjadi pondasi penting dalam pembentukan ketahanan siber ASEAN, terutama pada periode 2023–2025 ketika ancaman ransomware seperti LockBit meningkat secara signifikan dan menargetkan berbagai institusi strategis di kawasan sehingga berdampak *domino* bagi negara-negara anggota. Analisis ini menunjukkan bahwa ACCP berperan strategis dalam memperkuat ketahanan siber kawasan terhadap ancaman ransomware LockBit yang semakin kompleks dan bersifat *borderless*. LockBit 3.0, dengan model *Ransomware-as-a-Service* dan teknik enkripsi serta eksfiltrasi data yang sangat cepat, memanfaatkan kesenjangan dari kesiapan keamanan digital negara-negara anggota ASEAN.

Serangan terhadap Pusat Data Nasional Indonesia pada 2024 membuktikan bahwa ancaman ini menimbulkan dampak sistemik dan memerlukan respons kolektif dari negara-negara anggota. Melalui ACCP, ASEAN meningkatkan kapasitas teknis, berbagi intelijen IoC secara *real-time*, mempersiapkan infrastruktur kritis melalui *ransomware playbook*, serta menyelaraskan berbagai kebijakan keamanan siber kawasan. Kolaborasi dengan Europol, INTERPOL, OECD, dan CISA semakin memperkuat kemampuan investigasi dan respons multinasional. Secara keseluruhan, ACCP mampu mentransformasi tindakan ASEAN dari yang bersifat nasional-reaktif menjadi pertahanan siber regional yang terkoordinasi, adaptif, dan berbasis kapasitas bersama dari negara-negara anggota.

1.2 Saran

1. Penguatan Mekanisme Berbagi Intelijen Siber Regional

Penelitian selanjutnya disarankan untuk lebih menilai efektivitas platform berbagi Indicators of Compromise (IoC) antar-CSIRT ASEAN, termasuk hambatan teknis, birokratis, dan politik yang memengaruhi kecepatan respons terhadap ransomware seperti LockBit.

2. Evaluasi Implementasi Ransomware Playbook di Negara Anggota ASEAN

Studi lanjutan dapat mengukur sejauh mana regional ransomware playbook benar-benar diadopsi oleh negara anggota, terutama kesiapan pusat data nasional dan lembaga publik dalam menghadapi serangan berskala besar yang berdampak lintas sektor.

3. Analisis Kapasitas Nasional dan Kesenjangan Kelembagaan

Penelitian mendatang diharapkan dapat memetakan perbedaan kesiapan keamanan siber antarnegara ASEAN secara kuantitatif, sehingga dapat

mengidentifikasi faktor yang memperlemah efektivitas ACCP dalam penanganan ancaman siber kolektif.

4. Peran Aktor Non-Negara dalam Ketahanan Siber ASEAN

Studi lebih lanjut diperlukan untuk mengevaluasi kontribusi sektor swasta, penyedia cloud, dan perusahaan keamanan digital dalam mendukung kemampuan deteksi dan mitigasi ransomware di tingkat regional.

5. Model Governance Baru untuk Ancaman Siber Lintas-Batas

Penelitian dapat mengembangkan model tata kelola siber ASEAN berbasis multi-stakeholder ecosystem guna memperkuat respons terhadap kelompok ransomware global seperti LockBit, sekaligus memastikan konvergensi kebijakan yang lebih terukur.