BAB 1
PENDAHULUAN

A. LATAR BELAKANG

Indonesia tengah memasuki era revolusi industri 4.0, ditandai dengan pesatnya perkembangan teknologi informasi dan komunikasi, termasuk kecerdasan buatan (AI) dan internet of things (IoT). Hal ini direspons pemerintah melalui Peraturan Presiden Nomor 95 Tahun 2018, yang membentuk komite pengarah untuk memimpin transformasi digital dan meningkatkan daya saing Indonesia. Pemanfaatan internet yang meluas, dengan jumlah pengguna mencapai 202,6 juta pada awal 2021 (meningkat 16% dari tahun sebelumnya), menunjukkan ketergantungan yang tinggi terhadap teknologi. Namun, perkembangan ini juga membuka peluang kejahatan siber (*cybercrime*), yang meliputi pencurian data, serangan sistem komputer, penyebaran *malware*, dan berbagai bentuk kejahatan daring lainnya(Haryanto & Sutra, 2023).

Pelaku *cybercrime* beragam, mulai dari individu hingga entitas negara, yang menggunakan berbagai teknik seperti *phishing* dan *ransomware* untuk mencapai tujuan mereka. Dampak dari kejahatan siber adalah hilangnya data sensitif yakni pencurian identitas sehingga dapat menyebabkan kerugian finansial, gangguan operasional sistem, hingga merusak reputasi pribadi seseorang atau perusahaan. Negara di kawasan ASEAN dieksploitasi sebagai target serangan siber karena ketahanan siber dan tingkat proteksivitasnya masih rendah(Astarini & Rofii, 2021). Maka dari itu dibentuklah Badan Siber dan Sandi Negara melalui Perpres No. 53 Tahun 2017. BSSN memiliki peran strategis dalam mengarahkan kebijakan keamanan siber nasional, menanggulangi ancaman keamanan siber, dan melindungi infrastruktur informasi penting negara.

Menurut data dari BSSN, pada tahun 2018 negara Indonesia adalah negara kedua terbanyak yang memiliki kasus serangan siber di dunia setelah China dengan dengan jumlah serangan sebanyak 225,9 juta(Pratama, 2020). *Ransomware* merupakan ancaman serius di wilayah negara ASEAN dengan merujuk pada data statistik Kaspersky, pada laporan *Interpol Cyber Assessment Report* 2021 sekitar 2,7 juta kasus

ransomware terdeteksi di wilayah negara ASEAN selama tiga kuartal pertamatahun 2020. Di antara negara-negara yang ada di wilayah ASEAN, Indonesia adalah negara terbanyak dengan 1,3 juta kasus serangan siber, atau mencakup hampir setengah dari keseluruhan kasus yang terdeteksi(Tan et al., 2021).

Maraknya kasus *cybercrime* di negara Indonesia dikarenakan banyaknya perangkat yang terhubung ke internet (*Internet of Things*) rentan menjadi korban kejahatan siber. Kurangnya *patching* sistem keamanan, dan kelemahan dalam implementasi kebijakan keamanan siber menjadi pemicu terjadinya kejahatan siber. Keterbatasan jumlah ahli keamanan siber yang terampil dan terlatih dapat memperburuk situasi keamanan siber di Indonesia, mengingat kebutuhan akan tenaga ahli keamanan siber yang handal semakin meningkat(Pratama, 2020). Sejauh ini belum ada satupun peraturan resmi yang mengatur tindak *cyber security* di negara Indonesia karena kejahatan siber ini memiliki komplektivitas yang tinggi sehingga seringkali mencakup aspek-aspek teknis dan spesifik, oleh karena itu penegak hukum harus memiliki keahlian khusus dalam bidang teknologi informasi dan komunikasi. Sampai sekarang persoalan tentang kejahatan siber ini masih diatur oleh beberapa peraturan tentang dunia maya seperti UU ITE No. 19 Tahun 2016, tentang perlindungan data pribadi pengguna layanan elektronik, termasuk tata cara pengumpulan, penggunaan, penyebaran, dan penyimpanan data(Firdaus, 2024).

Implementasi *e-government* di Indonesia, meski meningkatkan efisiensi pelayanan publik, juga menimbulkan tantangan keamanan informasi yang serius. Ancaman kebocoran data oleh pelaku kejahatan siber menjadi masalah mendesak. Keamanan informasi, yang mencakup kerahasiaan, keutuhan, dan ketersediaan data, sangat penting untuk kelangsungan bisnis dan pengurangan risiko. Selain Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), regulasi lain seperti Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022 dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Sistem dan Transaksi Elektronik, mendukung upaya pengamanan data dan informasi di Indonesia.

Untuk menangani permasalahan khusus di ruang siber maka dibentuklah Badan Siber dan Sandi Negara di tahun 2017 melalui Perpres No. 53 Tahun 2017. Tahun 2019 BSSN berhasil mendirikan *National Security Operation Center* (NSOC) kemudian pada tahun 2020 Indonesia berhasil membuat *Government Cyber Security Incident Response Team* (Gov-CSIRT) dengan maksud untuk mendeteksi atau merespon kejadian di dalam lingkungan pemerintah baik di lingkungan pusat maupun daerah(Dahlan, 2023). Data Badan Siber dan Sandi Negara (BSSN) menunjukkan peningkatan drastis serangan siber di Indonesia, hampir lima kali lipat antara Januari hingga Juli 2019, mencapai 39,3 juta kasus(Tan et al., 2021). Laporan tahunan Gov-CSIRT tahun 2019 mencatat 105 insiden, dengan mayoritas (63%) berupa kerentanan sistem, diikuti oleh *web defacement* (14%), *phishing* (9%), dan *malware* (9%).

Serangan siber seringkali menargetkan instansi pemerintah hal ini menandakan bahwa instansi pemerintah Indonesia masih rentan terhadap serangan siber dan hal tersebut merupakan ancaman bagi negara Indonesia(M. Yusuf Samad, 2022). Dalam konteks ini, peran CSIRT sangat penting dalam upaya penanggulangan serta mitigasi serangan siber yang dapat merugikan keberlangsungan operasional pemerintahan. Tugas CSIRT adalah mendeteksi secara aktif dan melakukan pemantauan kontinu terhadap keamanan komputer serta jaringan untuk mengidentifikasi adanya ancaman yang berpotensi menjadi insiden serangan. Memberi respon secara cepat terhadap suatu insiden siber yang teridentifikasi bahaya untuk meminimalisir dampak dan memulihkan sistem yang terpengaruh(Prabaswari et al., 2022).

Sesuai Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara, Badan Intelijen Negara (BIN) berperan mendeteksi berbagai ancaman terhadap keamanan nasional, termasuk serangan siber. BIN melaksanakan deteksi ancaman siber, antara lain, melalui layanan *Security Assessment* yang disediakan oleh Deputi Bidang Intelijen Siber.

Di Kabupaten Ponorogo sendiri, *web defacement* merupakan salah satu jenis serangan siber yang paling sering terjadi, mengancam integritas dan keamanan data pemerintahan. Hal ini menunjukkan lemahnya sistem keamanan

siber di beberapa instansi pemerintahan Kabupaten Ponorogo. Hal ini dapat disebabkan oleh berbagai faktor, antara lain kurangnya kesadaran akan keamanan siber, kekurangan pelatihan dan pemahaman teknis bagi para pengelola sistem informasi, serta keterbatasan sumber daya dan infrastruktur keamanan siber yang memadai. Dampak dari serangan *web defacement* sangat merugikan, mulai dari kerusakan reputasi pemerintah daerah, gangguan pelayanan publik, hingga potensi kebocoran data penting. Untuk mengatasi permasalahan ini, Pemerintah Kabupaten Ponorogo telah membentuk Tim Tanggap Insiden Siber (CSIRT) berdasarkan Surat Keputusan Bupati Nomor: 188.45/1148/405.19/2022(SK CSIRT, 2022).

Peluncuran Ponorogo CSIRT dilakukan pada 25 Oktober 2023 oleh Bambang Suhendro Asisten I Bidang Pemerintahan dan Kesra Sekretariat Daerah Kabupaten Ponorogo, sejalan dengan Peraturan Bupati Ponorogo Nomor 71 Tahun 2023 tentang penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE). Pembentukan CSIRT ini merupakan langkah strategis dalam upaya meningkatkan keamanan siber dan menanggulangi serangan siber, termasuk *web defacement*. Namun, efektivitas peran CSIRT dalam menanggulangi serangan siber di Kabupaten Ponorogo masih perlu dikaji lebih lanjut.

Berdasarkan latar tersebut, maka sangat menarik untuk meneliti lebih dalam terkait dengan peran CSIRT dalam menanggulangi kasus serangan siber di lingkup Pemerintahan Kabupaten Ponorogo. Dengan menganalisis peran CSIRT dalam penanggulangan serangan siber, penelitian ini dapat memperkaya pemahaman teoritis tentang strategi dan taktik yang efektif dalam melindungi infrastruktur informasi pemerintahan dari ancaman siber(Rachmanu Krisnata et al., 2022). Dengan memahami bagaimana CSIRT beroperasi dan berkolaborasi dengan entitas terkait dalam penanggulangan serangan siber, penelitian ini bisa memberikan kontribusi dan wawasan yang lebih baik terkait pentingnya keberadaan CSIRT dalam menjaga keamanan informasi pemerintahan(Firmansyah & Yuswanto, 2022).

B. RUMUSAN MASALAH

Ponorogo, salah satu entitas pemerintahan di Indonesia yang pastinya tidak luput dari risiko serangan siber yang dapat mengganggu integritas, kerahasiaan, dan ketersediaan data penting pemerintah.

Maka rumusan masalah dari penelitian ini adalah “Bagaimana peran CSIRT dalam menanggulangi kasus serangan siber di lingkup Pemerintahan Kabupaten Ponorogo?”

C. TUJUAN PENELITIAN

Penelitian ini bertujuan untuk menganalisis peran CSIRT dalam penanggulangan serangan siber khususnya *web defacement*, di lingkungan Pemerintah Kabupaten Ponorogo.

.

D. MANFAAT PENELITIAN

Manfaat suatu penelitian merujuk pada kontribusi positif yang diperoleh dari hasil penelitian tersebut. Penelitian yang dilakukan dengan baik dan menghasilkan temuan yang berarti dapat memberikan berbagai manfaat, baik bagi masyarakat, lembaga, maupun perkembangan ilmu pengetahuan(Nashrullah et al., 2023). Penelitian dengan judul "Analisis Peran CSIRT dalam Penanggulangan Serangan Siber di Lingkup Pemerintahan Kabupaten Ponorogo" memiliki manfaat teoritis dan praktis dalam konteks keamanan siber di lingkup pemerintahan yaitu,

1. Manfaat teoritis yang dapat diperoleh dari penelitian ini:
    a. Pengembangan Teori Keamanan Siber: penelitian ini dapat memberikan kontribusi dalam pengembangan teori keamanan siber, khususnya dalam konteks pemerintahan daerah. Dengan menganalisis peran CSIRT (*Computer Security Incident Response Team*) dalam penanggulangan serangan siber, penelitian ini dapat memperkaya pemahaman teoritis tentang strategi dan taktik yang efektif dalam melindungi infrastruktur informasi pemerintahan dari ancaman siber.

b. Peran CSIRT dalam Pemerintahan Daerah: penelitian ini dapat memberikan wawasanmendalam tentang peran CSIRT dalam konteks pemerintahan daerah, khususnya di Kabupaten Ponorogo. Dengan memahami bagaimana CSIRT beroperasi dan berkolaborasi dengan entitas terkait dalam penanggulangan serangan siber, penelitian ini dapat memberikan pemahaman yang lebih baik tentang pentingnya keberadaan CSIRT dalam menjaga keamanan informasi pemerintahan.

c. Implementasi Kebijakan Keamanan Siber: penelitian ini dapat memberikan wawasan tentang implementasi kebijakan keamanan siber di lingkup pemerintahan daerah. Dengan menganalisis efektivitas CSIRT dalam melaksanakan kebijakan keamanan siber yang ada, penelitian ini dapat memberikan masukan berharga untuk perbaikan dan peningkatan kebijakan keamanan siber di Kabupaten Ponorogo.

d. Kolaborasi antara CSIRT dan Stakeholder: penelitian ini dapat memberikan pemahaman tentang pentingnya kolaborasi antara CSIRT dengan berbagai *stakeholder* terkait dalam penanggulangan serangan siber. Dengan menganalisis interaksi CSIRT dengan pihak terkait seperti lembaga pemerintahan, lembaga swasta,dan masyarakat, penelitian ini dapat memberikan wawasan tentang pentingnya kerjasama lintas sektor dalam menjaga keamanan siber.

2. Manfaat praktis yang dapat diperoleh dari penelitian ini:

a. Peningkatan respons terhadap serangan siber: dengan menganalisis peran CSIRT dalam penanggulangan serangan siber, penelitian ini dapat membantu meningkatkan respons dan tanggap darurat dalam menghadapi serangan siber di lingkup pemerintahan Kabupaten Ponorogo. Hal ini dapat membantu dalam deteksi dini, investigasi, dan penanganan serangan siber secara efektif.

b. Peningkatan keamanan informasi pemerintahan: penelitian ini dapat membantu meningkatkan keamanan informasi pemerintahan di Kabupaten Ponorogo dengan memperkuat peran CSIRT dalam melindungi infrastruktur informasi dan data sensitifpemerintah dari ancaman siber. Dengan demikian, integritas, kerahasiaan, dan ketersediaan informasi pemerintahan dapat terjaga dengan lebih baik.

c. Peningkatan kesiapan dan kapasitas CSIRT: penelitian ini dapat membantu meningkatkan kesiapan dan kapasitas CSIRT dalam menghadapi serangan siber dengan lebih efektif. Dengan menganalisis peran, prosedur operasional, dan kolaborasi CSIRT dengan entitas terkait, penelitian ini dapat memberikan rekomendasi untuk memperkuat kemampuan CSIRT dalam mengidentifikasi, menanggapi, dan merespons serangan siber.

d. Peningkatan kesadaran keamanan siber: penelitian ini dapat membantu meningkatkankesadaran tentang keamanan siber di kalangan pegawai pemerintahan Kabupaten Ponorogo. Dengan memahami peran CSIRT dan pentingnya keamanan informasi, pegawai pemerintahan dapat lebih waspada terhadap potensi serangan siber dan mengimplementasikan praktik keamanan siber yang lebih baik.

E. PENEGASAN ISTILAH

Penegasan istilah merujuk pada upaya untuk memberikan definisi yang jelas, spesifik, dan terperinci terhadap suatu istilah atau konsep tertentu dalam konteks tertentu. Penegasan istilah penting dilakukan dalam penulisan ilmiah, khususnya dalam bidang yang memiliki istilah khusus atau teknis, untuk memastikan pemahaman yang tepat dan konsisten terhadap konsep yang dibahas. Untuk memudahkan pembaca dalam memahami isi dari pembahasan pada penelitian ini berikut beberapa pengertian dari beberapa istilah kunci,

1. *E-government* memanfaatkan teknologi informasi dan komunikasi (TIK) untuk memberikan layanan publik yang lebih efisien, transparan, dan mudah diakses oleh masyarakat. Tujuannya adalah meningkatkan interaksi pemerintah-warga dan kualitas layanan publik.
2. CSIRT (*Computer Security Incident Response Team)* adalah tim yang bertanggung jawab untuk menangani insiden keamanan informasi dan merespons serangan keamanan komputer. Tugas utama CSIRT meliputi pemantauan keamanan, investigasiinsiden keamanan, merespons serangan keamanan, serta memberikan rekomendasi untuk mencegah insiden serupa di masa depan. CSIRT berperan penting dalam menjaga keamanan informasi dan melindungi data sensitif dari ancamankeamanan siber.
3. Serangan siber adalah serangkaian kegiatan ilegal yang dilakukan secara daring atau melalui jaringan komputer oleh oknum yang tidak bertanggungjawab dengan tujuan merusak infrastruktur, hingga menciptakan kekacauan dalam sistem. Kejahatan siber dapat mencakup berbagai jenis aktivitas kejahatan, termasuk mencuri data pribadi, melancarkan serangan terhadap sistem komputer, pencurian identitas, dan banyak lagi.

4. *Cybersecurity* adalah upaya untuk melindungi sistem komputer, jaringan, perangkat lunak, dan data dari serangan, pencurian, atau kerusakan yang dilakukan melalui dunia maya atau internet. Tujuan utama dari *cybersecurity* adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi serta sistem komputer. Keamanan siber melibatkan berbagai strategi, kebijakan, teknologi, dan praktik yang dirancang untuk mencegah serangan siber, mendeteksi ancaman keamanan, merespons insiden keamanan, dan memulihkan sistem setelah terjadi serangan.
5. *Malware* adalah singkatan dari *malicious software*, yaitu perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mencuri data dari sistem komputer atau perangkat lainnya tanpa izin pengguna.
6. *Phishing* adalah tindakan penipuan online di mana penipu mencoba untuk memperoleh informasi pribadi seperti kata sandi, informasi keuangan, atau data sensitif lainnya dengan menyamar sebagai entitas tepercaya. Penipu phishing sering kali menggunakan email, pesan teks, atau situs web palsu yang dirancang untuk menipu korban agar memberikan informasi pribadi mereka secara sukarela.
7. *Ransomware* adalah jenis *malware* yang dirancang untuk mengenkripsi data pada sistem komputer atau perangkat, dan kemudian meminta tebusan (ransom) kepada korban agar mereka dapat mendapatkan kunci dekripsi untuk mengembalikan akses ke data mereka. *Ransomware* sering kali mengancam untuk menghapus atau merusakdata jika tebusan tidak dibayar dalam jangka waktu tertentu.
8. *Hacking* adalah kegiatan di mana seseorang (*hacker*) menggunakan keterampilan teknis komputer untuk mengakses atau memanipulasi sistem komputer atau jaringan tanpa izin atau otorisasi. Aktivitas hacking dapat dilakukan dengan berbagai tujuan, mulai dari mencuri informasi sensitif, merusak data, hingga mengganggu operasi sistem atau jaringan.

F. LANDASAN TEORI

Landasan teori dalam penelitian merujuk pada kerangka konseptual atau teori yang menjadi dasar atau pijakan untuk merancang, melaksanakan, dan menginterpretasikan hasil penelitian. Penelitian ini menggunakan dua teori untuk melihat sejauh mana penerapan *e-government* yang ada di Kabupaten Ponorogo dan melihat fenomena *cyberattack* yang pernah terjadi pada tahapan *e-government* yang dilaksanakan oleh pemerintah Kabupaten Ponorogo.

1. Teori *e-government* :

   Salah satu pendekatan yang digunakan dalam penelitian ini adalah implementasi *e- government*, yang merupakan penerapan teknologi informasi dan komunikasi dalam penyelenggaraan pelayanan publik dan proses administrasi pemerintahan. Alshawi dan Aladwani dalam(Adjei-Bamfo et al., 2019) mendefinisikan *e-government* sebagai penggunaan teknologi informasi dan komunikasi dalam proses pemerintahan untuk meningkatkan efisiensi, efektivitas, transparansi, dan akuntabilitas pemerintahan. Menurut seorang penstudi *e-government* Gil-Garcia pada bukunya menyebutkanbahwa ukuran "kesuksesan" dari penerapan *e-government* sendiri akan mengalami pergeseran seiring dengan perkembangan teknologi terbaru yang sangat cepat serta kultur masyarakat yang sangat dinamis. Hal paling mendasar pada penggunaan teknologi adalah dimensi efisiensi serta *cost effectiveness* yang artinya dalam setiap penggunaan teknologi akan dikaitkan dengan efektifitas biaya yang dikeluarkan serta efisiensi waktu yang dihasilkan dari penggunaan teknologi tersebut. Oleh karena itu teknologi informasi terbaru yang terus berkembang akan mempengaruhi kriteria kesuksesan dari pengaplikasian *e-government*. Oleh sebab itu, *e-government* tidak hanya berurusan dengan persoalan efisiensi biaya dan kecanggihan teknologi namun juga berkaitan erat dengan keterwujudan nilai-nilai yang mencerminkan tata kelola pemerintahan yang baik seperti transparansi, keterbukaan, ketepatan kebijakan, peningkatan kualitas pelayanan publik dan

peningkatan partisipasi masyarakat. Gil- Garcia menyebutkan bahwa esensi dari *e-government* dapat dipahami melalui suatu pendekatan, salah satunya adalah pendekatan evolusioner yaitu memahami konsep *e-government* melalui suatu intrumen yang menggambarkan tahap-tahap yang bersifat evolusioner(Irawan & Hidayat, 2012). Di pemerintahan Kabupaten Ponorogo sendiri tahapan pengaplikasian *e- government* sesuai dengan model tahapan *e-government* versi United Nations model World Bank.Model ini menekankan pada "*the nature of communication*" dari suatu proyek *e- government* yang terdiri dari tiga tahapan yakni:

a. *publishing/informationale-government,* tidak berbeda dengan tahapan awal pada model evolusi lainnya, dimana fitur yang tersedia tidak lebih dari penampilan konten yang berisi informasi pelayanan publik, alamat kantor, nomor telepon kantor dan lain sebagainya. Tidak ada interaksi yang terjadi antara pemerintah danmasyarakat, peran masyarakat dalam konteks ini adalah sebagai pihak yang pasif menerima informasi publik. Tampilan *e-government* hampir sama seperti brosur layanan pemerintah yang berbentuk elektronik.
b. *interaction/responsive e-government,* dimana interaksi sederhana antara pemerintah dan masyarakat mulai terjadi. Tujuan utama dari pembukaan kanal interaksi ini adalah untuk mengurangi frekuensi kunjungan masyarakat ke kantor pelayanan seta mengurangi panggilan telepon yang masuk ke kantor pelayanan. Dengan demikian, maka masyarakat bisa menghemat waktu dan biaya untuk konsultasi pelayanan yang biasanya dilakukan secara fisik atau melalui telepon. Pada tingkat ini, sudah disediakan formulir untuk diunduh, alamat email yang bisadikontak dan bentuk interaksi lainnya.
c. *transaction/transactional e-government,* merupakan tingkat paling kompleks, ini memungkinkan adanya transaksi (informasi dan uang) antara pemerintah dan masyarakat melalui sistem *e-government*. Sama seperti tahapan pada

model yang lainnya dimana masyarakat bisa mengurus perpanjangan surat izin, membayar pajak dan denda serta layanan publik lainnya melaui satu platform elektronik.

2. Teori *Cybersecurity Framework* :

Dalam konteks keamanan informasi dan siber, penerapan *e-government* membawa tantangan tersendiri terkait dengan perlindungan data sensitif, infrastruktur kritis, dan kerentanan terhadap serangan siber(Irawan & Hidayat, 2012). Untuk mengatasi tantangan tersebut, diperlukan kerangka kerja keamanan siber yang kokoh dan terstruktur. Salah satu kerangka kerja keamanan siber yang dikenal luas adalah *Cybersecurity Framework* yang dikembangkan oleh (National Institute of Standards And Technology, 2018) di Amerika Serikat. Kerangka kerja ini memberikan panduan yang komprehensif untuk meningkatkan keamanan siber organisasi dengan pendekatan berbasis risiko dan prinsip-prinsip manajemen yang terstruktur. Kerangkakerja keamanan siber (*cybersecurity framework*) adalah sebuah panduan yang dikembangkan oleh *National Institute of Standards and Technology* (NIST) di Amerika Serikat. Kerangka kerja ini menawarkan pendekatan fleksibel untuk pengelolaan keamanan siber yang mencakup aspek fisik, siber, dan SDM, dan dapat diterapkan pada berbagai organisasi yang menggunakan teknologi, termasuk yang berbasis IT, ICS, CPS, dan IoT. Kerangka kerja ini membantu melindungi privasi pelanggan dan karyawan serta memandu pengembangan dan peningkatan kompetensi SDM di bidang keamanan siber. Kerangka kerja ini terdiri dari lima pilar utama yang saling terkait dan saling mendukung:

a. *Identify* (Identifikasi): Tahap pertama dalam kerangka kerja ini adalah mengidentifikasi aset informasi yang penting, ancaman potensial, dan kerentanan yang ada. Dengan memahami lingkungan informasi mereka secara menyeluruh, organisasi dapat menentukan langkah-langkah keamanan yang tepat.

b. *Protect* (Perlindungan): Tahap ini berkaitan dengan langkah-langkah untuk melindungi aset informasi yang penting dari ancaman dan kerentanan. Ini meliputi implementasi kontrol keamanan yang sesuai, pelatihan keamanan bagi karyawan, dan pengembangan kebijakan keamanan yang efektif.

c. *Detect* (Deteksi): Tahap ini fokus pada deteksi secara cepat terhadap insiden keamanan yang terjadi. Organisasi perlu memiliki mekanisme untuk mendeteksi serangan siber atau aktivitas mencurigakan agar dapat merespons dengan cepat.

d. *Respond* (Respons): Setelah deteksi insiden keamanan, tahap respons melibatkan tindakan cepat untuk merespons insiden tersebut. Organisasi perlu memiliki rencana respons keamanan yang terstruktur untuk mengurangi dampak serangan dan memulihkan sistem.

e. *Recover* (Pemulihan): Tahap terakhir adalah pemulihan, di mana organisasi perlu merestorasi sistem informasi mereka ke kondisi normal setelah terjadi insiden keamanan. Proses pemulihan ini mencakup evaluasi dampak, perbaikan sistem, danpenguatan keamanan untuk mencegah serangan serupa di masa depan. Kerangka kerja *cybersecurity framework* memberikan panduan yang fleksibel dan dapat disesuaikan dengan berbagai jenis organisasi dan industri. Dengan menerapkan kerangka kerja ini, organisasi dapat memperkuat pertahanan mereka terhadap ancaman siber,meningkatkan kesiapan dalam menghadapi insiden keamanan, dan melindungi informasi sensitif mereka dengan lebih efektif(Taherdoost, 2022).

Kerangka kerja ini menawarkancara yang fleksibel untuk mengatasi keamanan siber, termasuk efek keamanan siber pada dimensi fisik, siber, dan personil. Kerangka kerja ini dapat diterapkan pada organisasi yang mengandalkan teknologi, baik fokus keamanan sibernya pada teknologi informasi (IT), sistem kendali industri (ICS), sistem siber-ke-fisik (CPS), atau perangkat terhubung yang lebih umum, termasuk Internet untuk Segala (IoT). Kerangka kerja dapat membantu organisasi mengatasi keamanan siber karena berpengaruh pada privasi pelanggan, karyawan, dan pihak lain. Selain itu, hasil kerangka kerja berfungsi sebagai target

untuk kegiatan pengembangan dan evolusi tenaga kerja. CSIRT memiliki peran krusial dalam mendeteksi, merespons, dan memulihkan sistem setelah terjadi insiden keamanan siber. Penelitian ini bertujuan untuk menganalisis efektivitas peran CSIRT dalam konteks *e-government* di lingkup pemerintahan Kabupaten Ponorogo, dengan menggunakan *cybersecurity framework* sebagai landasan teoretis. Dengan memahami peran CSIRT dan menerapkan kerangka kerja keamanan siber yang tepat, diharapkan pemerintahan Kabupaten Ponorogo dapat meningkatkan ketahanan siber mereka dan melindungi informasi sensitif dari ancaman siber yang semakin kompleks(Pratomo et al., 2018).

G. DEFINISI OPERASIONAL

Dalam penelitian, definisi operasional digunakan untuk memberikan petunjuk yang jelas tentang cara mengukur variabel-variabel yang diteliti. Definisi operasional menjelaskan secara rinci bagaimana suatu konsep akan diukur atau diamati dalam konteks penelitian tertentu. Dengan adanya definisi operasional yang jelas dan terdefinisidengan baik, peneliti dapat mengukur variabel-variabel yang diteliti secara konsisten danakurat, sehingga memungkinkan untuk mendapatkan hasil penelitian yang valid dan dapat diandalkan. Berikut beberapa definisi operasional pada penelitian ini,

1. Teori *e-government* dalam penelitian ini digunakan untuk melihat tingkatan perkembangan penyelenggaraan *e-government* di Kabupaten Ponorogo. Sejauh mana tahapan penerapan *e-government* yang sudah dilaksanakan oleh pemerintah Kabupaten Ponorogo dengan tujuan untuk melihat kemungkinan-kemungkinan terjadiserangan siber.

a. *publishing/informational e-government,* merujuk pada tahapan *e-government* yang fokus pada penyediaan informasi dan publikasi data oleh pemerintah kepada masyarakat melalui platform digital. Dalam teori *e-governmnet, publishing/informational e-government* digunakan untuk melihat sejauh mana pemerintah Kabupaten Ponorogo menyediakan platform digital untuk kepentingan pelayanan publik.
b. *interaction/responsive e-government,* merujuk pada kemampuan pemerintahan Kabupaten Ponorogo untuk memberikan respons yang cepat dan efektif terhadap kebutuhan masyarakat serta interaksi yang sinergis antara pemerintah dan warga dalam memanfaatkan teknologi informasi dan komunikasi. Dalam teori *e-governmnet, interaction/responsive e-government* digunakan untuk melihat sejauh mana penerapan *e-government* untuk memberikan respon terkait pelayanan publikkepada masyarakat melalui platform sistem informasi pemerintahan.
c. *transaction/transactional e-government,* merujuk pada penggunaan internet atau teknologi informasi oleh lembaga pemerintah untuk melakukan transaksi, penggunaan teknologi informasi tersebut untuk meningkatkan layanan public dan mengoptimalkan efisiensi biaya dalam operasi pemerintah. Dalam teori *e-government transaction/ transactional e-government* digunakan untuk melihat sejauh mana penggunaan sistem informasi oleh pemerintah Kabupaten Ponorogo untuk melakukan transaksi dalam pelayanan publik.

2. NIST *Cybersecurity Framework* adalah kerangka kerja yang mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan sistem informasi dari serangan siber. Dalam penelitian ini, teori NIST *Cybersecurity Framework* digunakan sebagai pedoman untuk mengevaluasi kesiapan keamanan siber di lingkungan pemerintahan Kabupaten Ponorogo dan untuk merancang strategi penanggulangan serangan siber yang efektif.
    a. Identifikasi (*Identify*): Identifikasi dalam teori *cybersecurity framework* digunakan untuk melihat informasi yang penting terkait ancaman potensial dan kerentanan yang ada di Dinas Komunikasi dan Informatika dengan memahami lingkungan informasi penelitian untuk melihat aset informasi kritis dan infrastruktur TI yang rentan terhadap serangan siber di lingkup Pemerintahan Kabupaten Ponorogo.
    b. Perlindungan (*Protect*): Perlindungan dalam teori *cybersecurity framework* akan digunakan untuk melihat upaya CSIRT untuk meningkatkan perlindungan terhadap serangan siber dengan melakukan penyusunan kebijakan keamanan informasi, implementasi teknologi keamanan seperti *firewall* dan enkripsi.
    c. Deteksi (*Detect*): Deteksi dalam teori *cybersecurity framework* akan digunakan untuk melihat mekanisme deteksi dini terhadap serangan siber dengan cara pemasangan perangkat deteksi.
    d. Respons (*Respond*): Respons dalam teori *cybersecurity framework* akan digunakan untuk melihat tindakan respons cepat terhadap serangan sistem informasi milik pemerintah daerah Kabupaten Ponorogo oleh CSIRT
    e. Pemulihan (*Recover*): Pemulihan dalam teori *cybersecurity framework* akan digunakan untuk melihat proses pemulihan sistem informasi pasca serangan, evaluasi dampak serangan, dan kerentanan sistem, serta pembelajaran dari insiden untuk penguatan keamanan di masa depan.

H. METODOLOGI PENELITIAN

1. Pendekatan penelitian

Pendekatan penelitian merujuk pada strategi atau metode yang digunakan oleh peneliti untuk mendekati, merancang, dan melaksanakan suatu studi penelitian. Pendekatan penelitian memberikan kerangka kerja yang mengarahkan langkah- langkah yang akan diambil dalam proses penelitian(Anisah & Fasa, 2016). Pada penelitian dengan judul "Analisis Peran CSIRT dalam Penanggulangan Serangan Siber di Lingkup Pemerintahan Kabupaten Ponorogo" ini menggunakan pendekatan penelitian kualitatif untuk mendapatkan pemahaman mendalam tentang peran CSIRT dalam penanggulangan serangan siber di lingkup Pemerintahan Kabupaten Ponorogo.

Pendekatan kualitatif dipilih karena memungkinkan peneliti untuk mendapatkan pemahaman mendalam tentang peran CSIRT dan tantangan yang dihadapi dalam mengatasi serangan siber di lingkup pemerintahan Kabupaten Ponorogo. Menurut Creswell penelitian kualitatif adalah pendekatan penelitian yang digunakan untuk memahami makna yang diberikan oleh individu atau kelompok dalam konteks tertentu. Metode penelitian kualitatif ini bertujuan untuk menjelaskan fenomena yang kompleks melalui pengumpulan data berupa wawancara, dokumentasi gambar, rekaman suara, dan observasi yang mendalam(Jha, 2023). Penelitian kualitatif sering kali fokus pada interpretasi, pemahaman, dan konteks sosial dari suatu masalah, dan tidak terpaku pada pengukuran angka atau statistik. Penelitian ini menggunakan jenis penelitian studi kasus yakni mengkaji lebih dalam kasus serangan siber yang pernah terjadi di Kabupaten Ponorogo serta penanggulangan dari kasus tersebut. Maka, penelitian dengan metode kualitatif merupakan metode penelitian yang fokus pada obsevasi secara mendalam terhadap objek penelitian sehingga kajian yang dihasilkan lebih komprehensif(Anisah & Fasa, 2016).

2. Lokasi penelitian

Lokasi penelitian merujuk pada tempat atau wilayah di mana penelitian dilakukan atau data dikumpulkan. Lokasi penelitian dapat berbeda-beda tergantung pada jenis penelitian yang dilakukan dan objek penelitian yang diteliti.Pemilihan lokasi penelitian yang tepat sangat penting untuk memastikan bahwa penelitian dapat dilaksanakan dengan efektif, data dapat dikumpulkan secara akurat, dan hasil penelitian dapat mencerminkan konteks yang sesuai dengan tujuan penelitian. Ada beberapa alasan yang mendasari pemilihan Kabupaten Ponorogo sebagai tempat untuk melakukan penelitian dengan judul "Analisis Peran CSIRT dalam Penanggulangan Serangan Siber di Lingkup Pemerintahan Kabupaten Ponorogo", antara lain:

a. Relevansi Tema: Dalam era digital dan meningkatnya ancaman serangan siber, keamanan siber menjadi sangat penting, terutama bagi institusi pemerintahan. Penelitian ini relevan karena memberikan kontribusi dalam pemahaman tentang peran CSIRT dalam melindungi informasi sensitif dan infrastruktur TI pemerintahan di Kabupaten Ponorogo.
b. Kebutuhan akan Analisis Mendalam: Dengan melakukan analisis peran CSIRT, penelitian ini dapat memberikan wawasan yang mendalam tentang bagaimana timkeamanan informasi ini beroperasi, tantangan yang dihadapi, serta efektivitas langkah-langkah yang diambil dalam menanggulangi serangan siber.
c. Kontribusi terhadap Keamanan Siber Lokal: Penelitian ini dapat memberikan kontribusi langsung dalam meningkatkan keamanan siber di tingkat lokal, khususnya di lingkungan pemerintahan Kabupaten Ponorogo. Temuan penelitian dapat digunakan sebagai dasar untuk perbaikan kebijakan, prosedur, dan praktik keamanan siber di wilayah tersebut.

d. Peningkatan Kesadaran dan Kesiapan: Dengan menganalisis peran CSIRT, penelitian ini juga dapat membantu meningkatkan kesadaran dan kesiapan pemerintah daerah dalam menghadapi ancaman serangan siber yang semakin kompleks dan beragam.
e. Pemenuhan Kebutuhan Penelitian Lokal: Penelitian ini dapat menjadi sumbangan dalam pemahaman tentang keamanan siber di tingkat lokal, yang dapat menjadi acuan bagi kebijakan dan tindakan preventif dalam melindungi data dan sistem informasi pemerintahan Kabupaten Ponorogo.

3. Subjek/ informan penelitian

Informan dalam penelitian ini (individu, kelompok, atau entitas) berperan sebagai sumber data utama untuk menjawab pertanyaan penelitian(Lenaini, 2021). Penelitian ini menggunakan tiga sumber data utama ("3P"): person, place, dan paper. Pemilihan informan (person) menggunakan teknik purposive sampling, yaitu pemilihan sampel berdasarkan kriteria tertentu sesuai kebutuhan penelitian(Syafrida Hafni Sahir, 2022). Dalam studi ini subyek yang dipilih dengan memenuhi kriteria tertentu antara lain:

a. Keahlian, khususnya dalam bidang IT
b. Memiliki jabatan khusus sesuai kualifikasi bidang garapannya.

4. Teknik pengumpulan data

Teknik pengumpulan data dalam penelitian ini sangat penting untuk memastikan data yang diperoleh relevan dan akurat. Metode pengumpulan data dipilih agar sesuai dengan tujuan penelitian, jenis data yang dibutuhkan, dan karakteristik informan(Jha, 2023). Penelitian ini menggunakan pendekatan kualitatif untuk memahami secara mendalam tentang peran, tugas, dan tantangan tim CSIRT dalam menanggulangi serangan siber di Kabupaten Ponorogo. Pendekatan ini dihubungkan dengan sumber data yang digunakan:

a. Data primer: Wawancara mendalam dengan anggota tim CSIRT merupakan sumber utama data. Wawancara ini memungkinkan peneliti untuk mendapatkan informasi langsung dari para informan, termasuk pengalaman mereka dalam menghadapi serangan siber di masa lalu, saat ini, dan masa depan. Informasi ini memberikan wawasan yang kaya dan autentik tentang situasi di lapangan.

b. Data sekunder: Data sekunder, seperti analisis berita media terkait keamanan siber di Pemerintahan Kabupaten Ponorogo, dan dokumen kajian, digunakan sebagai data pendukung. Data sekunder ini memberikan konteks dan informasi tambahan yang membantu peneliti dalam menginterpretasikan data primer yang diperoleh dari wawancara. Dengan menggunakan kombinasi data primer dan sekunder, peneliti dapat memperoleh pemahaman yang komprehensif tentang topik penelitian. Data primer memberikan perspektif langsung dari para informan, sementara data sekunder memberikan konteks yang lebih luas dan mendukung interpretasi data primer. Pendekatan kualitatif memungkinkan peneliti untuk menggali makna dan pemahaman yang lebih dalam tentang fenomena yang diteliti.

5. Keabsahan data

Keabsahan data dalam konteks penelitian merujuk pada tingkat keandalan, ketepatan, dan kepercayaan data yang diperoleh dari sumber-sumber yang digunakandalam penelitian. Keabsahan data menjadi kunci penting dalam menjamin validitas dan kehandalan temuan yang dihasilkan dalam sebuah studi. Penulis menggunakan metode triangulasi data untuk memastikan validitas dan reliabilitas temuan penelitian yaitu dengan melibatkan pengumpulan data dari berbagai sumber atau melalui berbagai teknik untuk mengonfirmasi atau memperkuat temuan penelitian. Pada penelitian ini triangulasi data bersumber dari data wawancara, studi dokumen dan observasi(Anisah & Fasa, 2016).

Pada penelitian ini, triangulasi sumber data dilakukan dengan menggabungkan data dari wawancara dengan para tim keamanan siber, observasi langsung terhadap tim CSIRT, dan studi dokumen terkait kebijakan keamanan siber di Pemerintahan Kabupaten Ponorogo. Dengan mengkombinasikan berbagai sumber data ini, peneliti dapat memperoleh sudut pandang yang komprehensif dan memastikan keabsahan temuan(Norman K. Denzin, n.d.). Berikut metode pengumpulan data pada penelitian ini,

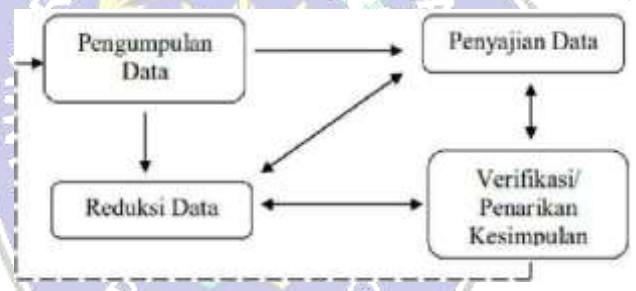
a. Wawancara yaitu dengan melakukan wawancara mendalam dengan anggota CSIRT Kabupaten Ponorogo, pejabat terkait di pemerintahan Kabupaten Ponorogo, dan para ahli keamanan siber untuk menggali informasi tentang peran CSIRT dalam penanggulangan serangan siber.
b. Observasi yaitu dengan mengamati langsung kegiatan CSIRT Kabupaten Ponorogo dalam menangani serangan siber, seperti proses identifikasi, analisis, dan penanganan insiden.
c. Dokumentasi yaitu dengan mengumpulkan data sekunder berupa dokumen resmi CSIRT Kabupaten Ponorogo, laporan insiden siber, dan kebijakan terkait keamanan siber di Kabupaten Ponorogo.

Melalui triangulasi keabsahan data, diharapkan penelitian ini dapat memberikan temuan yang valid dan dapat dipercaya sehingga penelitian ini dapat memberikan kontribusi yang signifikan dalam pemahaman tentang peran CSIRT dalam penanggulangan serangan siber di lingkup Kabupaten Ponorogo.

6. Metode analisis data

Analisis data dalam penelitian ini merupakan proses mengolah dan menginterpretasikan data yang dikumpulkan untuk menemukan makna dan kesimpulan yang valid dan dapat dipercaya. Proses analisis data mengikuti langkah-langkah Miles dan Huberman, yaitu reduksi data, penyajian data, dan verifikasi data. Tujuannya adalah untuk memahami data secara sistematis dan menghasilkan temuan yang relevan.

Gambar 1. 1 Skema analisis data : Miles, M.B & Huberman (1992:20)



Analisis data menurut Miles, M.B & Huberman pada penelitian yang berjudul "Analisis Peran CSIRT dalam Penanggulangan Serangan Siber di Lingkup Pemerintahan Kabupaten Ponorogo":

a. Pengumpulan data:

Pengumpulan data adalah proses mengumpulkan informasi yang relevan dengan topik penelitian berupa angka, teks, gambar, audio, atau video.Tujuan utama pengumpulan data adalah untuk mendapatkan bukti yang dapat digunakan untuk menjawab pertanyaan penelitian atau menguji hipotesis. Metode pengumpulan data yang digunakan sangat beragam, tergantung pada jenis penelitian dan data yang ingin dikumpulkan. Beberapa metode umum dalam pengumpulan data adalah wawancara, observasi, dan analisis dokumen.

b. Reduksi data:

Reduksi data adalah proses yang melibatkan penyederhanaan data "kasar" yang muncul dari catatan-catatan. Dalam konteks analisis data kualitatif, reduksi data merupakan langkah awal yang penting. Tujuan dari reduksi data adalah untuk mengurangi kompleksitas data mentah yang telah terkumpul menjadi bentuk yanglebih terkelola dan relevan untuk analisis lebih lanjut. Proses ini melibatkan penghapusan informasi yang tidak relevan, pengelompokan data, identifikasi pola atau tema yang muncul, dan ekstraksi makna dari data yang disusun kembali. Melalui reduksi data, peneliti dapat memfokuskan perhatian pada aspek-aspek kunci dari data yang akan membantu dalam memahami fenomena yang diteliti. Langkah ini memungkinkan peneliti untuk menyederhanakan kompleksitas data dan memperoleh wawasan yang lebih mendalam serta relevan terhadap topik penelitian yang sedang diinvestigasi. Reduksi data melibatkan proses penyusutan data yang komprehensif menjadi bentuk yang lebih terfokus dan relevan. Identifikasi data adalah poin yang paling penting dan relevan untuk menjawab pertanyaan penelitianterkait peran CSIRT dalam penanggulangan serangan siber di lingkup pemerintahan Kabupaten Ponorogo. Data yang dipilih harus mendukung tujuan penelitian dan memiliki nilai signifikan dalam konteks analisis yang dilakukan. Reduksi data juga melibatkan penyederhanaan informasi yang diperoleh dari berbagai sumber. Identifikasi informasi yang esensial dan relevan untuk menjaga fokus analisis, sambil menghilangkan data yang tidak terlalu penting atau tidak mendukung tujuan penelitian. Memastikan bahwa setiap data yang disimpan adalah unik dan memberikan kontribusi yang berarti dalam pemahaman peran CSIRT dalam penanggulangan serangan siber(Pratomo et al., 2018).

c. Penyajian data:

Penyajian data adalah proses yang melibatkan pengorganisasian, penggalian, dan penyajian informasi yang relevan dan signifikan dari data yang telah dikumpulkan dalam sebuah penelitian. Penyajian data ini bertujuan untuk mengkomunikasikan temuan yang didapat secara jelas, sistematis, dan mudah dipahami kepada pembaca atau pihak terkait. Dalam konteks analisis kualitatif, penyajian data menurut Miles M.B. & Huberman melibatkan berbagai teknik visualisasi, seperti tabel, grafik, diagram, narasi deskriptif, dan kutipan yang mendukung untuk mengilustrasikan temuan kunci, pola, dan hubungan yang muncul dari data kualitatif yang telah dianalisis. Penyajian data yang baik akan membantu pembacamemahami konteks, kompleksitas, dan implikasi dari temuan penelitian dengan lebih baik. Selain itu, penyajian data menurut Miles M.B. & Huberman juga menekankan pentingnya menyajikan data secara transparan, akurat, dan konsisten. Hal ini mencakup memberikan konteks yang memadai, menjelaskan metode analisis yang digunakan, dan memastikan bahwa interpretasi

data didasarkan pada bukti yang kuat. Penyajian data ini bertujuan untuk memberikan gambaran yang jelas dan terstruktur mengenai peran CSIRT dalam menangani serangan siber di wilayah pemerintahan Kabupaten Ponorogo. Memastikan bahwa informasi yang disajikan mudah dipahami, terorganisir dengan baik, dan mendukung analisis yangmendalam untuk memberikan pemahaman yang komprehensif mengenai kontribusi CSIRT dalam menjaga keamanan informasi di lingkup pemerintahan Kabupaten Ponorogo. Penyajian data yang memadai dan terstruktur sesuai dengan panduan akan menjadi kunci dalam menyoroti temuan dan implikasi dari penelitian mengenai peran CSIRT dalam penanggulangan serangan siber di wilayah Kabupaten Ponorogo(Rachmanu Krisnata et al., 2022).

d. Verifikasi data:

Verifikasi data adalah proses yang sistematis dan berkelanjutan untuk memeriksa, mengonfirmasi, dan memvalidasi kebenaran data yang dikumpulkan dalam penelitian. Verifikasi data merupakan langkah penting dalam penelitian kualitatif yang dilakukan untuk memastikan keakuratan dan keandalan informasi yang digunakan dalam analisis. Verifikasi data dilakukan dengan memastikan bahwa data yang digunakan berasal dari sumber yang terpercaya dan relevan terkait peran CSIRT dalam penanggulangan serangan siber di lingkup pemerintahan Kabupaten Ponorogo. Hal ini melibatkan mengonfirmasi keaslian dan keakuratan data yang diperoleh. Dengan melakukan verifikasi data yang cermat dan teliti dalam penelitian "Analisis Peran CSIRT dalam Penanggulangan Serangan Siber di Lingkup Pemerintahan Kabupaten Ponorogo," akan memastikan bahwa kesimpulan dan rekomendasi yang dihasilkan dari penelitian tersebut didasarkan pada data yang akurat dan dapat dipertanggungjawabkan.