BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pembahasan yang telah dijelaskan dalam penelitian ini bertujuan untuk menganalisis dampak serangan *ransomware Lockbit* 3.0 terhadap PDNS dan infrastruktur informasi vital nasional (IIV) di Indonesia, serta mengevaluasi kesiapan dan strategi mitigasi yang diterapkan dalam menghadapi serangan tersebut. Berikut adalah kesimpulan yang disangkutpautkan dengan tujuan penelitian ini:

1. **Analisis Dampak Serangan *ransomware Lockbit* 3.0 terhadap PDNS dan Infrastruktur Informasi Vital Nasional (IIV)**

   Serangan *ransomware Lockbit* 3.0 menunjukkan potensi ancaman serius terhadap PDNS dan IIV yang mendukung kedaulatan digital Indonesia. *Lockbit* 3.0 berhasil mengeksploitasi kerentanannya dalam sistem yang terhubung, menyebabkan dampak besar pada keamanan data dan operasional sistem. *Malware* ini memanfaatkan celah dalam pengelolaan kredensial dan kurangnya segmentasi jaringan untuk menyebar di dalam infrastruktur PDNS, yang dapat memperburuk ancaman terhadap data vital nasional. Dalam hal ini, serangan tersebut mengungkapkan betapa rentannya infrastruktur nasional Indonesia terhadap serangan *ransomware* yang semakin canggih.

2. **Identifikasi dan Evaluasi Dampak Langsung dan Tidak Langsung terhadap Aspek Operasional, Finansial, dan Keamanan Data**

   Dampak langsung serangan *ransomware Lockbit* 3.0 sangat terasa dalam aspek operasional PDNS, yang mencakup penurunan kinerja sistem akibat penggunaan CPU dan sumber daya yang tinggi oleh *Malware*. Dalam aspek finansial, biaya yang terkait dengan pemulihan, pengamanan data, serta potensi kerugian dari kebocoran data dapat sangat besar. Data vital yang terenkripsi atau hilang

menyebabkan kerugian lebih lanjut, mengganggu operasional harian dan mempengaruhi layanan yang bergantung pada data tersebut. Selain itu, kerugian tidak langsung meliputi dampak reputasi dan kepercayaan publik terhadap kemampuan PDNS dalam melindungi data dan menjaga sistem yang mendukung kedaulatan digital Indonesia.

3. **Penilaian Efektivitas Respons dan Strategi Mitigasi yang Dilakukan**

Respons dan strategi mitigasi yang diterapkan selama dan setelah serangan *ransomware* di PDNS menunjukkan beberapa kekuatan, seperti isolasi jaringan dan pemulihan data dari *backup* yang terisolasi. Namun, ada kelemahan yang signifikan dalam hal kecepatan deteksi, pemutusan koneksi, serta pembaruan dan efektivitas SOP mitigasi yang ada. SOP yang tidak diperbarui secara berkala dan tidak terstruktur menyebabkan keterlambatan dalam respons. Selain itu, kurangnya pelatihan dan simulasi serangan bagi staf menghambat kesiapan dalam menghadapi serangan yang kompleks. Oleh karena itu, meskipun ada respons yang berhasil dalam membatasi penyebaran *ransomware*, kesiapan dan efektivitas mitigasi perlu ditingkatkan secara signifikan.

4. **Rekomendasi Strategis untuk Meningkatkan Kesiapan dan Ketahanan Keamanan Siber PDNS dan IIV**

Berdasarkan analisis, terdapat beberapa rekomendasi strategis untuk meningkatkan kesiapan dan ketahanan PDNS dan IIV terhadap serangan *ransomware*. Pertama, pembaruan dan penyusunan ulang SOP mitigasi sesuai standar internasional, seperti NIST Cybersecurity *Framework*, diperlukan untuk meningkatkan respons dan pemulihan serangan. Kedua, sistem deteksi dini berbasis perilaku dan anomali serta pemutusan koneksi yang cepat harus diimplementasikan guna mengurangi dampak serangan. Selain itu, pelatihan rutin dan simulasi serangan *ransomware* akan memperkuat kesiapan staf menghadapi ancaman nyata. Kebijakan keamanan juga perlu diperkuat melalui

pengelolaan *backup* data yang aman, penerapan autentikasi multi-faktor (MFA), dan pengelolaan kredensial yang ketat. Terakhir, peningkatan kesadaran keamanan siber melalui pendidikan dan pelatihan berkelanjutan kepada seluruh staf sangat penting untuk memastikan kesiapan organisasi dalam mencegah serangan.

5.2 Saran

Berikut adalah saran pada penelitian yang sudah dikerjakan:

1. **Studi Perbandingan dengan Organisasi Lain**
   Lakukan perbandingan respons dan strategi mitigasi terhadap serangan *ransomware* di berbagai organisasi, baik di Indonesia maupun luar negeri, untuk memperoleh rekomendasi yang lebih luas.
2. **Penggunaan Teknologi AI dalam Deteksi *ransomware***
   Teliti penerapan kecerdasan buatan (AI) dan machine learning dalam deteksi dan respons serangan *ransomware* untuk meningkatkan kecepatan dan akurasi mitigasi.
3. **Evaluasi Dampak Jangka Panjang Serangan *ransomware***
   Lakukan analisis mendalam mengenai dampak ekonomi dan operasional jangka panjang dari serangan *ransomware* terhadap infrastruktur digital nasional Indonesia.
4. **Penerapan Kebijakan Keamanan yang Lebih Ketat**
   Evaluasi kebijakan keamanan siber di PDNS, termasuk autentikasi multi-faktor (MFA), untuk meningkatkan perlindungan terhadap data vital dan mengurangi risiko serangan.
5. **Pengembangan Simulasi Serangan *ransomware* yang Lebih Realistis**
   Kembangkan simulasi serangan *ransomware* yang lebih realistis dan terstruktur untuk meningkatkan kesiapan dan respons staf dalam menangani serangan dunia nyata.