BAB II
TINJAUAN PUSTAKA

2.1 Landasan Teori

Landasan teori berfungsi sebagai fondasi konseptual dari penelitian ini. Teori-teori yang dijelaskan dibawah ini mencakup konsep utama yang terkait dengan *ransomware*, keamanan siber pada Infrastruktur Informasi Vital (IIV), serta pendekatan mitigasi dan respons terhadap serangan *ransomware*.

2.1.1 Teori Sistem Keamanan Nasional

Teori sistem keamanan nasional adalah konsep yang mengacu pada kebijakan dan strategi suatu negara dalam menjaga stabilitas dan keselamatan dari ancaman internal maupun eksternal. Ini mencakup keamanan negara, publik, dan individu melalui pendekatan militer dan non-militer. Pendekatan ini melibatkan berbagai sektor seperti politik, ekonomi, dan diplomasi untuk memastikan ketahanan nasional. Keamanan nasional kini mencakup ancaman siber yang menjadi salah satu isu utama di era digital. Infrastruktur Informasi Vital (IIV) adalah bagian penting dari sistem keamanan nasional, karena gangguan pada infrastruktur ini dapat mengancam stabilitas negara, layanan publik, hingga ekonomi nasional. Ancaman siber seperti *ransomware*, termasuk varian *Lockbit* 3.0, menyoroti bagaimana teknologi dapat digunakan sebagai alat untuk mengganggu kedaulatan digital suatu negara.

2.1.1.1 Signifikansi IIV dalam Sistem Keamanan Nasional

IIV terdiri dari sistem dan jaringan yang mendukung fungsi-fungsi strategis negara, termasuk transportasi, energi, keuangan, kesehatan, dan pemerintahan. Serangan terhadap sektor ini dapat menyebabkan:

a. **Gangguan layanan publik:** Layanan penting seperti listrik, transportasi, atau komunikasi dapat terhenti, menciptakan ketidakstabilan sosial.
b. **Kerugian ekonomi:** Misalnya, laporan MIT menunjukkan bahwa *ransomware* menjadi ancaman utama dengan peningkatan sebesar

70% pada tahun 2023, dimana kerugian akibat serangan siber global diproyeksikan mencapai triliunan dolar setiap tahunnya (Cisa Gov, 2024) (MIT Sloan, 2024).

c. **Ancaman terhadap kedaulatan:** Ketika data sensitif dari infrastruktur nasional dicuri, ancaman ini dapat digunakan oleh aktor asing untuk melemahkan negara melalui spionase atau sabotase.

2.1.1.2 Ancaman *ransomware* terhadap IIV

Ransomware seperti *Lockbit* 3.0 menggunakan pendekatan *double extortion*, dimana pelaku tidak hanya mengunci akses data tetapi juga mencuri dan mengancam mempublikasikan informasi sensitif jika tuntutan tebusan tidak dipenuhi. Serangan ini sangat berbahaya bagi IIV karena:

- **Dampak fisik dan ekonomi:** Pada tahun 2024, sekitar 80% dari pelanggaran data global melibatkan infrastruktur berbasis *Cloud*, yang juga menjadi target utama *ransomware* (IBM Survey, 2023) (MIT Sloan, 2024).
- **Teknologi canggih:** *Lockbit* 3.0 menggunakan mekanisme enkripsi cepat dan teknik anti-forensik, membuatnya sulit dideteksi atau dihentikan oleh langkah keamanan tradisional.
- **Ekosistem *ransomware-as-a-service* (RaaS):** Model ini mempermudah aktor siber untuk melancarkan serangan, menyebabkan peningkatan drastis jumlah serangan *ransomware* di sektor publik dan kritis (Gartner, 2024) (MIT Sloan, 2024).

2.1.1.3 Kedaulatan Digital sebagai Bagian dari Keamanan Nasional

Kedaulatan digital adalah kemampuan negara untuk melindungi dan mengelola infrastruktur digital serta strategisnya. Kegagalan untuk melindungi IIV dari ancaman siber seperti *ransomware* dapat melemahkan stabilitas nasional melalui:

1. **Manipulasi informasi:** Kebocoran data dapat digunakan untuk menyebarkan informasi palsu atau menimbulkan ketidakpercayaan public terhadap pemerintah.

2. **Gangguan operasional:** Ketidakmampuan untuk memulihkan infrastruktur vital dalam waktu singkat dapat mengganggu fungsi pemerintah dan menurunkan legitimasi negara.

Laporan dari *Georgetown University* pada tahun 2024 menyoroti bahwa adopsi teknologi baru seperti AI dalam IIV dapat menciptakan peluan, tetapi juga meningkatkan risiko serangan siber melalui vektor baru, seperti kesalahan konfigurasi atau ekspoitasi *supply chain* (Georgetown University, 2024).

2.1.1.4 Langkah Strategis untuk Melindungi IIV

Teori Sistem Keamanan Nasional menekankan perlunya pendekatan komprehensif dalam melindungi IIV, termasuk:

1. **Regulasi yang ketat:** Mengimplementasikan kebijakan keamanan seperti Rencana Aksi Nasional Keamanan Siber *(RAN Kamsiber)*.
2. **Investasi dalam keamanan siber:** Memanfaatkan teknologi canggih seperti AI untuk deteksi dini ancaman, seperti yang diadopsi beberapa negara untuk memperkuat pelindungan IIV (Georgetown University, 2024) (Gartner, 2024).
3. **Kolaborasi lintas sektor:** Meningkatkan koordinasi antara pemerintah, sektor swasta, dan masyarakat untuk menciptakan respons yang cepat dan efisien.
4. **Pelatihan dan edukasi:** Meningkatkan kesadaran keamanan digital di seluruh lapisan masyarakat dan tenaga kerja (MIT Sloan, 2024).

2.1.1.5 Studi Kasus: Serangan *Lockbit* 3.0 di Sektor Kritis

Lockbit 3.0 telah menjadi ancaman utama bagi infrastruktur nasional di banyak negara sejak 2019. Di Indonesia, potensi serangan *ransomware* terhadap Pusat Data Nasional Sementara (PDNS) menempatkan data strategis pemerintah dan layanan publik dalam risiko tinggi. Tanpa perlindungan yang memadai, serangan semacam ini dapat mengakibatkan dampak ekonomi dan politik yang signifikan, seperti yang diamati dalam peningkatan serangan terhadap sektor keuangan dan infrastruktur berbasis *Cloud* pada tahun 2023-2024 (Cisa Gov, 2023) (MIT Sloan, 2024).

2.1.2 Dasar Hukum dan Regulasi Keamanan Siber

Regulasi keamanan siber adalah landasan penting dalam melindungi infrastruktur informasi, data, dan kepentingan negara dari ancaman siber seperti *ransomware*. Di Indonesia, berbagai kebijakan telah diterapkan untuk menghadapi tantangan keamanan siber, sementara di tingkat internasional, pendekatan multilateral dan kerangka hukum global juga memainkan peran penting.

2.1.2.1 Regulasi Keamanan Siber di Indonesia

1. **Rencana Aksi Nasional Keamanan Siber (RAN Kamsiber) 2024–2028**

   RAN Kamsiber adalah peta jalan strategis pemerintah Indonesia untuk melindungi Infrastruktur Informasi Vital Nasional (IIV). Fokusnya adalah pada peningkatan tata kelola keamanan siber, mitigasi risiko, peningkatan kesadaran publik, dan penguatan kolaborasi lintas sektor dalam melawan ancaman siber. Strategi ini juga mencakup koordinasi dengan Badan Siber dan Sandi Negara (BSSN) untuk mencegah serangan *ransomware* seperti *Lockbit* 3.0 (BSSN) (Europol IOCTA, 2023).

2. **Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)**

   UU ITE mengatur perlindungan data digital, penyalahgunaan teknologi, dan tindak pidana siber. Revisi terbaru dari UU ini menekankan perlunya kerangka hukum yang adaptif untuk mengatasi ancaman baru seperti serangan terhadap pusat data nasional dan pencurian data oleh *ransomware* (Kominfo).

3. **Undang-Undang Pelindungan Data Pribadi (UU PDP) 2022**

   UU PDP mengatur pengelolaan data pribadi untuk melindungi privasi pengguna di Indonesia. Hukum ini mensyaratkan perlindungan yang ketat terhadap data sensitif yang disimpan oleh entitas publik dan swasta, termasuk penunjukan *Data Protection Officer* dan evaluasi risiko pemrosesan data (Kominfo).

4. **Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE)**

   SPBE bertujuan menciptakan layanan digital yang aman dan efisien di pemerintahan. Peraturan ini mewajibkan instansi pemerintah menggunakan protokol keamanan tingkat tinggi untuk melindungi data dan layanan publik dari ancaman siber (Europol IOCTA, 2023) (Kominfo).

2.1.2.2 Regulasi Internasional dalam Keamanan Siber

1. **NIS2 *Directive* (European Union, 2024)**

   Uni Eropa meluncurkan NIS2 *Directive* sebagai pembaruan dari aturan *Network and Information Security* (NIS). Aturan ini mengharuskan negara anggota meningkatkan keamanan siber di sektor-sektor penting, seperti energi dan layanan digital. NIS2 mendorong adopsi standar keamanan internasional dan penanganan insiden dengan koordinasi antarnegara (Europol IOCTA, 2023).

2. **Kerangka Kerja PBB tentang Hukum Internasional di Dunia Maya**

   Melalui Resolusi PBB, beberapa negara mendorong penerapan hukum internasional untuk mencegah konflik di dunia maya. Fokus utamanya adalah melindungi kedaulatan digital negara, mengatur tanggung jawab negara untuk mencegah serangan yang berasal dari wilayahnya, dan meningkatkan akuntabilitas melalui kerja sama global (Carnegie Endowment).

3. **ASEAN Cybersecurity Cooperation Strategy**

   ASEAN telah merumuskan strategi kolaborasi keamanan siber yang bertujuan memperkuat perlindungan infrastruktur digital di Asia Tenggara. Strategi ini menekankan pentingnya pengembangan kapasitas siber regional, termasuk pelatihan keamanan dan peningkatan respons terhadap ancaman *ransomware* (ASEAN Cybersecurity Strategy, 2023) (BSSN).

4. **Budapest Convention on Cybercrime**

   Konvensi ini adalah kerangka kerja global pertama yang mengatur kejahatan siber, termasuk penanganan *ransomware*. Indonesia belum meratifikasi konvensi ini tetapi mengadopsi beberapa prinsipnya dalam pengembangan kebijakan domestik (Carnegie Endowment).

5. **Operasi Internasional seperti "Operation Cronos"**

   Operasi yang dipimpin Europol dan FBI pada 2024 berhasil melumpuhkan jaringan *Lockbit* 3.0. Ini menunjukkan pentingnya kolaborasi lintas negara untuk menangani kejahatan siber yang bersifat lintas batas (Europol IOCTA, 2023) (Carnegie Endowment).

2.1.3 Infrastruktur Informasi Vital

Infrastruktur Informasi Vital (IIV) adalah kumpulan jaringan, sistem, dan sumber daya penting yang mendukung fungsi strategis negara, seperti sektor pemerintahan, energi, transportasi, keuangan, dan kesehatan. Keamanan IIV merupakan prioritas karena gangguan pada infrastruktur ini dapat menimbulkan dampak besar, termasuk kerugian ekonomi, disfungsi layanan publik, dan risiko terhadap stabilitas nasional.

Menurut Peraturan Presiden Nomor 82 Tahun 2022, perlindungan terhadap IIV bertujuan untuk menghindari gangguan akibat penyalahgunaan teknologi informasi, termasuk serangan siber seperti *ransomware*. Kebijakan ini mengakui bahwa keberlanjutan IIV sangat tergantung pada ketahanan digital yang mencakup kemampuan untuk mencegah, mendeteksi, dan merespons ancaman dengan cepat (Aditya, Hafish., et al., 2024) (Aminudin, Agus. & Supriyanto, Aji., 2024).

Lockbit 3.0, salah satu ancaman *ransomware* paling signifikan, menunjukkan betapa rentannya infrastruktur ini. *Lockbit* menyerang dengan metode "*double extortion*," dimana pelaku tidak hanya mengenkripsi data tetapi juga mengancam mempublikasikannya, yang berisiko merusak kepercayaan publik terhadap institusi yang terlibat (Krishnan, Anupam., et al., 2024) (Aminudin, Agus. & Supriyanto, Aji., 2024).

Untuk menghadapi ancaman ini, pendekatan keamanan siber berbasis standar seperti NIST *Cybersecurity Framework* telah diterapkan di beberapa negara. *Framework* ini membantu memandu institusi dalam mengidentifikasi aset penting, melindungi sistem, mendeteksi ancaman, merespons serangan, dan memulihkan infrastruktur yang terkena dampak (Yang, Ester., et al., 2024).

Dalam konteks global, perlindungan IIV tidak hanya melibatkan teknologi tetapi juga tata kelola, pendidikan publik, dan kolaborasi internasional. Negara-negara seperti Amerika Serikat dan Uni Eropa telah menunjukkan bahwa pendekatan berbasis kolaborasi dan standar keamanan yang ketat dapat meningkatkan resiliensi terhadap ancaman siber yang terus berkembang (Krishnan, Anupam., et al., 2024) (Yang, Ester., et al., 2024).

2.1.4 Pusat Data Nasional Sementara (PDNS)

Pusat Data Nasional Sementara (PDNS) adalah komponen kunci dari Infrastruktur Informasi Vital (IIV) yang mendukung layanan publik dan pengelolaan data pemerintah secara terpusat. PDNS berperan dalam mengintegrasikan data dan aplikasi pemerintahan yang terdistribusi ke dalam satu pusat komputasi yang aman, efisien, dan terkelola.

2.1.4.1 Latar Belakang Pendirian PDNS

Menurut Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), pendirian PDNS merupakan langkah strategis untuk memastikan tata kelola data pemerintah yang terpusat dan terintegrasi. Lebih lanjut, Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur SPBE menekankan pentingnya pengintegrasian data, infrastruktur, dan layanan pemerintahan berbasis teknologi komputasi awan.

Saat ini, pembangunan Pusat Data Nasional yang permanen tengah dilakukan di beberapa lokasi, seperti Kabupaten Bekasi (Jawa Barat), Kota Batam (Kepulauan Riau), dan Ibu Kota Nusantara. Sementara itu, PDNS

disediakan sebagai layanan sementara berbasis *Cloud computing* melalui penyedia pihak ketiga hingga pembangunan fasilitas permanen selesai.

2.1.4.2 Keunggulan Teknologi *Cloud* dalam PDNS

Adopsi teknologi komputasi awan di PDNS menawarkan beberapa keunggulan signifikan:

1. **Skalabilitas:** Kapasitas penyimpanan dan pemrosesan data dapat disesuaikan dengan kebutuhan pemerintah tanpa investasi awal yang besar.
2. **Efisiensi Biaya:** Mengurangi biaya pengadaan infrastruktur fisik dan operasional, karena pemerintah hanya membayar berdasarkan penggunaan layanan.
3. **Ketersediaan Tinggi:** Teknologi *Cloud* menjamin layanan yang dapat diakses kapan saja dan dari berbagai lokasi, mendukung fleksibilitas operasional.
4. **Integrasi Data:** Memungkinkan penggabungan data dari berbagai instansi pemerintah, sehingga mendukung *big data analytics* dan pengambilan kebijakan berbasis data.

2.1.5 Teori Analisis *ransomware* dan *Lockbit* 3.0

Ransomware adalah jenis *Malware* yang dirancang untuk mengenkripsi data korban, kemudian menuntut pembayaran tebusan untuk mengembalikan akses. Salah satu varian paling canggih dalam kategori ini adalah *Lockbit* 3.0, yang telah menjadi ancaman global dengan kemampuan canggih dan pendekatan inovatif dalam menyerang sistem target. Teori ini membahas bagaimana *Lockbit* 3.0 bekerja, mulai dari penyebaran hingga dampaknya terhadap organisasi atau individu.

2.1.5.1 Karakteristik Utama *Lockbit* 3.0

1. ***Double extortion***

   Lockbit 3.0 memanfaatkan metode *double extortion* yang menggabungkan dua ancaman utama:

- **Enkripsi data:** Menggunakan algoritma enkripsi yang sangat kuat, *ransomware* ini mengunci data korban sehingga tidak dapat diakses tanpa kunci dekripsi.
- **Ancaman publikasi data:** Selain enkripsi, *Lockbit* 3.0 mencuri data sensitif dan mengancam untuk mempublikasikannya secara daring jika tebusan tidak dibayar. Strategi ini menambah tekanan psikologis pada korban, terutama organisasi yang menyimpan data rahasia seperti informasi pelanggan atau kebijakan internal (Unit 42, 2023) (Europol IOCTA, 2023).

2. **Penyebaran melalui *Phishing* dan Kerentanan Sistem**

   Lockbit 3.0 sering kali disebarkan melalui *email phishing* yang dirancang untuk mengelabui pengguna agar membuka lampiran atau tautan berbahaya. Selain itu, *ransomware* ini mengeksploitasi kerentanan dalam perangkat lunak yang belum diperbarui, sehingga memungkinkan akses tanpa otorisasi ke jaringan target (Accenture, 2023).

3. **Automasi dan Anti-Forensik**

   Varian ini dilengkapi dengan fitur otomatisasi untuk mempercepat penyebaran di dalam jaringan target, terutama melalui protokol SMB (*Server Message Block*). Selain itu, *Lockbit* 3.0 menggunakan teknik anti-forensik untuk menghapus jejaknya, membuat proses investigasi menjadi lebih sulit bagi pakar keamanan siber (Accenture, 2023) (MIT, 2023).

2.1.5.2 Dampak *ransomware Lockbit* 3.0

Lockbit 3.0 tidak hanya menggangu akses data tetapi juga menciptakan kerugian besar secara operasional, finansial, dan reputasi:

1. **Gangguan Operasional**

   Sistem yang diserang menjadi lumpuh, menyebabkan layanan penting tidak dapat berfungsi, terutama dalam organisasi besar atau sektor kritis seperti kesehatan, energi, atau pemerintahan. Contoh

dampak serupa adalah serangan terhadap Pelabuhan Nagoya di Jepang pada 2023, yang menghambat 10% perdagangan negara itu (Europol IOCTA, 2023).

2. **Kerugian Finansial**

   Biaya pemulihan dari serangan *ransomware* termasuk tebusan, kehilangan pendapatan, dan biaya teknis untuk memulihkan sistem. *ransomware* secara global diperkirakan menyebabkan kerugian sebesar $20 miliar pada 2023 (Accenture, 2023).

3. **Risiko Kebocoran Data**

   Ancaman publikasi data sering kali berdampak lebih besar daripada enkripsi itu sendiri. Kebocoran data dapat menyebabkan pelanggaran hukum privasi, kehilangan kepercayaan pelanggan, dan kerusakan reputasi organisasi (Europol IOCTA, 2023) (MIT, 2023).

2.1.5.3 Strategi Mitigasi dan Pencegahan

1. **Perbarui Perangkat Lunak Secara Berkala**

   Menutup celah keamanan dengan melakukan pembaruan rutin pada sistem operasi dan aplikasi adalah langkah penting untuk mencegah serangan berbasis eksploitasi kerentanan (Unit 42, 2023) (Accenture, 2023).

2. **Pelatihan Kesadaran Siber**

   Memberikan pelatihan kepada karyawan tentang ancaman *phishing* dan praktik terbaik keamanan siber membantu mengurangi risiko awal serangan (Europol IOCTA, 2023).

3. ***Backup* Data Secara Teratur**

   Membuat salinan data secara berkala dan menyimpannya di lokasi yang terisolasi dari jaringan utama dapat meminimalkan dampak serangan (MIT, 2023).

4. **Pemantauan Jaringan *Real-time***

   Menggunakan teknologi seperti *Intrusion Detection and Prevention Systems* (IDPS) untuk mendeteksi aktivitas mencurigakan secara

real-time membantu mempercepat respons terhadap ancaman (Accenture, 2023) (MIT, 2023).

2.1.6 Kerangka Kerja Keamanan Siber NIST

Kerangka Kerja Keamanan Siber NIST (*National Institute of Standards and Technology*) adalah kerangka kerja yang diakui secara luas dan diterapkan yang menyediakan pendekatan terstruktur dan proaktif untuk mengelola risiko keamanan siber. Dirancang untuk organisasi dari semua ukuran, kerangka kerja ini berfokus pada peningkatan postur keamanan siber melalui penilaian risiko, perencanaan, dan penerapan tindakan perlindungan. Kerangka kerja ini terstruktur di sekitar lima fungsi inti, yang menciptakan siklus peningkatan yang berkelanjutan: Identifikasi, Lindungi, Deteksi, Tanggap, dan Pulihkan.

1. **Identifikasi**

   Fungsi ini melibatkan pemahaman tentang aset-aset penting organisasi, potensi ancaman, dan kerentanan. Fungsi ini membantu memprioritaskan sumber daya untuk manajemen keamanan siber. Tindakan spesifik meliputi:

   - Inventarisasi dan klasifikasi aset.
   - Penilaian risiko dan identiikasi proses bisnis yang penting.
   - Menetapkan kebijakan keamanan siber organisasi (NIST, 2020) (Journal of Cybersecurity and Privacy Management, 2023).

   Contoh: Organisasi mengidentifikasi sistem dan data mana (misalnya, basis data *Cloud*, *platform* rantai pasokan) yang sangat penting untuk operasi dan paling berisiko terkena *ransomware*, seperti yang terlibat pada serangan global terhadap industri penting (WEF, 2023) (Accenture, 2024).

2. **Melindungi**

   Fungsi “Lindungi” berfokus pada penerapan perlindungan untuk membatasi dampak peristiwa keamanan siber. Langkah-langkahnya meliputi:

- Menerapkan *firewall*, enkripsi data, dan autentikasi multifactor.
- Menetapkan kontrol akses yang ketat dan pembaruan perangkat lunak secara teratur untuk mengurangi kerentanan.
- Mengadakan pelatihan karyawan untuk mengenali upaya *phishing* dan menghindari aktivitas berbahaya (WEF, 2023) (Accenture, 2024) (HealthTech, 2023).

Contoh: Melidungi kontrol akses yang kuat dalam operasi industri untuk mencegah pelanggaran *ransomware* seperti yang menargetkan sektor perawatan Kesehatan dan manufaktur pada tahun 2023 (Journal of Cybersecurity and Privacy Management, 2023) (HealthTech, 2023).

3. **Mendeteksi**

   Mendeteksi anomali atau potensi ancaman secara *real-time* sangatlah penting. Ini melibatkan:

   - Menerapkan Sistem Deteksi dan Pencegahan Intrusi (IDS/IPS) yang canggih.
   - Memantau aktivitas jaringan untuk mengetahui perilaku yang mencurigakan menggunakan *platform* intelijen ancaman berbasis AI.
   - Menyimpan catatan yang diperbarui untuk audit keamanan dan analisis forensik (WEF, 2023) (Journal of Cybersecurity and Privacy Management, 2023).

   Contoh: Sistem deteksi proaktif dapat mengurangi risiko yang ditimbulkan oleh serangan *ransomware* MGM Resorts pada tahun 2023 yang menyebabkan waktu henti operasional (Accenture, 2024).

4. **Menanggapi**

   Fungsi ini menekankan pada pengambilan tindakan segera untuk mengatasi dan menangani insiden keamanan siber. Langkah-langkah utamanya meliputi:

- Membentuk tim tanggap insiden dengan peran dan tanggung jawab yang jelas.
- Mengembangkan protokol komunikasi untuk menginformasikan pemangku kepentingan selama pelanggaran.
- Mengambil tindakan penahanan segera, seperti mengisolasi sistem yang terinfeksi (WEF, 2023) (Accenture, 2024).

Contoh: Organisasi yang terkena dampak serangan *ransomware*, seperti Medibank di Australia, mengurangi kerusakan lebih lanjut dengan mengisolasi *server* yang disusupi (Journal of Cybersecurity and Privacy Management, 2023) (HealthTech, 2023).

5. **Memulihkan**

Pemulihan berfokus pada pemulihan data dan layanan setelah kejadian keamanan siber. Hal ini meliputi:

- Mengembangkan rencana pemulihan bencana untuk memastikan kesinambungan.
- Menguji dan memvalidasi cadangan untuk pemulihan yang cepat.
- Belajar dari insiden untuk meningkatkan strategi respons di masa depan (NIST, 2020) (Accenture, 2024).

Contoh: Setelah serangan *ransomware Latitude Financial* tahun 2023, strategi pemulihan yang kuat memastikan gangguan minimal pada operasi keuangan (Accenture, 2024) (HealthTech, 2023).

2.1.6.1 Aplikasi dan Manfaat

(a) **Skabilitas:** Kerangka kerja ini diadaptasi untuk organisasi kecil dan perusahaan besar.

(b) **Standardisasi:** Selaras dengan standar global seperti ISO 27001 untuk manajemen keamanan siber.

(c) **Ketahanan:** Dengan berfokus pada deteksi proaktif, respons insiden, dan pemulihan bencana, organisasi meningkatkan kemampuan mereka untuk bertahan dan pulih dari serangan siber

(WEF, 2023) (Journal of Cybersecurity and Privacy Management, 2023) (Accenture, 2024).

2.1.6.2 Tantangan

a) **Biaya Implementasi:** Organisasi kecil sering kali kesulitan mengalokasikan anggaran untuk alat yang canggih.
b) **Faktor Manusia:** Kelalaian karyawan masih menjadi titik lemah dalam penerapan protokol keamanan.
c) **Evolusi Ancaman yang Cepat:** Pembaruan terus-menerus pada kerangka kerja diperlukan untuk mengatasi ancaman yang muncul seperti *ransomware-as-a-service* (Journal of Cybersecurity and Privacy Management, 2023) (HealthTech, 2023).

2.1.7 Kerangka Kerja MITRE ATT&CK

Kerangka Kerja MITRE ATT&CK adalah alat yang diakui secara global yang digunakan untuk memahami dan menganalisis taktik, teknik, dan prosedur (TTP) musuh, termasuk operator *ransomware* seperti *Lockbit* 3.0. Dikembangkan oleh MITRE *Corporation*, alat ini menyediakan taksonomi vektor serangan yang terperinci, sehingga memungkinkan organisasi untuk mengidentifikasi kerentanan, memperkuat pertahanan, dan membuat strategi untuk mitigasi ancaman.

2.1.7.1 Elemen Inti Kerangka Kerja ATT&CK MITRE

a) **Taktik dan Teknik**

Kerangka kerja ini mengkategorikan serangan ke dalam berbagai tahap, seperti Akses Awal, Eksekusi, Eskalasi Hak Istimewa, dan Eksfiltrasi.

- Untuk *ransomware* seperti *Lockbit* 3.0, teknik yang umum digunakan adalah mengeksploitasi kerentanan pada *Remote Desktop Protocol* (RDP) atau mengirimkan muatan berbahaya melalui *email phishing* (MITRE ATT&CK) (Journal of Cybersecurity Research and Practice, 2023).

- Teknik *Lockbit* yang spesifik termasuk penggunaan alat gerakan lateral otomatis untuk menyebar melalui jaringan dan mengenkripsi data (Unit 42, 2023) (Kaspersky, 2023).

b) **Pola Serangan *Lockbit* 3.0**

- **Pemerasan Ganda:** Mencuri dan mengenkripsi data sensitif untuk meminta uang tebusan sambil mengancam pemaparan public jika tuntutan tidak dipenuhi.
- **Teknik Anti-forensik:** Menonaktifkan *log* sistem dan menggunakan mekanisme enkripsi untuk menghindari deteksi.
- **Otomatisasi dalam Eksekusi:** *Lockbit* 3.0 memanfaatkan alat otomatis untuk tingkat infeksi yang lebih cepat dan kompromi sistem (Unit 42, 2023) (Kaspersky, 2023).

c) **Deteksi dan Respons**

Dengan memetakan serangan ke teknik MITRE ATT&CK, organisasi dapat mengidentifikasi:

- Indikator utama kompromi (IoC), seperti aktivitas *PowerShell* yang mencurigakan atau lalu lintas jaringan yang tidak normal.
- Strategi respons yang disesuaikan dengan tahapan *ransomware* tertentu, seperti mengisolasi titik akhir yang terinfeksi atau menganalisis *log* untuk akses data yang tidak sah (MITRE ATT&CK) (Accenture, 2024).

2.1.7.2 Aplikasi MITRE ATT&CK dalam Mempertahankan Diri dari *Lockbit* 3.0

a) **Perburuan Ancaman**

Dengan menggunakan kerangka kerja ini, tim keamanan siber dapat secara proaktif memburu aktivitas *ransomware* di dalam jaringan. Misalnya, mengidentifikasi penggunaan alat enkripsi yang tidak sah atau pola akses *file* yang tidak normal.

b) **Analisis Kesenjangan Keamanan**

Organisasi dapat menganalisis langkah-langkah keamanan yang ada terhadap katalog teknik MITRE, seperti mendeteksi kelemahan dalam keamanan *email* yang biasanya dieksploitasu oleh *Lockbit* untuk akses awal (MITRE ATT&CK) (Accenture, 2024).

c) **Perencanaan Respons Insiden**

MITRE ATT&CK membantu dalam menyusun protokol respons insiden dengan menyediakan rincian langkah demi langkah dari scenario serangan potensial. Hal ini memastikan respons yang lebih cepat dan lebih terkoordinasi terhadap insiden *ransomware* (Unit 42, 2023).

2.1.7.3 Manfaat Utama

- **Pemahaman Ancaman yang Komprehensif:** Kerangka kerja ini memberikan wawasan tentang metode serangan, sehingga memungkinkan tindakan pertahanan yang lebih efektif.
- **Komunikasi Terstandarisasi:** Tim keamanan di berbagai organisasi dapat berkolaborasi menggunakan bahasa yang sama untuk TTP.
- **Pertahanan Proaktif:** Mengidentifikasi dan mengatasi kerentanan sebelum serangan terjadi secara signifikan mengurangi eksposur risiko (Journal of Cybersecurity Research and Practice, 2023) (Kaspersky, 2023).

2.1.7.4 Tantangan dalam Implementasi

- **Kompleksitas:** Sifat MITRE ATT&CK yang mendetail dapat membebani organisasi dengan keahlian keamanan siber yang terbatas.
- **Ancaman yang Berkembang dengan Cepat:** Kelompok-kelompok *ransomware* seperti *Lockbit* 3.0 terus memperbarui metode mereka, sehingga membutuhkan pembaruan terus menerus untuk strategi pertahanan (Unit 42, 2023) (Kaspersky, 2023).

2.1.8 Analisis *Malware* (Statis dan Dinamis)

Analisis *Malware* adalah proses sistematis untuk memahami cara kerja *Malware*, termasuk *ransomware* seperti *Lockbit* 3.0. Pendekatan ini membantu mengidentifikasi mekanisme serangan, pola perilaku, dan potensi mitigasi. Analisis *Malware* terdiri dari dua jenis utama: analisis statis dan analisis dinamis. Keduanya memainkan peran penting dalam mengembangkan pertahanan yang efektif terhadap serangan siber.

1. **Analisis Statis**

   Analisis statis melibatkan pemeriksaan *Malware* tanpa menjalankannya, sehingga aman untuk menganalisis struktur *file* dan kodenya. Tujuannya adalah untuk memahami karakteristik dan potensi anacaman dari *Malware*. Beberapa metode yang digunakan:

   a. **Dekompilasi Kode:** Menggunakan alat seperti IDA Pro atau Ghidra untuk membongkar kode biner dan mengubahnya menjadi representasi yang lebih mudah dipahami, seperti *assembly*. Ini membantu mengidentifikasi algoritma enkripsi yang digunakan oleh *ransomware* seperti *Lockbit* 3.0.

   b. **Pemeriksaan String:** Analisis string dalam *Malware* sering mengungkapkan detail penting, seperti pesan tebusan, URL *server Command and Control* (C2), atau parameter enkripsi.

   c. **Analisis Metadata *File*:** Memeriksa header *file* dan struktur *file* untuk informasi tambahan, termasuk versi *Malware* dan kerentanannya terhadap sistem tertentu (Sikorski & Honig, 2021) (Guven, 2024).

   Keunggulan analisis statis adalah keamanannya karena *Malware* tidak dieksekusi. Namun, teknik ini terbatas jika *ransomware* menggunakan mekanisme *obfuscation* atau enkripsi yang kompleks untuk menyembunyikan kodenya (Sikorski & Honig, 2021).

2. **Analisis Dinamis**

   Analisis dinamis melibatkan eksekusi *Malware* di lingkungan terkendali, seperti *sandbox*, untuk mengamati perilaku aktualnya.

Teknik ini penting untuk memahami interaksi *Malware* dengan sistem, termasuk:

a. **Perubahan Sistem *File*:** Memantau *file* yang diubah, dihapus, atau dienkripsi oleh *ransomware*. *Lockbit* 3.0, misalnya, dikenal karena enkripsi cepatnya terhadap *file* penting.
b. **Pemantauan Lalu Lintas Jaringan:** Mengidentifikasi komunikasi dengan *server* C2, yang sering digunakan untuk menerima perintah tambahan atau mengunggah data curian.
c. **Perilaku Proses:** Observasi terhadap proses *Malware*, seperti penciptaan layanan baru atau manipulasi registry, yang merupakan langkah khas *ransomware* dalam menyerang sistem target (Guven, 2024) (Kaspersky, 2023).

Keunggulan analisis dinamis adalah kemampuannya untuk mengungkap perilaku tersembunyi yang tidak terlihat dalam analisis statis. Namun, ini memerlukan lingkungan yang sangat aman agar *Malware* tidak melarikan diri dan menyerang sistem eksternal (Guven, 2024).

2.1.8.1 Manfaat Analisis *Malware* dalam Menangani *Lockbit* 3.0

(a) **Identifikasi Indikator Ancaman:** Menentukan indicator kompromi (IoC) yang spesifik untuk *ransomware*, seperti pola enkripsi atau domain C2.
(b) **Pengembangan Antivirus:** Informasi dari analisis membantu menciptakan tanda tangan (*signatures*) untuk deteksi dan pencegahan.
(c) **Penguatan Pertahanan:** Menyediakan wawasan tentang cara *ransomware* mengeksploitasi kerentanan, memungkinkan organisasi untuk memperbaiki celah keamanan di jaringan mereka.

2.1.8.2 Tantangan dalam Analisis *Malware*

(a) **Teknologi Anti-Analisis:** *ransomware* seperti *Lockbit* 3.0 sering kali menggunakan teknik *anti-debugging* dan *anti-sandboxing* untuk menghindari deteksi.

(b) **Kompleksitas *Malware*:** *Envolving techniques, such as polymorphism* (kode yang terus berubah), membuat analisis menjadi lebih sulit (Kaspersky, 2023) (Accenture, 2024).

2.1.9 Kerangan Resiliensi Siber (*Cyber Resilience Framework)*

Kerangka Resiliensi Siber (*Cyber Resilience Framework*) adalah pendekatan komprehensif untuk memastikan bahwa sistem digital dapat bertahan, beradaptasi, dan pulih dari ancaman siber, termasuk *ransomware*. Kerangka ini tidak hanya mencakup pencegahan ancaman, tetapi juga menekankan kesiapan operasional, kemampuan pemulihan, dan pembelajaran dari insiden sebelumnya untuk meningkatkan ketahanan sistem secara berkelanjutan. Dalam konteks *ransomware*, kerangka ini menjadi landasan penting bagi organisasi, terutama Infrastruktur Informasi Vital (IIV), untuk tetap operasional di tengah ancaman.

2.1.9.1 Komponen Utama Kerangka Resiliensi Siber

a) **Perencanaan Pemulihan Bencana (*Disaster Recovery Planning*)**
Perencanaan pemulihan bencana adalah elemen penting dalam resiliensi siber. Hal ini mencakup strategi untuk memulihkan data yang hilang atau terenkripsi akibat *ransomware*. Organisasi yang tangguh biasanya memiliki:
   - Cadangan data berkala di lokasi terisolasi.
   - Prosedur pemulihan cepat, termasuk penggunaan *disaster recovery sites* dan infrastruktur cadangan untuk meminimalkan waktu henti operasional.
   - Studi oleh *World Economic Forum* (2022) menekankan bahwa 70% organisasi yang berhasil memulihkan operasi dari serangan *ransomware* memiliki sistem cadangan yang kuat (WEF, 2022).

b) **Simulasi Serangan Siber (*Cybersecurity Simulations*)**
Kerangka resiliensi siber mengintegrasikan simulasi serangan rutin untuk menguji kesiapan sistem dan tim keamanan. Simulasi ini melibatkan:

- Penilaian terhadap respons tim saat menghadapi serangan *phishing* atau eksploitasi kerentanan perangkat lunak.
- Identifikasi kelemahan dalam protokol deteksi dan mitigasi ancaman (Journal of Cybersecurity Education, Research, and Practice, 2023) (NIST, 2023).

(c) **Koordinasi Lintas Lembaga dan Kolaborasi Global**

Kerangka ini menekankan pentingnya kolaborasi antarinstansi pemerintah, sektor swasta, dan organisasi internasional. Contohnya adalah operasi internasional seperti "*Operation Cronos*" yang melibatkan Europol dan FBI dalam melumpuhkan jaringan *ransomware* pada tahun 2024. Kolaborasi semacam ini mempercepat pertukaran informasi intelijen dan mempermudah respons kolektif terhadap ancaman global (Europol IOCTA, 2023) (NIST, 2023).

(d) **Kesadaran dan Pelatihan Siber**

Peningkatan kesadaran keamanan siber di tingkat individu dan organisasi adalah langkah kunci dalam kerangka ini. Pelatihan rutin, terutama untuk mendeteksi *email phishing*, membantu mengurangi risiko serangan awal yang biasanya menjadi pintu masuk *ransomware* seperti *Lockbit* 3.0 (NIST, 2023)

2.1.9.2 Manfaat Kerangka Resiliensi dalam Menghadapi *ransomware*

1. **Mengurangi Waktu Pemulihan**

   Dengan memiliki rencana pemulihan yang jelas, organisasi dapat memulihkan data dan layanan dalam waktu singkat, sehingga dampak serangan *ransomware* dapat diminimalkan.

2. **Meningkatkan Kepercayaan Publik**

   Implementasi kerangka resiliensi siber menunjukkan bahwa organisasi siap menghadapi ancaman, yang dapat meningkatkan kepercayaan masyarakat dan pelanggan terhadap keamanan data mereka.

3. **Mencegah Gangguan Operasional Jangka Panjang**

   Kerangka ini membantu memastikan keberlangsungan layanan penting, terutama dalam sektor kritis seperti kesehatan, energi, dan pemerintahan.

2.1.9.3 Tantangan dalam Implementasi Kerangka Resiliensi Siber

(1) **Keterbatasan Anggaran dan Sumber Daya**

Tidak semua organisasi memiliki kapasitas finansial untuk mengadopsi teknologi deteksi lanjutan atau membangun infrastruktur cadangan yang memadai (WEF, 2022) (NIST, 2023).

(2) **Evolusi Cepat Ancaman Siber**

Ancaman seperti *Lockbit* 3.0 terus berkembang, sehingga memerlukan pembaruan kerangka secara berkala untuk tetap relevan dan efektif.

(3) **Kurangnya Kesadaran Siber di Tingkat Individu**

Faktor manusia tetap menjadi titik lemah utama dalam keamanan siber, terutama dalam mendeteksi ancaman seperti *email phishing* (NIST, 2023).

2.1.10 *Disaster Recovery dan Business Continuity*

Disaster Recovery (DR) dan *Business Continuity* (BC) adalah strategi utama yang dirancang untuk memastikan kelangsungan operasional organisasi setelah serangan siber, termasuk *ransomware*. Dengan implementasi yang tepat, pendekatan ini dapat mengurangi dampak serangan, mempercepat pemulihan, dan menjaga integritas layanan kritis.

2.1.10.1 Komponen Utama dalam DR dan BC

1. **Pencadangan Data Berkala (*Regular Data Backups)***

   Pencadangan data yang teratur adalah langkah mendasar dalam DR. Organisasi harus memastikan bahwa:

   - Data disimpan di lokasi terpisah (*off-site*) atau menggunakan solusi berbasis *Cloud* yang aman.

- Cadangan dienkripsi untuk melindungi informasi dari kebocoran selama pemindahan atau penyimpanan.
- Pengujian pemulihan cadangan dilakukan secara berkala untuk memastikan keandalan data (Patel, 2024) (Accenture, 2023).

2. **Rencana Pemulihan Bencana (*Disaster Recovery Plan*)**
   Rencana ini mencakup langkah-langkah sistematis untuk memulihkan sistem, aplikasi, dan data setelah serangan *ransomware*. Beberapa elemen penting meliputi:
   - Identifikasi aset-aset kritis yang harus diprioritaskan dalam pemulihan.
   - Pemanfaatan pusat pemulihan bencana (*disaster recovery sites*), baik berbasis *Cloud* maupun fisik.
   - Pengaturan prosedur isolasi dan pembersihan sistem yang terinfeksi (NIST, 2022) (Accenture, 2023).
3. **Latihan Simulasi Insiden (*Incident Simulations*)**
   Latihan ini dilakukan untuk menguji kesiapan organisasi dalam menghadapi insiden siber. Simulasi membantu tim keamanan siber:
   - Memperbaiki kelemahan dalam rencana DR dan BC.
   - Mengembangkan respons yang lebih cepat dan terkoordinasi selama serangan.
   - Melatih staf untuk mendeteksi tanda-tanda awal *ransomware* seperti *Lockbit* 3.0 (Patel, 2024).

2.1.10.2 Manfaat Implementasi DR dan BC

(1) **Mengurangi *Downtime* Operasional:** Dengan rencana pemulihan yang matang, organisasi dapat meminimalkan waktu henti layanan publik atau operasional bisnis.

(2) **Meningkatkan Kepercayaan *Stakeholder*:** Implementasi BC menunjukkan kesiapan organisasi untuk melindungi data pelanggan dan memastikan layanan tetap berjalan meskipun terjadi serangan.

(3) **Mengurangi Kerugian Finansial:** Strategi DR yang baik mengurangi biaya pemulihan dari serangan *ransomware* dan potensi kerugian akibat hilangnya pendapatan atau denda hukum (NIST, 2022) (Accenture, 2023).

2.1.10.3 Tantangan dalam Pelaksanaan

(a) **Keterbatasan Sumber Daya:** Banyak organisasi, khususnya yang kecil, mungkin kekurangan anggaran atau tenaga ahli untuk mengimplementasikan solusi DR dan BC yang komprehensif.

(b) **Kerumitan Teknologi:** Mengintegrasikan solusi berbasis *Cloud* dan otomatisasi dalam strategi BC memerlukan pengetahuan teknis yang mendalam.

(c) **Evolusi Ancaman Siber:** Ancaman seperti *Lockbit* 3.0 terus berkembang, sehingga strategi DR dan BC harus diperbarui secara berkala (Patel, 2024).

2.2 Hasil Penelitian Terdahulu

Hasil penelitian terdahulu merupakan rangkuman dan analisis dari berbagai penelitian atau literatur yang relevan dengan topik atau permasalahan yang berkaitan dengan penelitian ini. Tujuannya adalah untuk menyediakan dasar pengetahuan yang kuat dan konteks untuk penelitian yang sedang dilakukan. Adapun beberapa penelitian terdahulu yang dijadikan rujukan dan dasar pemikiran pada penelitian ini yaitu:

Tabel 2. 1 Penelitian Terdahulu

No	Penulis	Judul	Metode dan Hasil	Relevansi	Perbedaan
1.	Hull, G., et al., 2019	*ransomware Deployment Methods and Analysis*	Penelitian ini membahas metode penyebaran *ransomware*, seperti eksploitasi kerentanan sistem dan *phishing email*, dengan fokus pada pola teknis serangan untuk mendukung upaya mitigasi.	Fokus pada pola serangan *ransomware* secara teknis.	Membahas *ransomware* secara umum, tidak hanya *Lockbit* 3.0.

2.	Ahmed, M., et al., 2024	*AI-Based ransomware Detection: A Comprehensive Review*	Artikel ini membahas penerapan AI dan teknik pembelajaran mesin untuk mendeteksi *ransomware* modern dan meningkatkan respons terhadap ancaman.	Membahas *ransomware* modern termasuk *Lockbit* 3.0.	Berfokus pada penerapan AI, tidak pada dampak spesifik pada IIV atau PDNS.
3.	Gupta, S. & Tripathi, R., 2021	*Systematic Literature Review on ransomware Detection*	Studi ini mengevaluasi strategi deteksi *ransomware*, membandingkan metode berbasis tanda tangan dan analitik perilaku untuk menentukan pendekatan paling efektif.	Meninjau strategi deteksi *ransomware*.	Fokus pada deteksi, bukan mitigasi atau pemulihan.
4.	Zhou, L., et al., 2022	*ransomware Prevention and Mitigation Techniques*	Penelitian ini mengkaji pencegahan dan mitigasi *ransomware* melalui studi kasus, menyoroti teknik seperti *backup* data dan kontrol akses.	Menganalisis langkah mitigasi *ransomware* termasuk pemulihan bencana.	Membahas mitigasi *ransomware* secara umum tanpa studi kasus khusus.
5.	Smith, R., et al., 2020	*Dynamic Analysis of ransomware Attacks*	Artikel ini menganalisis *ransomware* dengan *sandbox*, memantau perilaku seperti enkripsi *file* dan komunikasi dengan *server* C2.	Fokus pada teknik serangan *ransomware* yang kompleks.	Tidak membahas kerangka mitigasi atau respons berbasis kebijakan seperti di Indonesia.
6.	Yang, J., et al., 2023	*The Evolution of Double extortion in ransomware Attacks*	Studi ini membahas strategi *double extortion ransomware*, yang mengancam publikasi data dan enkripsi, serta dampaknya pada finansial dan reputasi korban.	Membahas strategi "*double extortion*" *ransomware* termasuk *Lockbit* 3.0.	Berfokus pada teknik serangan tanpa analisis dampak pada sistem pemerintah seperti PDNS.
7.	Perez, A. & Li, C., 2024	*Impact of ransomware on Cloud-Based Data Centers*	Penelitian ini mengkaji dampak *ransomware* dan kerentanan pada infrastruktur *Cloud* serta pentingnya keamanan	Fokus pada dampak *ransomware* terhadap pusat	Tidak mencakup kerangka kerja mitigasi atau strategi pemulihan di tingkat nasional.

			untuk melindungi data strategis.	data berbasis *Cloud*.	
8.	Jones, D., et al., 2023	*Business Continuity in the Age of ransomware*	Artikel ini membahas strategi keberlangsungan bisnis untuk menghadapi *ransomware*, dengan fokus pada perencanaan pemulihan dan simulasi insiden.	Membahas strategi keberlangsungan bisnis setelah serangan *ransomware*.	Fokus lebih pada dunia bisnis daripada infrastruktur vital nasional seperti PDNS.
9.	Ahmad, F., et al., 2023	*Lockbit 3.0 and Advanced ransomware Techniques*	Penelitian ini menganalisis teknik canggih *Lockbit* 3.0, seperti automasi dan enkripsi cepat, untuk memahami penyebarannya di jaringan.	Fokus pada teknik enkripsi dan penyebaran otomatis *Lockbit* 3.0.	Tidak mencakup evaluasi dampak di sektor publik atau rekomendasi kebijakan mitigasi.
10.	Miller, P., et al., 2022	*ransomware Impact on Critical Infrastructure*	Artikel ini membahas dampak *ransomware* pada infrastruktur kritis dan pentingnya kerja sama internasional serta kebijakan mitigasi.	Membahas dampak *ransomware* pada sektor penting, termasuk energi dan transportasi.	Tidak membahas kerangka mitigasi berbasis kebijakan keamanan siber nasional seperti RAN Kamsiber.

Dalam menjelaskan hasil penelitian terdahulu dapat saya narasikan sebagai berikut:

1. Pada penelitian Hull, G., et al. (2019) ini mengulas metode penyebaran *ransomware*, termasuk melalui *phishing email* dan eksploitasi kerentanan sistem. Fokus utama adalah pada pola serangan teknis yang umum digunakan oleh berbagai varian *ransomware*. Analisis ini memberikan wawasan tentang bagaimana *ransomware* dapat menyebar dengan cepat melalui jaringan, menyoroti pentingnya deteksi dini untuk mitigasi serangan.
2. Ahmed, M., et al. (2024) membahas penerapan kecerdasan buatan (AI) dalam mendeteksi *ransomware* modern, termasuk *Lockbit* 3.0. Dengan meninjau berbagai model AI, studi ini menunjukkan

bagaimana teknik pembelajaran mesin dapat meningkatkan deteksi ancaman dan mengurangi respons waktu terhadap serangan. Penelitian ini menyoroti AI sebagai alat penting untuk melawan *ransomware* yang semakin canggih.

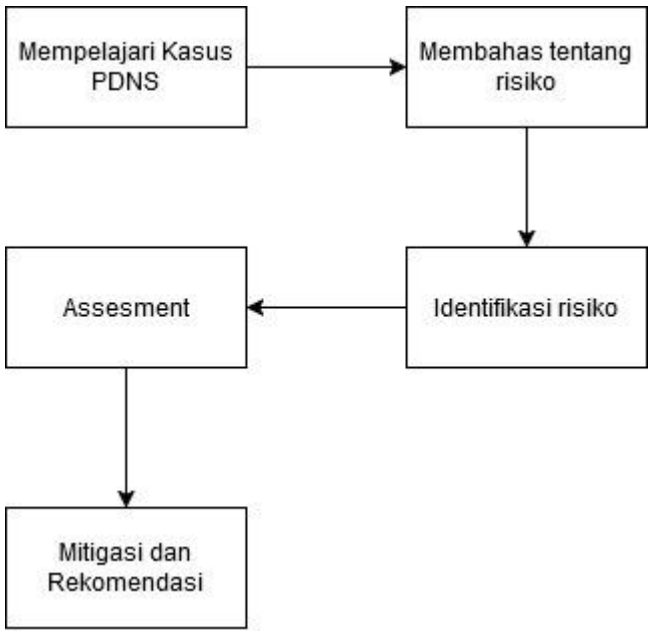
3. Gupta, S. & Tripathi, R. (2021) membahas strategi deteksi *ransomware* menggunakan teknik analitik data. Fokusnya adalah pada pendekatan berbasis tanda tangan (*signature-based*) dan analitik perilaku (*behavioral analytics*), menawarkan evaluasi komprehensif tentang metode yang paling efektif untuk mendeteksi ancaman *ransomware*.
4. Penelitian Zhou, L., et al. (2022) menganalisis berbagai teknik pencegahan dan mitigasi *ransomware*, seperti *backup* data, kontrol akses ketat, dan *firewall* berbasis aturan. Studi kasus dalam penelitian ini memperlihatkan bagaimana strategi mitigasi dapat diterapkan untuk meminimalkan dampak serangan *ransomware*.
5. Smith, R., et al. (2020) mengeksplorasi analisis dinamis *ransomware* dengan memanfaatkan lingkungan *sandbox*. Penelitian ini mendokumentasikan bagaimana *ransomware* memanipulasi *registry*, enkripsi *file*, dan mengkomunikasikan data ke *server Command and Control* (C2), memberikan wawasan tentang perilaku aktual *Malware*.
6. Penelitian oleh Yang, J., et al. (2023) berfokus pada evolusi strategi *double extortion*, dimana *ransomware* seperti *Lockbit* 3.0 tidak hanya mengenkripsi data tetapi juga mencuri informasi sensitif untuk meningkatkan tekanan pada korban. Penelitian ini menggambarkan bagaimana metode ini menargetkan organisasi besar dengan konsekuensi serius pada keuangan dan reputasi.
7. Perez, A. & Li, C. (2024) mengeksplorasi dampak *ransomware* terhadap pusat data berbasis *Cloud*. Studi kasus menunjukkan bagaimana infrastruktur *Cloud* yang tidak dilindungi dengan baik rentan terhadap serangan *ransomware*, dengan penekanan pada

pentingnya arsitektur keamanan berbasis *Cloud* untuk melindungi data sensitif.

8. Penelitian oleh Jones, D., et al. (2023) membahas strategi *Business Continuity (BC)* untuk mengatasi gangguan operasional akibat *ransomware*. Penelitian ini menyoroti pentingnya perencanaan pemulihan bencana, cadangan data reguler, dan simulasi insiden dalam menjaga kelangsungan operasional bisnis pasca-serangan.
9. Penelitian yang dilakukan Ahmad, F., et al. (2023) menganalisis teknik canggih *Lockbit* 3.0, termasuk algoritma enkripsi cepat dan teknik anti-forensik. Studi ini memberikan wawasan tentang bagaimana *ransomware* memanfaatkan automasi untuk mempercepat penyebaran di jaringan korban.
10. Miller, P., et al. (2022) menyoroti dampak *ransomware* pada infrastruktur kritis, termasuk sektor energi dan transportasi. Penelitian ini menyarankan strategi mitigasi berbasis kebijakan dan kerja sama internasional untuk meningkatkan ketahanan terhadap serangan *ransomware*.

2.3 Kerangka Pemikiran

Kerangka pemikiran adalah elemen esensial dalam penelitian ilmiah yang berfungsi sebagai pedoman dalam merumuskan pemahaman awal mengenal masalah penelitian. Kerangka ini dibangun berdasarkan hasil tinjauan pustaka serta penelitian terdahulu yang relevan, yang memberikan dasar teori dan konsep untuk mendukung penelitian yang dilakukan. Melalui kerangka pemikiran, peneliti dapat menegaskan hubungan antara variabel-variabel yang diteliti, baik variabel *independent*, dependen, maupun variabel kontekstual.



Gambar 2. 1 Kerangka Pemikiran

Kerangka pemikiran ini dirancang untuk memahami dan menganalisis dampak serangan *ransomware Lockbit* 3.0 terhadap Pusat Data Nasional Sementara (PDNS) dan Infrastruktur Informasi Vital (IIV). Setiap tahapan dalam diagram memiliki keterkaitan logis yang mendukung proses penelitian ini, sebagai berikut:

1. **Mempelajari Kasus PDNS**

   Penelitian dimulai dengan mengkaji secara mendalam kasus serangan *ransomware Lockbit* 3.0 terhadap Pusat Data Nasional Sementara. Tahapan ini bertujuan untuk memahami konteks kejadian, skala serangan, serta sistem yang terdampak. Studi ini didukung oleh data primer dan sekunder yang relevan, seperti laporan insiden dan analisis teknis.

2. **Membahas Tentang Risiko**

   Setelah memahami kasus PDNS, penelitian bergerak untuk mendiskusikan risiko yang muncul akibat serangan *ransomware*, baik terhadap aspek keamanan data, layanan publik, maupun kedaulatan digital Indonesia. Tahapan ini berfokus pada dampak langsung dan tidak langsung terhadap IIV.

3. **Identifikasi Risiko**

   Pada tahap ini, dilakukan identifikasi risiko terkait kerentanan sistem yang dieksploitasi dalam serangan *ransomware*. Fokus utamanya mencakup metode serangan, celah keamanan, serta teknik yang digunakan oleh *Lockbit* 3.0 (seperti *double extortion*). Hasil identifikasi ini menjadi dasar dalam mengukur sejauh mana sistem memiliki kesiapan terhadap ancaman serupa.

4. ***Assessment***

   Selanjutnya, dilakukan penilaian (*assessment*) menyeluruh terhadap hasil identifikasi risiko. Proses ini bertujuan untuk mengevaluasi dampak serangan, efisiensi mitigasi yang sudah ada, serta kelemahan dalam sistem keamanan PDNS dan IIV.

5. **Mitigasi dan Rekomendasi**

   Berdasarkan hasil *assessment*, tahapan terakhir adalah merumuskan langkah-langkah mitigasi dan rekomendasi strategis. Mitigasi ini mencakup penerapan kerangka kerja keamanan, seperti *NIST Cybersecurity Framework* atau *MITRE ATT&CK*, peningkatan ketahanan digital, pelatihan rutin, serta penguatan kebijakan keamanan siber. Rekomendasi ini diharapkan dapat meningkatkan kesiapsiagaan, respons, dan pemulihan dalam menghadapi serangan *ransomware* di masa mendatang.

Dengan pendekatan ini, penelitian memberikan gambaran yang komprehensif tentang dampak serangan *ransomware* terhadap infrastruktur kritis di Indonesia serta solusi yang dapat diimplementasikan untuk meningkatkan ketahanan siber nasional.