BAB II

TINJAUAN PUSTAKA

A. Penelitian Terdahulu

Untuk membantu dalam penelitian tentang analisis strategi Dinas Komunikasi Dan Informatika Dalam Menghadapi Ancaman Siber Di Kabupaten Tabalong, penulis membandingkan beberapa penelitian terdahulu sebagai berikut :

1. Studi oleh (Hilma Harmen, 2025) yang berjudul “Strategi Penguatan Keamanan Informasi Digital dalam Menghadapi Ancaman Siber: Studi Kasus Kementrian Kominfo” Penelitian ini mengkaji strategi penguatan keamanan informasi digital di Indonesia dalam menghadapi berbagai ancaman siber, dengan menitikberatkan pada peran Kementerian Komunikasi dan Informatika (Kominfo). Pendekatan kualitatif digunakan dengan menelaah berbagai literatur serta kebijakan yang relevan. Hasil kajian menunjukkan bahwa upaya penguatan keamanan informasi dilaksanakan melalui empat pendekatan utama, yaitu penguatan regulasi dan kebijakan, peningkatan kapasitas sumber daya manusia, penerapan teknologi keamanan informasi, serta pelaksanaan edukasi kepada masyarakat. Strategi tersebut memiliki peran penting dalam menjaga kedaulatan digital dan membangun ekosistem digital yang aman serta terpercaya di Indonesia.

2. Studi oleh (Sahat Parulian, 2021) yang berjudul “Studi Tentang Ancaman dan Solusi Serangan Siber di Indonesia” mengatakan bahwa sepanjang periode Januari hingga Juli 2021 tercatat sebanyak 741.441.648 ancaman siber terjadi di Indonesia. Ancaman tersebut berpotensi menimbulkan dampak yang serius, khususnya terhadap keamanan akun dan data pribadi pihak yang menjadi sasaran serangan. Penelitian ini bertujuan untuk menjelaskan konsep ancaman siber, menganalisis jenis-jenis serangan siber yang sering terjadi, mengidentifikasi faktor-faktor yang memengaruhi meningkatnya ancaman siber, menelaah dampak ancaman siber terhadap perlindungan data pribadi, serta mengkaji upaya pencegahan yang dapat dilakukan dalam menghadapi ancaman tersebut. Metode penelitian yang digunakan adalah studi literatur dengan menelaah sumber-sumber tepercaya melalui pengamatan dan analisis terhadap berbagai kasus siber yang berkembang. Hasil kajian menunjukkan adanya peningkatan ancaman siber sebesar 6,15 persen di Indonesia pada periode 2020 hingga 2021. Jenis ancaman yang paling sering terjadi meliputi serangan *Denial of Service* (DoS), seperti *syn flood* dan *ICMP flood*, serangan *phishing*, serta pencurian data pribadi. Adapun langkah mitigasi yang dapat dilakukan antara lain meningkatkan kewaspadaan terhadap informasi palsu atau hoaks, melakukan verifikasi terhadap setiap informasi yang diterima, serta menerapkan praktik keamanan digital yang baik untuk melindungi data dan akun pribadi.

3. Studi oleh (Damar Apri Sudarmadi, 2019) yang berjudul "Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia" mengatakan bahwa tata kelola keamanan siber di Indonesia hingga saat ini masih bersifat parsial dan sektoral, sehingga penanganan permasalahan keamanan siber belum terintegrasi secara menyeluruh. Kondisi ini membuat ancaman siber semakin nyata, terutama apabila dikaitkan dengan ancaman terhadap keamanan siber pada institusi pemerintah dan swasta. Oleh karena itu, pengelolaan keamanan siber harus dilakukan secara terintegrasi guna mencegah ancaman siber di seluruh aspek kehidupan berbangsa dan bernegara. Pada tahun 2017, Badan Siber dan Sandi Negara (BSSN) dibentuk berdasarkan Peraturan Presiden tentang BSSN yang menyatakan bahwa BSSN bertugas melaksanakan keamanan siber secara efektif dan efisien melalui pemanfaatan, pengembangan, serta konsolidasi seluruh pihak yang terkait dengan keamanan siber. Pembentukan BSSN dilatarbelakangi oleh pertimbangan bahwa sektor keamanan siber merupakan salah satu bidang pemerintahan yang perlu diperkuat dan didorong guna mewujudkan keamanan nasional, meningkatkan pertumbuhan ekonomi, serta menjamin pelaksanaan kebijakan dan program pemerintah di bidang keamanan siber. BSSN dibentuk berdasarkan kebutuhan yang mendesak di tengah berbagai tantangan dan permasalahan yang berkaitan dengan penyelenggaraan keamanan siber dan persandian. BSSN merupakan lembaga pemerintah yang berada di bawah dan bertanggung

jawab kepada Presiden. Pembentukan BSSN diharapkan mampu menghadapi berbagai permasalahan dan tantangan pada era siber saat ini maupun di masa yang akan datang. Penelitian ini merupakan penelitian deskriptif dengan menggunakan pendekatan kualitatif yang bertujuan untuk menjelaskan strategi Badan Siber dan Sandi Negara (BSSN) dalam meningkatkan komitmen di bidang keamanan siber guna menghadapi ancaman siber di Indonesia.

4. Studi oleh (Wahyuni Susilowati, 2024) yang berjudul "Studi Literatur: Strategi Pengamanan Siber dalam Menghadapi Cyber Crime". Tujuan penelitian ini adalah untuk mempelajari tentang strategi pengamanan siber dalam menghadapi. Metode yang digunakan dalam penelitian ini adalah tinjauan literatur. Jurnal ini dibuat berdasarkan analisis hasil penelitian yang berasal dari berbagai jurnal yang diakses melalui sumber data sekunder yaitu database google scholar, e-resource dari springer, cambridge maupun taylor and francis. Hasil penelitian menunjukkan bahwa implementasi teknologi seperti enkripsi, otentikasi multifaktor, serta pelatihan pengguna, merupakan beberapa langkah efektif yang telah terbukti mampu mengurangi risiko. Namun, tantangan dalam implementasi strategi ini tetap ada, baik dari segi teknis maupun non-teknis, yang memerlukan perhatian khusus dari peneliti dan praktisi di bidang keamanan siber.
5. Studi oleh (Bilqis, 2025) yang berjudul "Geopolitik cyber security: Strategi menghadapi ancaman siber terhadap keamanan informasi pada

era digital” Penelitian ini mengkaji geopolitik cyber security ancaman-ancaman yang dihadapi negara dalam konteks geopolitik dan strategi menghadapi serangan dalam keamanan siber. Menggunakan metode kualitatif deskriptif dimana ini mengumpulkan data-data yang akurat dari dokumen resmi pemerintah dalam menganalisis geopolitik cyber security. Hasil penelitian indonesia menjadi sasaran terbanyak dalam serangan siber. Pada tahun 2024 lebih dari 330 juta serangan siber terjadi di indonesia. Lemahnya sistem keamanan negara memberikan celah untuk melakukan serangan-serangan pada keamnan informasi negara. Peneliti megharapkan pemerintah dapat melakuakan strategi Penguatan sistem pada Badan Siber dan Sandi Negara (BSSN), menjalin kerja sama luar negeri, peningkatan sumber daya manusia menjadi hal penting dalam menjalankan strategi mengahadapi serangan siber. Penting meningkatkan pertahanan sistem keamanan dalam menghadapi serangan-serangan siber.

6. Studi oleh (Ramadhan, 2025) yang berjudul “Analisis Strategi Keamanan Nasional Indonesia dalam Menghadapi Ancaman Siber” Penelitian ini bertujuan untuk menganalisis strategi keamanan nasional Indonesia dalam merespons ancaman siber melalui pendekatan kualitatif deskriptif berbasis studi literatur dan analisis dokumen. Hasil kajian menunjukkan bahwa Indonesia telah mengimplementasikan berbagai kebijakan strategis, antara lain pembentukan Badan Siber dan Sandi Negara(BSSN), pengesahan regulasi seperti Undang-Undang

Perlindungan Data Pribadi, serta penguatan kerja sama internasional, pengembangan sumber daya manusia, dan pemanfaatan teknologi keamanan. Namun, tantangan signifikan seperti lemahnya koordinasi antar lembaga, rendahnya literasi digital, serta keterbatasan infrastruktur masih menjadi hambatan utama dalam efektivitas pelaksanaannya. Studi ini merekomendasikan penguatan tata kelola, peningkatan kapasitas institusional, dan pelibatan multipihak guna membentuk sistem keamanan siber nasional yang adaptif, inklusif, dan berkelanjutan.

7. Studi oleh (Alfredo Kristian, 2025) yang berjudul "Strategi Mitigasi Ancaman Siber di Era Teknologi Berkembang: Systematic Literature Review". Penelitian ini bertujuan untuk menganalisis berbagai strategi dan pendekatan mitigasi yang telah dirancang dan diterapkan dalam beberapa tahun terakhir guna menangani ancaman siber. Metodologi yang digunakan adalah systematic literature review (SLR) terhadap 20 artikel jurnal ilmiah yang relevan dan diterbitkan dalam rentang waktu 2018 hingga 2024. Hasil studi mengungkapkan bahwa strategi mitigasi yang efektif meliputi penerapan sistem pertahanan berlapis, pemanfaatan teknologi kecerdasan buatan untuk deteksi awal serangan, serta peningkatan literasi dan kesadaran keamanan di kalangan pengguna. Selain itu, peran kebijakan yang solid dan sinergi antar institusi juga terbukti krusial dalam mengelola risiko siber. Adapun tantangan utama yang teridentifikasi mencakup keterbatasan tenaga ahli, ketimpangan infrastruktur, serta cepatnya perkembangan metode serangan. Dengan

demikian, dibutuhkan suatu pendekatan komprehensif yang mencakup dimensi teknis, kelembagaan, dan kebijakan publik dalam menghadapi dinamika ancaman siber di era digital.

Penelitian di atas menunjukkan bahwa isu keamanan siber di Indonesia telah menjadi perhatian serius. Berbagai kajian telah mengungkap bahwa strategi keamanan siber umumnya difokuskan pada penguatan regulasi dan kebijakan, penerapan teknologi keamanan, peningkatan kapasitas sumber daya manusia, serta koordinasi antar lembaga pemerintah, khususnya pada institusi strategis seperti Kementerian Komunikasi dan Informatika dan Badan Siber dan Sandi Negara (BSSN). Selain itu, sejumlah penelitian juga menekankan tingginya intensitas dan kompleksitas ancaman siber, serta pentingnya upaya mitigasi teknis dan peningkatan kesadaran keamanan informasi.

Namun demikian, terdapat celah (*research gap*) dalam penelitian - penelitian tersebut. Sebagian besar penelitian masih berfokus pada tingkat makro atau nasional, sehingga belum banyak mengkaji secara mendalam tentang strategi keamanan siber pada tingkat pemerintah daerah, khususnya di tingkat kabupaten. Selain itu, penelitian terdahulu banyak yang menggunakan pendekatan studi literatur, sehingga belum cukup menggambarkan pengalaman langsung oleh pemerintah dalam menghadapi ancaman siber.

B. Landasan Teori

1. Administrasi Publik

Secara umum Administrasi Publik adalah proses penyelenggaraan pemerintahan yang mencakup perencanaan, pengorganisasian, pelaksanaan, dan pengawasan berbagai aktivitas yang ditujukan untuk memenuhi kebutuhan masyarakat. Administrasi Publik berfokus pada bagaimana kebijakan pemerintah dirumuskan, diterjemahkan ke dalam program, serta diimplementasikan secara efektif sehingga menghasilkan pelayanan publik yang berkualitas. Dalam praktiknya, Administrasi Publik juga melibatkan pengelolaan sumber daya manusia, keuangan, informasi, dan teknologi untuk memastikan bahwa setiap kegiatan pemerintahan berjalan efisien, transparan, akuntabel, dan berorientasi pada kepentingan publik. Dengan demikian, Administrasi Publik menjadi kerangka kerja yang memandu pemerintah dalam mewujudkan tata kelola pemerintahan yang baik (*good governance*) dan pelayanan publik yang responsif.

(Erika Revida, 2021) dalam bukunya mengatakan bahwa Administrasi berasal dari kata ”*ad*” yang artinya cepat dan ”*ministrare*” yang artinya membantu atau melayani. Dengan demikian *administrare* artinya membantu atau melayani dengan cepat. Pengertian administrasi terdiri dari dua kategori yaitu dalam arti sempit dan dalam arti luas. Administrasi dalam pengertian sempit diartikan yaitu setiap kegiatan yang dilakukan oleh tata usaha yaitu ketik mengetik, catat mencatat, tulis menulis, agenda, surat menyurat, dan

kegiatan yang berhubungan dengan pembukuan. Administrasi dalam arti sempit sudah dilakukan oleh manusia sejak manusia ada.

(Wilson, 1887) mengatakan bahwa Administrasi merupakan ranah kegiatan yang berhubungan dengan pelaksanaan hukum dan kebijakan negara melalui proses organisasi yang rasional, sistematis, serta efisien. Dalam pandangannya, administrasi publik berfungsi sebagai instrumen teknis yang memastikan bahwa keputusan politik dapat diwujudkan secara efektif di tingkat operasional pemerintahan. Wilson menekankan adanya distingsi konseptual antara politik dan administrasi, di mana politik berfokus pada penetapan tujuan melalui pembuatan kebijakan, sedangkan administrasi bertanggung jawab pada implementasi kebijakan secara profesional, netral, dan bebas dari intervensi politik praktis. Dengan demikian, administrasi dilihat sebagai suatu ilmu praktis yang memerlukan metode, prinsip, dan kajian ilmiah demi mencapai efisiensi dan ketertiban dalam penyelenggaraan tugas-tugas publik.

(Henry, 2013) di dalam (Gede Wirata, 2024) mengatakan bahwa Administrasi Publik didefinisikan sebagai aktivitas yang berkaitan dengan pelaksanaan kebijakan pemerintah, baik pada level pusat ataupun daerah. Definisi ini menekankan pentingnya peran Administrasi Publik sebagai alat untuk menerjemahkan kebijakan menjadi aksi nyata yang dapat dirasakan oleh masyarakat. Hal ini menunjukkan bahwa tanpa adanya Administrasi Publik yang efektif, kebijakan pemerintah tidak akan mencapai tujuan yang diinginkan.

2. Manajemen Publik

Manajemen publik, yang juga dikenal sebagai manajemen pemerintahan, pada dasarnya merupakan proses yang dilakukan oleh pemerintah untuk memenuhi kebutuhan masyarakat melalui pemanfaatan sumber daya, sarana, dan prasarana yang tersedia. Dalam perspektif manajerialisme, manajer publik dituntut untuk menjalankan fungsi fungsi strategis, seperti perumusan strategi, perencanaan strategis, serta penyusunan program, sebagai bagian penting dalam penyelenggaraan pemerintahan.

(Ghofur, 2014) mendefinisikan manajemen publik sebagai manajemen pemerintah yang mencakup perencanaan, pengorganisasian, dan pengendalian pelayanan kepada masyarakat. Definisi ini menekankan peran pemerintah dalam mengatur sumber daya untuk kesejahteraan publik.

(Shafritz, 1997) dalam (Keban, 2008) menyatakan manajemen publik sebagai studi interdisipliner yang menggabungkan fungsi manajemen seperti planning, organizing, dan controlling dengan elemen sumber daya manusia, keuangan, fisik, informasi, serta politik. Pendekatan ini mencerminkan pengaruh scientific management dan tekanan antara orientasi politik serta kebijakan.

Sedangkan (Hughes, 1994) mengatakan bahwa manajemen publik adalah tidak termasuk administrasi, akan tetapi melibatkan organisasi dalam mencapai tujuan dengan efisiensi maksimum serta tanggung jawab penuh untuk mendapatkan hasil.

3. Manajemen Risiko

Dalam Administrasi Publik, Manajemen risiko adalah suatu proses yang sistematis dan berkelanjutan untuk mengidentifikasi, menganalisis, menilai, serta mengendalikan berbagai potensi risiko yang dapat menghambat pencapaian tujuan penyelenggaraan pemerintahan dan pelayanan publik. Risiko yang dimaksud dapat berupa risiko kebijakan, keuangan, operasional, hukum, teknologi informasi, hingga reputasi lembaga publik. Melalui manajemen risiko, instansi pemerintah diharapkan mampu meminimalkan dampak negatif ketidakpastian, meningkatkan efektivitas dan akuntabilitas kinerja, serta memastikan bahwa setiap program dan kebijakan publik dilaksanakan secara transparan, efisien, dan sesuai dengan prinsip tata kelola pemerintahan yang baik (*good governance*). SNI ISO 31000 mendefinisikan risiko sebagai dampak dari ketidakpastian terhadap pencapaian tujuan, yang dapat bersifat positif maupun negatif. Dalam SNI ISO 31000, manajemen risiko tidak hanya dipahami sebagai upaya menghindari kerugian, tetapi sebagai proses terintegrasi yang membantu organisasi dalam pengambilan keputusan, perencanaan, dan peningkatan kinerja. Manajemen risiko harus diterapkan secara terstruktur, komprehensif, dan berkelanjutan, serta disesuaikan dengan konteks organisasi.

4. Analisis

Di dalam Kamus Besar Bahasa Indonesia, Analisis adalah pengeraian suatu pokok atas berbagai bagiannya dan penelaahan bagian itu sendiri serta hubungan antarbagian untuk memperoleh pengertian yang tepat dan

pemahaman arti keseluruhan. Secara sederhana analisis berarti kegiatan menguraikan suatu masalah atau objek menjadi bagian-bagian kecil, kemudian mengkaji hubungan antarbagian tersebut agar dapat dipahami secara menyeluruh dan mendalam.

(Wiradi, 2006) mengatakan bahwa "Analisis adalah aktivitas yang memuat sejumlah kegiatan seperti menguasai, membedakan, memilah sesuatu untuk di golongkan dan di kelompokkan kembali menurut kriteria tertentu kemudian dicari kaitannya dan di tafsirkan maknanya".

(Keraf, 2004) juga mengatakan bahwa "Analisis adalah sebuah proses untuk memecahkan masalah sesuatu ke dalam bagian-bagian yang saling berkaitan satu dengan yang lainnya"

Berdasarkan pemahaman diatas maka dapat disimpulkan bahwa analisis merupakan suatu proses atau aktivitas sistematis untuk menguraikan suatu masalah atau objek ke dalam bagian-bagian yang lebih kecil, kemudian memilah, mengelompokkan, serta mengkaji hubungan antarbagian tersebut berdasarkan kriteria tertentu, sehingga makna, keterkaitan, dan pemahaman terhadap keseluruhan masalah dapat diperoleh secara tepat dan mendalam.

5. Strategi

Di dalam Administrasi Publik, Strategi adalah serangkaian rencana, arah tindakan, dan pendekatan terpadu yang dirancang oleh organisasi pemerintah untuk mencapai tujuan tertentu dalam penyelenggaraan pelayanan publik dan implementasi kebijakan. Strategi mencakup proses analisis lingkungan, penentuan prioritas, alokasi sumber daya, serta

penetapan langkah-langkah operasional yang memungkinkan instansi publik merespons tantangan, memecahkan masalah, dan meningkatkan kinerja pemerintahan. Strategi berfungsi sebagai pedoman yang mengarahkan bagaimana organisasi pemerintah menyesuaikan diri dengan dinamika sosial, politik, ekonomi, dan teknologi agar pelayanan publik dapat diberikan secara lebih efektif, efisien, dan berorientasi pada kebutuhan masyarakat.

Sudarmadi & Runturambi (2019) mengatakan Strategi adalah alat untuk mencapai tujuan atau keunggulan bersaing dengan melihat faktor eksternal dan internal organisasi. Organisasi melakukan tindakan yang dapat menjadikan keuntungan baik untuk organisasi maupun pihak lain yang berada di bawah kendali organisasi. Identifikasi faktor internal yaitu dengan merumuskan keunggulan dan kelemahan yang berasal dari dalam organisasi, sedangkan identifikasi faktor eksternal yaitu dengan merumuskan peluang dan ancaman yang berasal dari luar organisasi.

(Bryson J. M., 1988) menyatakan bahwa strategi adalah pola keputusan yang koheren dan terintegrasi yang dirancang untuk menentukan arah organisasi, memanfaatkan peluang, mengatasi tantangan, serta mengalokasikan sumber daya secara efektif guna mencapai misi dan tujuan organisasi. Dalam konteks sektor publik, strategi berfungsi sebagai pedoman utama yang membantu organisasi pemerintah menanggapi dinamika lingkungan eksternal, menetapkan prioritas, dan memastikan bahwa tindakan organisasi selaras dengan misi dan nilai publik.

6. Analisis SWOT

Analisis SWOT adalah suatu kerangka kerja sistematis yang digunakan untuk mengevaluasi kondisi internal dan eksternal organisasi dengan cara mengidentifikasi Strengths (kekuatan), Weaknesses (kelemahan), Opportunities (peluang), dan Threats (ancaman). Analisis ini bertujuan untuk memahami posisi strategis organisasi sehingga dapat merumuskan strategi yang efektif dalam menghadapi dinamika lingkungan.

(Rangkuti, 2015) mengatakan bahwa Analisis SWOT merupakan instrumen analisis yang menggambarkan kondisi internal organisasi (kekuatan dan kelemahan) serta kondisi eksternal organisasi (peluang dan ancaman) untuk menentukan strategi yang paling tepat dalam mencapai tujuan.

(John A. Pearce, 2014) Analisis SWOT merupakan alat untuk mengukur dan mencocokkan sumber daya internal organisasi dengan peluang dan ancaman dari lingkungan luar sehingga menghasilkan strategi yang sesuai dengan kondisi organisasi.

7. Ancaman Siber

Ancaman siber dapat dipahami sebagai potensi risiko yang berpeluang menimbulkan kerugian, gangguan, maupun serangan terhadap keamanan informasi, khususnya yang berkaitan dengan aspek kerahasiaan, integritas, dan ketersediaan sistem serta data. Ancaman tersebut dapat diklasifikasikan berdasarkan sasaran atau pihak yang menerima dampak secara langsung.

Sumber ancaman siber merujuk pada individu atau kelompok yang memiliki niat serta melakukan tindakan yang melanggar hukum dan prinsip keamanan informasi dengan tujuan memperoleh keuntungan, baik yang bersifat material maupun nonmaterial, melalui pemanfaatan ruang siber.

Pada era perkembangan teknologi digital saat ini, berbagai jenis data yang bersifat sensitif dan bernilai tinggi banyak disimpan dalam bentuk digital, seperti data pribadi, aset digital, maupun informasi penting milik suatu organisasi atau perusahaan. Seiring dengan kemajuan teknologi dan meningkatnya ketergantungan masyarakat terhadap sistem digital, praktik penyimpanan data secara digital juga semakin meluas. Kondisi tersebut berdampak pada meningkatnya potensi ancaman dan menjadikan data digital sebagai sasaran utama kejahatan siber. Oleh karena itu, diperlukan upaya perlindungan yang memadai melalui penerapan keamanan siber. Keamanan siber (*cybersecurity*) merupakan serangkaian praktik yang bertujuan untuk melindungi aset digital, termasuk komputer, jaringan, aplikasi, sistem, dan data, dari berbagai bentuk serangan siber. Secara umum, keamanan siber mencakup tindakan pencegahan, pendeteksian, serta penanganan terhadap ancaman atau serangan. Penerapan keamanan siber tidak hanya terbatas pada individu, tetapi juga menjadi kebutuhan penting bagi organisasi dan perusahaan dalam menjaga kerahasiaan serta integritas data sensitif dari akses yang tidak berwenang.

Sumber ancaman siber dapat berasal dari pihak internal maupun eksternal, antara lain unsur intelijen, individu yang merasa tidak puas,

kepentingan investigatif tertentu, organisasi ekstremis, *hacktivist*, kelompok kejahatan terorganisir, persaingan usaha, konflik atau permusuhan, hingga penyalahgunaan teknologi. Selain itu, ancaman siber juga beririsan dengan berbagai aspek kehidupan, seperti ideologi, politik, ekonomi, sosial budaya, pertahanan dan keamanan, serta perkembangan ilmu pengetahuan dan teknologi. Oleh karena itu, ancaman siber tidak hanya berdampak pada kepentingan negara, tetapi juga dapat menyasar kepentingan individu maupun organisasi, sehingga siapa pun berpotensi menjadi sumber maupun target ancaman siber.

Dalam Permenhan No. 82 Tahun 2014 tentang Pertahanan Siber mengatakan bahwa ancaman siber memiliki 3 jenis diantaranya adalah :

1) Ancaman perangkat keras atau *hardware threat*, adalah ancaman yang disebabakan oleh instalasi suatu perangkat tertentu pada hardware yang bertujuan untuk melakukan kegiatan tertentu di dalam sistem komputer, hasil akhir dari pemasangan perangkat tersebut adalah dapat terjadi gangguan pada jaringan software dan hardware pada suatu komputer.
2) Ancaman perangkat lunak atau *software threat*, adalah suatu ancaman pada sebuah komputer yang penyebabnya adalah dikarenakan adanya *software* tertentu yang masuk dan bertujuan untuk melakukan hal-hal ilegal seperti mencuri, merusak dan memanipulasi informasi ada dalam komputer itu.
3) Ancaman pada data/informasi atau data *information threat*, merupakan salah satu jenis ancaman yang penyebabnya adalah karena adanya penyebaran beberapa data atau informasi untuk suatu tujuan tertentu.

C. Kerangka Konseptual

