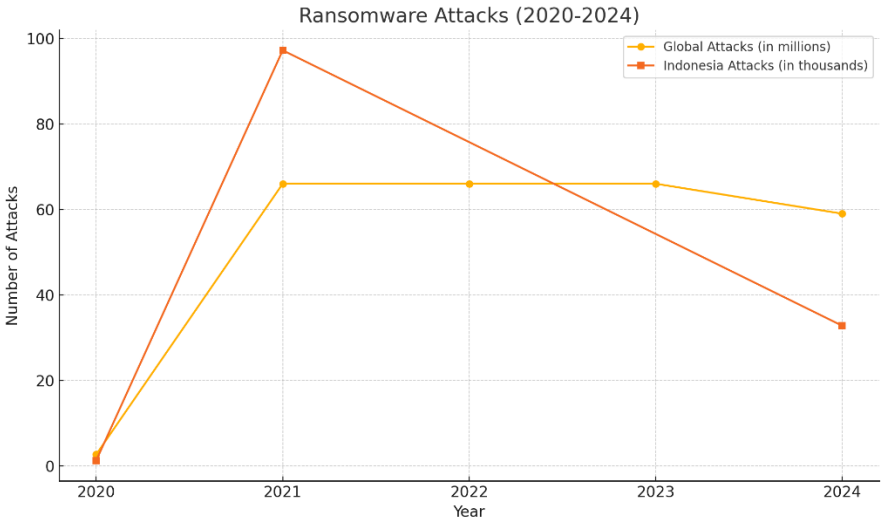
BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin maju, Infrastruktur Informasi Vital (IIV) menjadi tulang punggung berbagai sektor strategis di Indonesia, seperti keuangan, energi, kesehatan, transportasi, dan pemerintahan. Salah satu komponen utama IIV adalah Pusat Data Nasional Sementara (PDNS), yang berfungsi sebagai penyimpan, pengelola, dan pelindung data penting yang mendukung berbagai layanan publik dan operasional pemerintah. PDNS memainkan peran penting dalam mendukung Sistem Pemerintahan Berbasis Elektronik (SPBE) yang aman dan efisien. Namun, seiring dengan perkembangan teknologi, peningkatan digitalisasi ini juga diiringi dengan ancaman keamanan siber yang semakin kompleks dan meningkat, termasuk serangan *ransomware*, yang menjadi perhatian serius bagi keamanan nasional (Smith et al., 2023).



Gambar 1. 1 Serangan ransomware

ransomware adalah salah satu bentuk serangan siber yang memiliki dampak destruktif dan luas. Pelaku *ransomware* mengenkripsi data korban dan meminta tebusan sebagai syarat pemulihan. Varian *ransomware* seperti *Lockbit* 3.0 bahkan menggunakan metode *double extortion*, dimana mereka tidak hanya menuntut tebusan tetapi juga mengancam untuk

mempublikasikan data sensitif jika tuntutan tidak dipenuhi. Menurut *World Economic Forum* (2023), *ransomware* kini berkembang menjadi ancaman serius terhadap keamanan nasional karena dampaknya yang tidak hanya bersifat ekonomi tetapi juga berpotensi merusak kepercayaan publik dan stabilitas layanan vital (Perez & Collins, 2024).

Ancaman *ransomware* di Indonesia semakin nyata, terutama dengan adanya insiden-insiden yang menargetkan lembaga pemerintah dan sektor vital lainnya. Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN), insiden *ransomware* di Indonesia meningkat signifikan dalam beberapa tahun terakhir, mencapai kenaikan 40% hanya dalam dua tahun terakhir. Serangan *ransomware* terhadap PDNS, misalnya, dapat menyebabkan kerugian finansial yang besar, gangguan operasional, penurunan kepercayaan publik, dan ancaman terhadap keamanan nasional. Selain itu, dokumen Rencana Aksi Nasional Keamanan Siber (RAN Kamsiber) 2024-2028 menekankan pentingnya keamanan siber sebagai prioritas utama dalam menjaga kedaulatan digital Indonesia. Rencana ini menyoroti perlindungan terhadap IIV dan pentingnya kerjasama *multi-stakeholder* dalam menghadapi ancaman yang terus berkembang.

Meskipun berbagai langkah telah dilakukan, termasuk penerapan standar keamanan tinggi, tantangan signifikan masih dihadapi dalam menangani ancaman *ransomware* terhadap PDNS dan IIV. Dokumen KAK PDNS 2023 menunjukkan bahwa ketergantungan pada satu pusat data menimbulkan risiko *single point of failure*, yang berpotensi meningkatkan kerentanan jika serangan siber berhasil menembus lapisan keamanan PDNS. Sebagai perbandingan, negara-negara seperti Thailand telah menerapkan pendekatan yang lebih fleksibel dengan menggandeng konsorsium layanan *Cloud* swasta, sehingga memperkuat redundansi dan ketahanan siber pada pusat data nasional mereka (KAK PDNS, 2023; Insiden Siber PDNS, 2023)

Selain itu, evaluasi penanganan insiden *ransomware* pada PDNS menunjukkan bahwa mitigasi sering kali terkendala oleh kurangnya sistem deteksi dini dan sumber daya keamanan siber yang memadai. Standar-standar internasional seperti MITRE ATT&CK, NIST CSF, dan ISO 27035 menekankan pentingnya strategi respons yang komprehensif dalam menghadapi ancaman siber. Namun, implementasi strategi-strategi ini di Indonesia masih menghadapi kendala sumber daya dan kesadaran keamanan yang belum merata (IBM Security X-Force, 2023). Berdasarkan temuan ini, ada kebutuhan mendesak akan penelitian yang lebih mendalam untuk memahami dampak serangan *ransomware* pada IIV di Indonesia, terutama dalam konteks PDNS, guna merumuskan langkah mitigasi yang tepat.

Melalui studi ini, diharapkan akan diperoleh pemahaman yang lebih baik mengenai risiko dan dampak serangan *ransomware* terhadap IIV serta perumusan rekomendasi kebijakan dan strategi mitigasi yang lebih efektif untuk memperkuat ketahanan siber Indonesia di masa depan.

1.2 Identifikasi Masalah

Serangan *ransomware* yang dilakukan oleh kelompok menggunakan varian seperti *Lockbit* 3.0 telah menjadi ancaman serius bagi Infrastruktur Informasi Vital (IIV), termasuk di Indonesia. Berdasarkan identifikasi masalah dalam konteks ini, terdapat beberapa isu utama yang perlu diperjelas:

1. Risiko Tinggi Serangan pada Pusat Data Nasional Sementara (PDNS) sebagai Infrastruktur Vital. Ketergantungan pada PDNS sebagai pusat data strategis meningkatkan risiko *single point of failure*, dimana serangan *ransomware Lockbit* 3.0 dapat mengganggu operasional layanan publik dan menurunkan kepercayaan publik.
2. Kurangnya Pemahaman Dampak *ransomware* terhadap Infrastruktur Informasi Vital (IIV). Dampak jangka panjang *ransomware* pada IIV di Indonesia belum dipahami secara

mendalam, khususnya dalam konteks keamanan nasional dan stabilitas publik.

3. Keterbatasan dalam Strategi Mitigasi dan Deteksi Dini. Evolusi *ransomware* yang semakin canggih menuntut strategi keamanan yang lebih efektif, namun implementasi standar keamanan masih terkendala pada deteksi dini dan respons insiden yang belum optimal.
4. Tingginya Ketergantungan Digital Tanpa Investasi Keamanan Siber Memadai. Transformasi digital yang cepat tidak diiringi dengan investasi yang cukup dalam keamanan siber, menjadikan IIV rentan terhadap serangan, sehingga mengancam sektor-sektor strategis dan stabilitas nasional.

1.3 Rumusan Masalah

Berdasarkan identifikasi masalah diatas, penelitian ini merumuskan beberapa pertanyaan kunci sebagai berikut:

1. Bagaimana serangan *ransomware Lockbit* 3.0 memengaruhi Pusat Data Nasional Sementara (PDNS) dan Infrastruktur Informasi Vital (IIV) di Indonesia, khususnya dalam hal operasional dan keamanan data?
2. Bagaimana dampak langsung dan tidak langsung dari serangan *ransomware* terhadap aspek operasional, finansial, serta keamanan data di PDNS?
3. Bagaimana efektivitas respons dan upaya mitigasi yang dilakukan selama dan setelah terjadinya serangan *ransomware* di PDNS?
4. Rekomendasi strategis apa yang dapat diterapkan untuk memperkuat keamanan siber PDNS dan melindungi IIV dari ancaman *ransomware* di masa depan?

1.4 Pembatasan Masalah

Batasan masalah diperlukan untuk memastikan bahwa penelitian ini memiliki fokus yang jelas dan dapat dilakukan secara spesifik serta

mendalam. Adapun pembatasan masalah dalam penelitian ini adalah sebagai berikut:

1. **Fokus pada Serangan *ransomware Lockbit* 3.0**
   Penelitian ini difokuskan pada *ransomware* varian *Lockbit* 3.0 sebagai studi kasus utama. Pemilihan varian ini didasarkan pada fakta bahwa *Lockbit* 3.0 adalah salah satu ancaman *ransomware* paling signifikan dengan kemampuan canggih yang memungkinkan serangan cepat dan sulit dideteksi. Pendekatan ini memungkinkan penelitian untuk mendalami dampak spesifik dari *ransomware* varian ini terhadap infrastruktur vital nasional, tanpa mencakup ancaman siber lainnya.
2. **Analisis Dampak pada Pusat Data Nasional Sementara (PDNS)**
   Ruang lingkup penelitian dibatasi pada dampak serangan *Lockbit* 3.0 terhadap PDNS, yang mewakili Infrastruktur Informasi Vital (IIV) di Indonesia. Fokus penelitian ini adalah pada dampak operasional, finansial, dan keamanan data yang timbul dari serangan tersebut. Analisis tidak mencakup infrastruktur lain di luar PDNS untuk menjaga kedalaman dan ketelitian kajian pada satu pusat data strategis yang krusial bagi operasional pemerintahan dan sektor publik di Indonesia.
3. **Penekanan pada Dampak dan Strategi Mitigasi**
   Penelitian ini menitikberatkan analisis pada dampak langsung dan tidak langsung dari serangan *ransomware Lockbit* 3.0 terhadap PDNS, termasuk kerugian operasional dan risiko keamanan nasional. Selain itu, penelitian ini juga mengevaluasi efektivitas strategi mitigasi yang diterapkan oleh PDNS. Walaupun karakteristik teknis dari *Lockbit* 3.0 dijelaskan sebagai latar belakang, penelitian ini tidak akan membahas kode *Malware* atau aspek teknis lainnya secara rinci.

4. **Rentang Waktu Studi Kasus**

   Analisis dalam penelitian ini dibatasi pada insiden serangan *ransomware Lockbit* 3.0 yang terjadi dalam rentang waktu satu tahun terakhir. Fokus pada periode ini memungkinkan identifikasi peristiwa yang paling relevan dan berdampak besar terhadap PDNS, serta memastikan bahwa data yang digunakan adalah yang terbaru. Studi ini tidak mencakup serangan *ransomware* di luar rentang waktu tersebut untuk menjaga ketepatan konteks penelitian.

1.5 Tujuan Penelitian

Penelitian ini bertujuan untuk memberikan pemahaman mendalam mengenai dampak serangan *ransomware* pada Infrastruktur Informasi Vital (IIV) dengan studi kasus serangan *Lockbit* 3.0 pada Pusat Data Nasional Sementara (PDNS). Secara spesifik, tujuan penelitian ini adalah:

1. Menganalisis dampak serangan *ransomware Lockbit* 3.0 terhadap PDNS dan infrastruktur informasi vital nasional di Indonesia, serta mengidentifikasi kerentanan dan risiko yang dihadapi guna menjaga kedaulatan digital Indonesia dari ancaman serangan siber.
2. Mengidentifikasi dan mengevaluasi dampak langsung dan tidak langsung dari serangan *ransomware* terhadap aspek operasional, finansial, dan keamanan data di PDNS.
3. Menilai efektivitas respons dan strategi mitigasi yang dilakukan selama dan setelah terjadinya serangan *ransomware* di PDNS, serta mengidentifikasi kekuatan dan kelemahan dalam pendekatan yang diterapkan.
4. Merumuskan rekomendasi strategis untuk meningkatkan kesiapan dan ketahanan keamanan siber PDNS dan IIV, termasuk penguatan protokol keamanan, peningkatan kesadaran, serta kesiapan mitigasi terhadap serangan *ransomware* di masa depan.

1.6 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat bagi berbagai pihak yang terlibat dalam pengelolaan dan perlindungan Infrastruktur Informasi Vital (IIV), khususnya dalam konteks keamanan siber. Beberapa manfaat utama dari penelitian ini meliputi:

1.6.1 Manfaat Teoritis

a. **Bagi Pengembangan Teori**

   Penelitian ini diharapkan dapat memperkaya literatur terkait keamanan siber, khususnya dalam konteks dampak serangan *ransomware* pada IIV. Penelitian ini juga dapat menjadi dasar untuk mengembangkan model-model teoretis baru dalam mengidentifikasi dan mengelola risiko keamanan siber terhadap infrastruktur vital.

b. **Bagi Pengembangan Keilmuan**

   Hasil penelitian ini dapat mendukung pengembangan keilmuan di bidang keamanan siber, terutama mengenai analisis risiko, respons, dan strategi mitigasi serangan *ransomware* pada pusat data nasional. Temuan ini diharapkan memberikan wawasan yang dapat digunakan dalam studi keamanan informasi di Indonesia dan negara-negara lain.

c. **Bagi Peneliti**

   Penelitian ini memberikan kesempatan bagi peneliti untuk memperoleh pemahaman mendalam tentang ancaman *ransomware* pada IIV dan meningkatkan keahlian dalam mengkaji dan menganalisis strategi mitigasi serta protokol keamanan siber yang efektif.

1.6.2 Manfaat Praktis

a. **Bagi Pengawak PDNS dan IIV**

   Penelitian ini dapat memberikan rekomendasi praktis untuk meningkatkan kesiapan dan respons keamanan siber di PDNS dan IIV. Rekomendasi ini dapat membantu pengelola pusat data dalam

menghadapi serangan *ransomware* secara lebih efektif dan mengurangi potensi dampak operasional maupun kerugian finansial.

b. **Bagi *Stakeholder* Terkait (BSSN, Kominfo, dll)**

   Hasil penelitian ini dapat menjadi referensi bagi lembaga-lembaga pemerintah seperti BSSN dan Kominfo dalam merumuskan kebijakan keamanan siber yang lebih komprehensif untuk melindungi IIV dari ancaman *ransomware* dan serangan siber lainnya.

c. **Bagi Praktisi Keamanan Siber**

   Penelitian ini dapat memberikan wawasan tambahan bagi praktisi keamanan siber mengenai pola dan dampak serangan *ransomware*, serta strategi mitigasi yang efektif. Temuan penelitian ini juga dapat digunakan sebagai bahan untuk meningkatkan protokol keamanan dan respons insiden di sektor-sektor vital.

d. **Bagi Industri**

   Penelitian ini dapat membantu perusahaan, khususnya yang mengelola data sensitif atau berperan dalam IIV, untuk memahami pentingnya investasi dalam keamanan siber dan mendukung penerapan strategi mitigasi yang lebih kuat terhadap ancaman *ransomware*.

e. **Bagi Masyarakat Umum**

   Penelitian ini diharapkan dapat meningkatkan kesadaran masyarakat tentang pentingnya keamanan siber, terutama dalam konteks perlindungan terhadap data publik dan layanan yang disediakan oleh IIV. Dengan meningkatnya kesadaran, masyarakat dapat mendukung dan mendorong perlindungan data yang lebih baik oleh pemerintah dan industri.

Manfaat penelitian ini diharapkan dapat berkontribusi dalam pengembangan teori dan praktik keamanan siber, serta mendukung perlindungan dan pengelolaan yang lebih baik terhadap IIV di Indonesia.