BAB II

TINJAUAN PUSTAKA

2.1 Teori Dasar

2.1.1. Kejahatan Siber

Menurut Harruma (2022), Kejahatan siber adalah sebuah tindakan kriminal yang menggunakan perangkat elektronik dan koneksi internet sebagai alat tindakan kejahatan. Kejahatan siber ini memiliki karakteristik seperti bersifat global, dapat menimbulkan kekacauan yang tidak terlihat, pelaku tidak mengenal usia dan bersifat universal, menggunakan teknologi yang sulit dimengerti orang awam, dan dapat menimbulkan kerugian material dan atau non-material.

Menurut Bahri dalam bukunya yang berjudul *Cyber Crime* dalam sorotan hukum pidana (2020), Kejahatan siber ini dibagi menjadi berbagai macam, yaitu *Cyber Laundering, Cyber Terrorism, Cyber-Fraud, Cyber Gambling*, dan *Cyber Sex*.

Sesuai dengan penjelasan Wibawa (2017), *Cyber Laundering* adalah sebuah tindakan kriminal yang dilakukan dengan cara melakukan pencucian uang tetapi dilakukan di dunia maya. Sama dengan pencucian uang, *cyber laundering* juga melalui tiga tahapan aktivitas, yakni *placement, layering*, dan *integration*.

Menurut Sheldon (2022), *Cyber Terrorism* adalah sebuah serangan terencana yang menyerang sistem informasi, program, dan data-data penting. Sekarang, pengertian tersebut diperluas mencakup dunia maya. Serangan tersebut biasanya bersifat politik, sifatnya mengintimidasi pengguna, dan merusak atau mengganggu infrastruktur.

Menurut Chusna (2023), *Cyber-fraud* adalah sebuah tindakan kriminal yang dilakukan dengan cara menipu para pengguna melalui dunia maya. Biasanya, *cyber-fraud* dilakukan untuk mendapat informasi penting si korban untuk kepentingan pelaku. *Cyber-fraud* ada berbagai jenis, yaitu *phising, ransomware, carding, cracking,* OTP *fraud,* dan *cyberbullying*.

Gambar 2.1. *Ransomware* merupakan salah satu bagian Cyber-Fra

2.1.2. Keamanan Siber

Menurut Basmatulhana (2022), keamanan siber (*cyber security*) adalah upaya yang dilakukan untuk melindungi sistem komputer dari berbagai ancaman atau akses ilegal. Biasanya Keamanan Siber ini biasanya bersangkutan dengan alat, kebijakan, dan konsep keamanan yang digunakan untuk melindungi asset organisasi atau negara dan meminimalisir munculnya resiko ke dalam komputer.

Menurut Hesantry (2023), keamanan siber merupakan salah satu hal yang wajib diperhatikan di masa modern, utamanya untuk pelaku yang berfokus pada bidang bisnis. Semua orang yang membuat aplikasi perlu memahami konsep dari keamanan siber ini untuk menciptakan kegiatan perbisnisan yang nyaman dalam melakukan kegiata perbisnisan.

Ketika membahas keamanan siber, Mack dalam bukunya yang berjudul *Cyber Security* (2018), mengatakan bahwa keamanan siber biasanya menyangkut empat wilayah utama, yaitu:
Keamanan Aplikasi (Application Security)
Keamanan Informasi (Information Security)
Pemulihan Bencana (Disaster Recovery)
Keamanan Jaringan (Network Security)

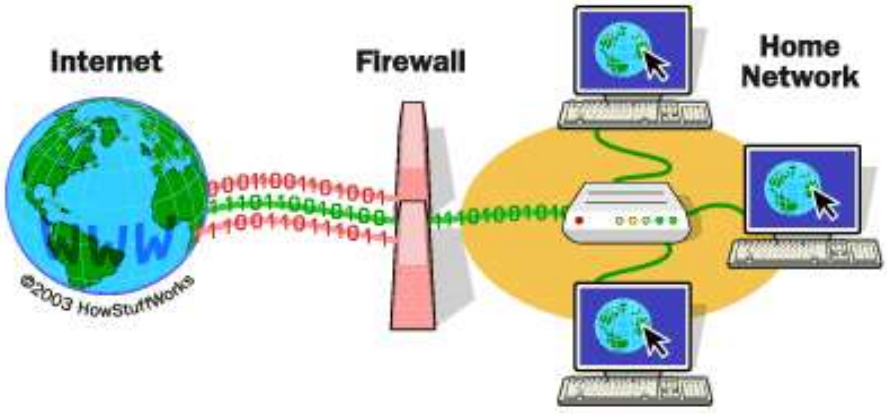
Keamanan aplikasi mencakup tindakan yang harus diambil selama siklus pengembangan aplikasi. Tindakan ini dilakukan untuk melindungi aplikasi yang sedang dikembangkan dari ancaman yang muncul melalui kekurangan yang ada di aplikasi tersebut.

Keamanan informasi mencakup pengamanan informasi dari akses yang tidak sah sehingga tidak terjadi pencurian identitas dan menjaga privasi pengguna. Keamanan informasi memiliki teknik utama yang mencakup identifikasi, autentifikasi, penguasaan pengguna, dan

ilmu pembacaan sandi.

Pemulihan bencana mencakup percobaan penilaian resiko, menetapkan prioritas, dan mengembangkan rancangan pemulihan jika ada bencana dalam aplikasi. Semua perusahaan yang berfokus dalam kegiatan bisnis harus punya rencana pemulihan bencana yang kuat agar kegiatan perbisnisan bisa berjalan normal secepatnya.

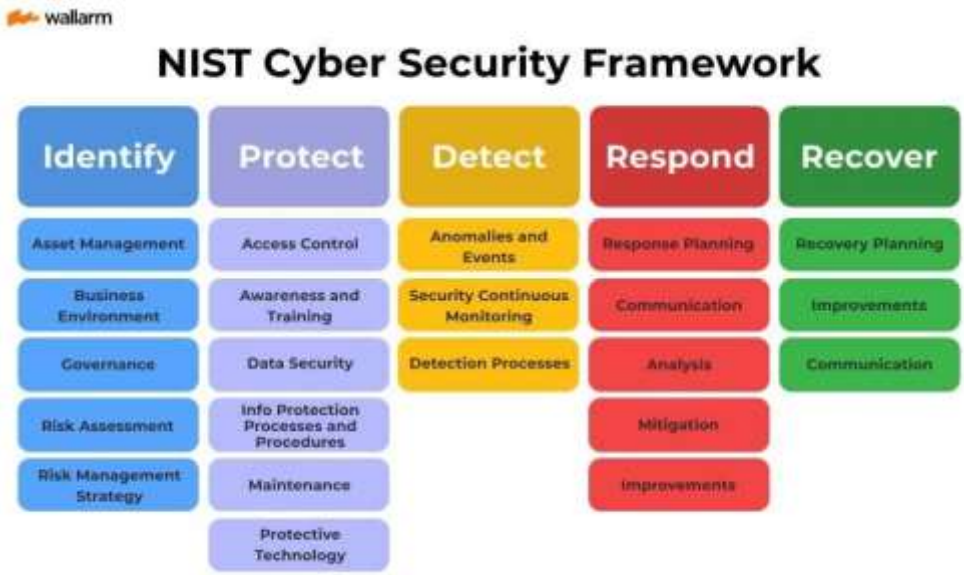
Keamanan jaringan mencakup kegiatan melindungi kegunaan, keandalan, integritas dan keamanan jaringan. keamanan jaringan yang efektif menargetkan berbagai ancaman dan menghentikannya memasuki atau menyebar di internet. Komponen dari keamanan jaringan adalah *anti-virus, anti-spyware, firewall, intrusion prevention system,* dan *Virtual Private Network.*



Gambar 2.2. Bagaimana *firewall* bekerja sebagai keamanan siber

2.1.3. *NIST Cyber Security Framework*

Menurut Tan (2022), *NIST Cyber Security Framework* adalah sebuah *framework* yang bertujuan sebagai pengimplementasi atau peningkatan keamanan siber. *Framework* tersebut juga digunakan dalam melakukan deteksi, mitigasi, dan respon terhadap serangan siber dalam perusahaan atau organisasi. Banyak orang menggunakan *framework* ini karena mudah digunkanan dan mudah juga untuk digabungkan dengan *framework* yang sudah dimiliki perusahaan atau *framework* yang belum dimiliki.



Gambar 2.4. NIST Cyber Security Framework (linkedin.com)

Framework NIST cyber security memiliki inti yang berisi dengan fungsi, kategori, sub kategori, dan informasi referensi untuk menggunakan *framework* tersebut. Inti dari *framework NIST* terdiri dari *Core, Tiers*, dan *Profile*. *Core* berfungsi sebagai memberikan informasi rekomendasi keamanan siber, teknik, hasil, operasional, dan manajemen kontrol. *Tiers* berfungsi sebagai memberi penilaian terhadap keamanan siber yang dimiliki perusahaan. Profil berfungsi sebagai penjelasan situasi terhadap keamanan siber yang dimiliki perusahaan dan target yang ingin dicapai untuk keamanan siber tersebut.

Inti dari *framework NIST* memiliki banyak penjelasan sebagai berikut:

- *Function* berfungsi untuk membantu organisasi melakukan risiko serangan siber
- *Categories* bagian dari *function* dan berfungsi sebagai aspek keamanan siber
- *Subcategories* merupakan pernyataan yang diberikan untuk meningkatkan keamanan siber
- *Informative Reference* adalah referensi yang berfungsi membantu inti *framework* untuk mencapai target dari *subcategories*
- Fungsi dari inti *framework* ada lima fungsi, yaitu *identity, protect, detect, response,* dan *recovery*. *Identity* mengidentifikasi aset IT yang ada di organisasi. Hal tersebut mempermudah membuat keamanan siber untuk organisasi tersebut. *Protect* melindungi aset IT organisasi sehnigga meminimalisir potensi serangan siber. *Detect* memantau aktivitas pada infrastruktur IT organisasi untuk mengetahui aktivitas abnormal terhadap infrastruktur IT. *Response* menindaklanjuti kerusakan aset IT dan menimalisir kerusakan, dan *recovery* memulihkan aset-aset IT yang dirusak oleh serangan siber

tersebut.

2.2 Tinjauan Studi

Tinjauan studi yang dilakukan untuk mendukung penelitian yang dilakukan.

1. Tinjauan studi pada jurnal yang berjudul ”Keamanan siber untuk institusi pendidikan tinggi: mengadopsi kerangka peraturan” Jurnal ini ditulis oleh Kustodio Eunice Bondoc dan Tumibay Gilbert Malawit pada tahun 2020. Diterbitkan oleh Jurnal Global Kemajuan Teknik dan Teknologi. Permasalahan yang diangkat pada jurnal ini adalah menggali berbagai kerangka kerja Keamanan Siber dan lingkungan peraturan yang disajikan melalui tinjauan literatur terkait. Salah satu kerangka tersebut adalah Cybersecurity Framework yang dirilis pada tahun 2014 oleh National Institute of Standards and Technology (NIST). Penetapan kebijakan dan prosedur keamanan siber internal, pengelolaan risiko keamanan siber, dan penyelarasan terhadap standar keamanan informasi internasional akan menjadi sorotan utama dalam tinjauan literatur penelitian ini. Tahap II akan fokus pada perancangan, dan analisis kesepakatan keamanan siber spesifik yang dipandu oleh kerangka peraturan standar yang ditujukan untuk Institusi Negeri terpilih di Wilayah III di Filipina. Menghadapi ancaman serangan siber, para peneliti percaya bahwa administrator dan pemimpin pendidikan perlu menerapkan solusi yang tepat untuk melindungi sumber daya mereka dari ancaman siber. Semua organisasi perlu memahami ancaman siber yang mereka hadapi. Tantangannya saat ini adalah menetapkan tugas-tugas penting terkait dengan pelestarian kerahasiaan, integritas, dan ketersediaan informasi di Ruang Siber sekaligus memfasilitasi fungsi pengoperasian yang penting. Tujuan dalam penelitian ini adalah untuk meninjau literatur terkait tentang Keamanan Siber. Tinjauan pustaka mengenai kebijakan dan prosedur, pengelolaan risiko keamanan siber serta penyelarasan dengan standar keamanan informasi internasional akan menjadi dasar dalam mengusulkan kerangka Keamanan Siber yang ditujukan untuk institusi pendidikan khususnya perguruan tinggi dengan transaksi online. Para peneliti percaya bahwa setiap organisasi baik pemerintah maupun swasta, akan terus memiliki risiko unik, ancaman berbeda, toleransi risiko, dan kerentanan yang perlu diatasi. Kebijakan, pedoman dan prosedur dalam penerapan kerangka yang diusulkan pada dasarnya akan berkonsentrasi pada kebutuhan infrastruktur jaringan institusi pendidikan tinggi. Kesimpulan dari jurnal ini adalah Keamanan Siber yang efektif menghadirkan tantangan kompleks yang memerlukan kolaborasi dari seluruh lingkungan Internet.

Kerangka Keamanan Siber membangun fleksibilitas yang diperlukan untuk implementasi yang efektif dan inovasi yang berkelanjutan. Fleksibilitas ini sangat penting karena memungkinkan organisasi untuk beradaptasi dan berkembang seiring dengan perubahan lanskap ancaman. Kerangka Keamanan Siber dapat menunjukkan kepemimpinan internasional dengan menunjukkan bahwa kemitraan efektif antara pemerintah dan industri merupakan cara paling efektif untuk melawan serangan siber. Menetapkan kerangka praktik dan standar terbaik merupakan langkah penting menuju peningkatan infrastruktur penting dan postur keamanan negara ini. Terakhir, kerangka keamanan siber ditujukan untuk mengurangi dan mengelola risiko keamanan siber dengan lebih baik. Kerangka ini merupakan dokumen yang hidup dan akan terus diperbarui dan ditingkatkan seiring dengan masukan dari industri mengenai implementasinya.

2. Tinjauan studi pada jurnal yang berjudul ” Analisis dan Evaluasi Akademik, Keamanan Sistem Informasi Menggunakan Kerangka NIST SP 800-26” Jurnal ini ditulis oleh Poningsih dan Muhammad Ridwan Lubis pada tahun 2021. Diterbitkan oleh Sinkron : Jurnal dan Penelitian Teknik Informatika. Permasalahan yang diangkat pada jurnal ini adalah Seiring dengan perkembangan teknologi dan informasi yang semakin pesat, saat ini persaingan antar lembaga pendidikan semakin ketat. Apabila suatu lembaga tidak mampu mengikuti kemajuan teknologi informasi yang berkembang sangat pesat, maka dapat dipastikan lembaga tersebut akan tertinggal sangat jauh dari segala sisi. Namun ada hal yang sangat perlu diperhatikan sehubungan dengan perkembangan teknologi informasi, yaitu pertimbangan keamanan sistem informasi yang dimiliki oleh Lembaga. Untuk itu diperlukan suatu analisis dan evaluasi terhadap sistem informasi yang digunakan untuk mengidentifikasi keamanan pada sistem informasi. Jika analisis dan evaluasi tidak dilakukan maka akan timbul permasalahan terkait keamanan suatu sistem informasi seperti data yang rentan terhadap ancaman seperti data rusak dan hilang sehingga data menjadi tidak valid. Jika datanya tidak valid, maka dapat dipastikan informasi yang dihasilkan juga tidak dapat dipercaya. Evaluasi keamanan sistem informasi dapat dilakukan dengan framework. NIST adalah kerangka kerja yang dapat digunakan untuk mengevaluasi dan mengidentifikasi keamanan dan risiko dalam sistem informasi. Proses evaluasi keamanan sistem informasi dilakukan dengan menyebarkan kuesioner kepada civitas akademika sesuai dengan framework NIST SP 800-26 dan datanya dikelola hingga

diperoleh hasil akhir. Hasil evaluasi keamanan sistem informasi akademik mempunyai nilai akhir keseluruhan sebesar 91,6%. Tujuan dalam penelitian ini adalah Berdasarkan latar belakang permasalahan diatas maka dapat disimpulkan bahwa keamanan sistem informasi akademik merupakan salah satu pilar yang sangat penting dalam meningkatkan kualitas layanan informasi dan cara menjaga keamanan sistem informasi sehingga perlu adanya upaya untuk menjaga keamanan sistem informasi akademik. menganalisis dan mengevaluasi sistem informasi. Tujuannya untuk menjawab permasalahan diatas yaitu menganalisis dan mengevaluasi keamanan sistem informasi akademik yang digunakan saat ini di AMIK Tunas Bangsa Pematangsiantar. Kesimpulan dari jurnal ini adalah NIST adalah kerangka kerja yang dapat digunakan untuk mengevaluasi dan mengidentifikasi keamanan dan risiko dalam sistem informasi. Proses evaluasi keamanan sistem informasi dilakukan dengan menyebarkan kuesioner kepada civitas akademika sesuai dengan framework NIST SP 800-26 dan datanya dikelola hingga diperoleh hasil akhir. Hasil evaluasi keamanan sistem informasi akademik mempunyai nilai akhir keseluruhan sebesar 91,6%.

3. Tinjauan studi pada jurnal yang berjudul ” AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN FRAMEWORK NIST SP 800-26 (Studi Kasus : Institusi Sangga Buana YPKP Bandung)” “Jurnal ini ditulis oleh Rangga Satria Perdana pada tahun 2018. Diterbitkan oleh Jurnal Infotronik. Permasalahan yang diangkat pada jurnal ini adalah Seiring dengan kemajuan teknologi informasi, peran teknologi informasi juga semakin terasa signifikan. Namun, dampak dari perkembangan teknologi informasi tersebut membuat tingkat keamanan sistem informasi menjadi rentan. Oleh karena itu, penting untuk melakukan identifikasi terhadap aspek keamanan pada sistem informasi tersebut. Tanpa melakukan audit keamanan, sistem informasi dapat mengalami masalah serius, seperti kehilangan data yang menyebabkan ketidakvalidan data, ketidakakuratan data yang mengurangi kepercayaan, dan rentannya sistem informasi terhadap ancaman. Audit keamanan dapat dilakukan dengan menerapkan standar kerangka kerja tertentu, salah satunya adalah NIST. NIST merupakan kerangka kerja yang umum digunakan untuk mengidentifikasi keamanan dan risiko pada sistem informasi. Proses penilaian audit keamanan sistem informasi dapat dilaksanakan dengan menyebarkan kuesioner berdasarkan framework NIST SP 800-26, dan hasil data tersebut dikelola untuk mendapatkan kesimpulan akhir. Tujuan dari penelitian ini adalah menjawab perumusan masalah sebelumnya, yakni

menganalisis sistem keamanan yang diterapkan pada sistem informasi akademik di Institusi Sangga Buana YPKP. Kesimpulan dari penelitian ini menyatakan bahwa berdasarkan hasil penilaian audit keamanan terhadap sistem informasi akademik di Institusi Sangga Buana YPKP, dapat disimpulkan bahwa sistem tersebut berada pada tingkat 3, yaitu implemented procedures and controls. Hal ini menunjukkan bahwa prosedur dan pengendalian yang telah ditetapkan oleh pihak institusi telah dijalankan. Kesimpulan ini didasarkan pada hasil penilaian audit keamanan secara keseluruhan, yang mencapai skor 3,7005 dari total skor 5.

4. Tinjauan studi pada jurnal yang berjudul ”Penganalisaan Manajemen Risiko pada Sistem Keamanan IDS (Intrusion Detection System) Menggunakan Framework NIST (National Institute of Standards and Technology) SP 800-30. (Studi Kasus: Disinfolahtaau Mabes TNI AU)” “Jurnal ini ditulis oleh Anggi Elanda dan Djajasukma Tjahjadi pada tahun 2018. Diterbitkan oleh Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK. Permasalahan yang diangkat pada jurnal ini adalah Penulis memutuskan untuk menganalisis manajemen risiko dari aplikasi Cybersensor sebagai IDS dengan mengidentifikasi risiko-risiko yang mungkin terjadi di masa depan. Hasil analisis ini akan disusun dalam sebuah laporan yang nantinya akan disampaikan kepada pihak manajemen. Laporan tersebut bertujuan sebagai panduan terhadap peristiwa-peristiwa yang telah terjadi atau yang belum terjadi, sehingga pihak terkait dapat lebih waspada ketika menghadapi serangan. Cybersensor sendiri dikembangkan dengan menggunakan bahasa pemrograman PHP dan Python, serta disertakan dengan integrasi aplikasi Snort. Tujuan utama penelitian ini adalah mempermudah auditor keamanan internet dalam melaksanakan audit pada IDS (Intrusion Detection System), yang diharapkan dapat menghasilkan banyak pengembangan di masa mendatang. Kesimpulan dari jurnal ini menyatakan bahwa berdasarkan hasil identifikasi karakteristik, ancaman, serta kerentanan, terdapat beberapa sumber ancaman yang dapat menimbulkan risiko pada sistem Cybersensor. Antara lain, Human Disaster dan Technology Disaster, di mana Human Disaster mencakup Virus, Malware, Kehilangan Data, Salah Pengoperasian, Hacker, Distribusi File Tanpa Izin, Pencurian Hardware, Software Versi Lama, Instalasi Tanpa Izin. Sementara itu, Technology Disaster mencakup Gangguan Tegangan Listrik. Penentuan skala risiko dilakukan dengan menggunakan skala risk level untuk menganalisis lebih lanjut hasil analisis ancaman yang mungkin terjadi dan yang sudah terjadi. Dilakukan analisis pengendalian dan

dampak risiko yang terjadi pada sistem Cybersensor dengan mempertimbangkan skala risk level yang teridentifikasi. Dari analisis tersebut, dihasilkan beberapa rekomendasi agar kejadian serupa tidak terulang di masa mendatang. Mitigasi risiko juga dilakukan dengan menentukan total biaya yang timbul dari setiap kerusakan akibat ancaman yang teridentifikasi. Untuk menghindari ancaman yang berdampak negatif pada sistem Cybersensor, diperlukan dokumentasi mengenai hasil penilaian risiko, upaya peringanan risiko, dan evaluasi risiko.

Dalam jurnal yang dibuat oleh Briliyant yang berjudul "Rencana Implementasi Manajemen Risiko Cyber dengan Menggunakan NIST CSF dan COBIT 5", Peneliti menganalisa sebuah organisasi dan di organisasi tersebut ada unit yang bertugas sebagai pemelihara sistem informasi internal organisasi tersebut. Peneliti akhirnya membuat sebuah susunan Rencana implementasi manajemen risiko siber dengan memanfaatkan NIST CSF dan COBIT 5. sebagai alat pendukung pekerjaannya. Hasil dari penelitian yang dilakukan adalah Peneliti dapat menyimpulkan bahwa profil unit dari organisasi tersebut baru mencapai *tier* 1, yang berarti *cyber security* yang dilakukan di organisasi tersebut masih belum terbentuk secara formal. Peneliti menuturkan bahwa organisasi tersebut memiliki 13 risiko tinggi dan 12 risiko sedang terkena serangan siber. Penelitu juga mengatakan bahwa organisasi tersebut menargetkan *tier* tiga NIST CSF agar proses *cyber-risk management* dapat dilakukan secara formal.