Jurnal Bisnis dan Kewirausahaan (Journal of Business and Entrepreneurship)
Vol. 11, No. 1 Mei 2023, e-ISSN: 2685-6255; p-ISSN: 2302-4119, Hal 23-33
doi: https://doi.org/10.46273/job&e.v11i1.365

Manajemen Keamanan Cyber di Era Digital

Edy Susanto
Teknik Perminyakan, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia

Lady Antira
Teknik Perminyakan, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia

Kevin Kevin
Teknik Perminyakan, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia

Edo Stanzah
Teknik Perminyakan, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia

Assyeh Annasrul Majid
Teknik Perminyakan, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia

Original Research
Received 30 March 2023
Revised 15 Apr 2023
Accepted 14 May 2023
Additional information at the end of the article

Abstract : *In this rapidly growing digital era, cyber security has become one of the most important aspects to pay attention to. Technological development information and communication has provided many benefits to our lives, they also present serious risks related to data security.. Cyber can be in the form of data theft, destruction systems, manipulation of information, or identity theft. First, cyberattacks are getting more complex and constantly evolving with time technology advances. Attackers can variety of methods and tools sophisticated way to exploit system vulnerabilities and gain access invalid. Second, cyber are often cross-border in nature, where attackers can operate overseas making difficult to identify and law enforcement. In addition, technological advances have also expanded attacks into new domains, such as the Internet of Things (IoT), autonomous vehicle systems, and artificial intelligence. Expanding connectivity between devices and internet-connected infrastructure increases security complexity cyber. However, it is important to remember that cyber security is not a challenge can't be overcome. In an effort to protect data and computer systems using various security strategies and measures can be implemented. With a combination of technical approaches, strong security policies, training user awareness, and cooperation between the parties involved, security cyber can be significantly improved.*

Keywords : *Cyber Attactk, Management Security, Security, System, Technology*

Abstrak : Di era digital yang berkembang pesat ini, keamanan siber menjadi salah satu aspek yang sangat penting untuk diperhatikan. Perkembangan teknologi informasi dan komunikasi telah memberikan banyak manfaat bagi kehidupan kita, juga menghadirkan risiko serius terkait keamanan data. Siber dapat berupa pencurian data, perusakan sistem, manipulasi informasi, atau pencurian identitas. Pertama, serangan siber semakin kompleks dan terus berkembang seiring kemajuan teknologi waktu. Penyerang dapat menggunakan berbagai metode dan alat canggih untuk mengeksploitasi kerentanan sistem dan mendapatkan akses yang tidak valid. Kedua, dunia maya seringkali bersifat lintas batas, di mana penyerang dapat beroperasi di luar negeri sehingga sulit untuk diidentifikasi dan penegakan hukum. Selain itu, kemajuan teknologi juga memperluas serangan ke ranah baru, seperti Internet of Things (IoT), sistem kendaraan otonom, dan kecerdasan buatan. Memperluas konektivitas antara perangkat dan infrastruktur yang terhubung ke internet meningkatkan kompleksitas keamanan

* Edy Susanto, edy.soesanto@dsn.ubharajaya.ac.id

dunia maya. Namun, penting untuk diingat bahwa keamanan siber bukanlah tantangan yang tidak dapat diatasi. Dalam upaya melindungi data dan sistem komputer menggunakan berbagai strategi dan tindakan keamanan dapat diterapkan. Dengan kombinasi pendekatan teknis, kebijakan keamanan yang kuat, pelatihan kesadaran pengguna, dan kerja sama antara pihak-pihak yang terlibat, keamanan siber dapat ditingkatkan secara signifikan.

Kata Kunci: Serangan Siber, Manajemen Keamanan, , Sistem Keamanan, Teknologi

PENDAHULUAN

Keamanan *cyber* telah menjadi isu yang semakin mendesak dalam era digital saat ini. Dalam beberapa tahun terakhir, kita telah menyaksikan peningkatan jumlah dan kompleksitas serangan *cyber* yang mengancam sistem komputer dan data di seluruh dunia. Serangan seperti pencurian data, serangan *malware*, peretasan, dan serangan *DDoS* telah menyebabkan kerugian finansial yang signifikan, kerusakan reputasi, dan gangguan pada operasi bisnis.

Tingginya tingkat ancaman ini mendorong perlunya upaya yang lebih kuat dalam memahami dan mengatasi tantangan keamanan *cyber*. Para peneliti dan praktisi di bidang keamanan informasi terus bekerja keras untuk mengembangkan strategi yang lebih efektif dalam melindungi data dan sistem komputer dari serangan siber. Penelitian ini bertujuan untuk menyelidiki aspek-aspek kunci yang terkait dengan keamanan *cyber* di era digital. Kami ingin memahami tantangan terbaru yang dihadapi oleh organisasi dan individu dalam menjaga keamanan data mereka. Selain itu, kami juga akan mengkaji strategi dan langkah-langkah keamanan yang paling efektif dalam melawan serangan siber.

Dengan memperoleh pemahaman yang lebih mendalam tentang keamanan *cyber*, diharapkan penelitian ini akan memberikan wawasan yang berharga kepada para profesional TI, perusahaan, dan pengguna individu tentang tindakan yang dapat mereka ambil untuk mengurangi risiko serangan siber. Melalui upaya kolaboratif antara akademisi, praktisi, dan pemerintah, kita dapat membangun lingkungan digital yang lebih aman dan dapat diandalkan.

Dunia *Cyber* atau dalam istilah Indonesia dikenal dengan dunia maya (atau disebut juga ruang siber atau mayantara; bahasa Inggris: *cyberspace*) merupakan sebuah media elektronik dalam jaringan komputer yang banyak dipakai untuk keperluan komunikasi satu arah maupun timbal-balik secara online (terhubung langsung). Kata "*cyberspace*" (dari *cybernetics* dan *space*) berasal dan pertama kali diperkenalkan oleh penulis novel fiksi ilmiah, William Gibson dalam buku ceritanya, "*Burning Chrome*", 1982 dan menjadi populer pada novel berikutnya, *Neuromancer*, 1984 yang menyebutkan bahwa: *Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding*. Jadi secara singkat kita dapat menyebutkan bahwa *Cyber Crime* adalah kejahatan yang terjadi di dunia siber.

Adapun definisi tentang cybercrime ini sangat banyak, baik menurut para ahli maupun berdasarkan peraturan perundang-undangan.

Cybercrime yaitu sebuah kejahatan yang ditujukan pada sebuah komputer atau *system* komputer. Peter menambahkan bahwa sifat kejahatan *cyber* sangat kompleks, dari hal sederhana seperti penyadapan atau pengintaian ke dalam sistem komputer yang mana kita tidak memiliki otorisasi terhadap komputer tersebut, atau kejahatan berupa penyebaran virus yang dilakukan oleh seorang karyawan yang merasa tidak puas terhadap kebijakan dalam organisasinya. *Cyber crime*, atau kejahatan di dunia maya, adalah jenis kejahatan yang dilakukan melalui komputer dan jaringan. Komputer sendiri merupakan alat utama untuk melakukan *cyber crime* ini, tetapi seringkali komputer juga dijadikan sebagai target dari kejatahan ini. Biasanya, *cyber crime* membahayakan seseorang karena pencurian data

hingga keuangan.

Dunia maya ini merupakan gabungan dari berbagai peralatan teknologi komunikasi dan jaringan komputer yang dapat menghubungkan peralatan komunikasi (komputer, telepon genggam, instrumentasi elektronik, dan lain-lain) yang tersebar di seluruh penjuru dunia secara interaktif. Ada beberapa jenis *cyber crime* yang kerap kali ditemui ketika beraktivitas di dunia maya, antara lain:

a. E-Commerce
Kegiatan perdagangan yang dilakukan melalui layanan elektronik, dalam hal ini melalui sarana internet baik sistem promosi, sistem transaksi, sistem pembayaran, dan lain-lain. Landasan yang dipakai adalah electronic basen dan *Information Technology*, khususnya Internet dan Web. Dengam hadirnya *E-Commerce*, perdagangan dapat dilakukan sangat efektif, karena publik dapat mengakses suatu toko dari rumah masing-masing, tanpa harus memasuki toko atau perusahaan tersebut.

b. Website perusahaan dapat dianggap sebagai sebuah toko, karena dalam.
Website itu tersedia ruangan-ruangan maya yang menyediakan layanan spesifikasi barang-barang yang diperdagangkan. Adapun motif kejahatan yang terjadi dalam komunitas *E-Commerce* ini, bisa berbentuk pemalsuan kartu kredit, persaingan usaha tidak sehat, monopoli barang perdagangan, HaKI, dan lain-lain.

c. Cybersex
Cybersex adalah dunia pornografi yang dilakukan di internet, yang dapat diakses secara bebas. Ada yang membayar, namun ada juga yang gratis. Situs ini dapat diakses bebas, meskipun mereka masih belum cukup umur.

d. Hacker
Hacker adalah orang yang memasuki atau mengakses jaringan komputer secara tidak sah (tanpa ijin) dengan suatu alat dan progran tertentu, bertujuan untuk merusak, merubah data dengan menambah atau mengurangi kejahatan ini berdampak terhadap kerusakan jaringan komputer. Unsur-unsur kejahatan dimaksud belum terjangkau oleh undang-undang. Kalau kejahatan konvensional, seperti memasuki pekarangan orang lain tanpa ijin sudah jelas aturannya sebagaimana yang tertuang dalam pasal 167 KUHP. Kalau Hacker memasuki jaringan computer tidak secara fisik, melainkan menggunakan alat dengan program tertentu. Dengan *system* hukum yang berlaku di Indonesia alat bukti elektronik seperti ini belum diatur, oleh karenanya saat ini diperlukan perangkat hukum khusus *Cybercrime*. Situs-situs milik pemerintah atau situs lainnya yang ditunjukan untuk konsumsi publik adalah situs potensial bagi semua pihak, dengan tujuan awal adalah untuk memberikan informasi yang diperlukan oleh masyarakat. Niat baik ini bisa rusak apabila ada tangan-tangan jahil yang berusaha untuk merusaknya. Apabila data yang disajikan itu adalah data pemerintahan sebagai pusat informasi, kalau dirusak karena kepentingan tertentu maka akan merugikan negara dan masyarakat. Belum lagi kalau ada yang berusaha untuk menyusup ke situs tersebut kemudian merubah segala data yang ada.

e. Cyber Terrorism
Cyber terrorism, atau terorisme siber, merupakan salah satu jenis *cyber crime* yang merugikan negara, bahkan mengancam keselamatan warga negara dan pemangku kepentingan yang mengatur jalannya pemerintahan. Aktivitas *cyber terrorism* ini mengacu pada serangan terhadap komputer, jaringan, dan system informasi suatu negara dengan tujuan untuk mengintimidasi dan menekan pemerintah untuk kepentingan tertentu.

f. Penipuan OTP
OTP, atau *On Time Password*, adalah kode rahasia elektronik yang dikirimkan khusus kepada penggunanya. Biasanya, OTP akan dikirimkan ketika perusahan hendak melakukan transaksi keuangan secara online untuk memastikan bahwa perusahaan adalah pengguna aslinya. Penipuan

OTP ini adalah kejahatan yang dilakukan dengan cara mencuri kode rahasia elektronik tersebut. Biasanya, pelaku akan menyamar menjadi pihak dari suatu aplikasi di mana transaksi tersebut dilakukan agar korban dapat memercayainya dan memberikan kode OTP Kepada pelaku.

g. Phising
Phising adalah cara untuk melakukan penipuan dengan tujuan mencuri akun dari korban. Biasanya, pelaku mengincar korban melalui email atau pesan di dunia maya lainnya seperti pesan Facebook, Instagram, twitter, dan lain sebagainya. Phisingjuga dapat diartikan sebagai upaya untuk memperoleh informasi mengenai data seseorang dengan menggunakan teknik penipuan, biasanya dengan mengaku sebagai orang lain atau dengan mengirimkan sebuah link yang dapat mencuri informasi. Data dan informasi yang dimaksud adalah data pribadi seperti nama, umur, alamat, dan informasi akun tertentu atau bahkan data serta informasi keuangan.

Dengan adanya banyak sekali jenis *cyber crime* yang kerap kali dilakukan, maka ada banyak pula metode untuk melakukannya. Berikut ini adalah beberapa metode *cyber crime* yaitu :

a. *Password Cracker*
Password cracker adalah tindakan mencuri kata sandi dari akun orang lain dengan menggunakan program yang dapat mengenkripsi kata sandi. Tindakan ini juga sering dilakukan untuk menonaktifkan sistem keamanan kata sandi.

b. *Spoofing*
Spoofing adalah situasi di mana pelaku, atau program yang digunakan oleh pelaku, berhasil mengidentifikasi dirinya sebagai orang lain, biasanya pengguna aslidari komputer atau jaringan, dengan cara memalsukan data. Ada banyak cara spoofing yang dapat dilakukan seperti melalui email, SMS, dan lain sebagainya.

c. *DDoS (Distributed Denial of Service Attacks)*
DDoS merupakan serangan yang dilakukan pada server komputer atau jaringan dari korban. Serangan *DDoS* ini ditujukan untuk menguras sumber daya yang ada pada server komputer atau jaringan hingga tidak dapat lagi menjalankan fungsinya dengan baik.

d. *Sniffing*
Sniffing merupakan salah satu metode *cyber crime* di mana pelaku mencuri username dan kata sandi dari korban secara sengaja maupun tidak sengaja. Pelaku kemudian dapat menggunakan akun korban untuk melakukan penipuan yang mengatasnamakan korban atau merusak serta menghapus data korban.

e. Mengirimkan *Malware*
Metode *cyber crime* lainnya adalah dengan cara mengirimkan *malware* yang tujuannya untuk merusak atau menghancurkan data di server komputer atau jaringan korban. Beberapa yang termasuk ke dalam malware ini adalah virus, *worm*, *trojan*, *spyware*, *ransomware*, *adware*, dan lain sebagainya.

Bagi perusahaan dan bisnis, ada banyak sekali ancaman dari *cyber crime* ini, antara lain :

1. Pencurian Data Perusahaan
Ancaman yang pertama dari *cyber crime* terhadap sebuah perusahaan dan bisnis adalah pencurian data perusahaan. Data yang dimaksud di sini adalah inovasi produk, strategi bisnis, hingga laporan-laporan penting lainnya yang bisa disalahgunakan.

2. Pencurian Data Pegawai
Selain data dari perusahaan, data dari para pegawai yang bekerja di perusahaan tersebut juga bisa

dicuri. Nantinya, data tersebut bisa disalahgunakan untuk merusak nama baik perusahaan. Selain itu, hal ini juga sangat buruk dan dapat memengaruhi kinerja pegawai.

3. Pencurian Data Konsumen
   Data yang diberikan oleh konsumen merupakan data yang sangat sakral dan tidak boleh sampai tersebar luas. Jika sampai data dari konsumen ini dicuri dan disebarluaskan, hal tersebut jelas akan sangat merusak nama baik perusahaan. Selain itu, konsumen juga dapat menuntut perusahaan jika sampai data mereka disalahgunakan dan merugikan mereka secara langsung

Serangan kejahatan siber tidak hanya dapat memberikan dampak finansial atau operasional perusahaan. Berikut adalah beberapa kerugian yang harus ditanggung perusahaan jika lumpuh akibat serangan siber :

1. Dituntut Oleh Konsumen
   Jika data pribadi konsumen perusahaan dibocorkan oleh pihak penyerang, maka konsumen akan memiliki alasan kuat untuk mengajukan komplain hingga melayangkan gugatan pada perusahaan perusahaan. Hal ini dapat berujung pada kerugian finansial yang besar serta hilangnya kepercayaan konsumen serta orang lain terhadap perusahaan.

2. Bocornya Informasi Perusahaan
   Tidak hanya informasi pribadi konsumen perusahaan yang terancam ketika sistem jaringan perusahaan lumpuh; informasi perusahaan juga berada dalambahaya. Pelaku kejahatan siber bisa saja membocorkan strategi pemasaran atau bisnis perusahaan yang kemudian dapat berdampak pada dicurinya informasi-informasi perusahaan oleh kompetitor.

3. Rusaknya Reputasi Perusahaan
   Perusahaan tidak hanya akan mendapat kerugian dari segi finansil tapi juga reputasi. Ketika orang-orang tahu bahwa sistem jaringan bisnis, apa yang membuat mereka harus berbisnis perusahaan? Pada akhirnya, mereka akan mencari perusahaan lain untuk berbisnis dan hal ini tentu saja akan kembali menambah besar kerugian finansial perusahaan

Di dalam *cyber security* terdapat beberapa elemen yang menjadi fondasi. Berikut ini adalah beberapa elemen pokok *cyber security* tersebut :

1. Document *Security Policy Dokument* ini berupa kebijakan keamanan yang menjadi elemen standar acuan dalam menjalankan semua proses terkait keamanan siber. Dokumen ini menjadi panduan dan standar operasional prosedur dari *cyber security*.

2. Information Infrastructure
   Merupakan elemen perangkat keras dan perangkat lunak yang mendukung untuk melakukan aktivitas *cyber security*.

3. Perimeter *Defense*
   Perimeter *defense* merupakan elemen perangkat yang digunakan sebagai komponen utama dari pertahanan seperti *Intrusion Prevention System* (IPS), *Intrusion Detection System* (IDS) dan *firewall*. Dimana perangkat ini sebagai garda terdepan untuk pertahanan keamanan teknologi informasi.

4. *Network Monitoring System*
   Merupakan elemen media yang memiliki peran dalam memonitor jalannya perangkat cyber *security*. Selain itu juga memonitor infrastruktur dari keamanan siber seperti perangkat keras dan perangkat lunaknya.

5. *System Information and Event Management*
   Merupakan elemen sistem informasi dan insiden *handling* atau pencatatan dan pelaporan kejadian dalam menangani *cyber security*.

6. *Network Security Assessment*
   Elemen ini merupakan elemen *cyber security* yang memiliki peran untuk memberikan penilaian dan kontrol dalam mengukur level dari keamanan teknologi informasi atau keamanan siber.

7. *Human Resource dan Security Awareness*
   Elemen terakhir yaitu elemen manusia itu sendiri atau user dimana manusia adalah mata rantai terlemah dari keamanan teknologi informasi. Oleh karena itu, elemen ini perlu ditingkatkan kesadaran akan pentingnya keamanan teknologi informasi atas *cyber security*

Salah satu kegunaan dari keamanan siber adalah sebagai pengamanan infrastruktur dari perangkat telekomunika dan informatika. Biasanya penyerang akan mengganggu kinerja dari perangkat IT sehingga fungsi dari perangkat bisa tidak maksimal. Saat ini keamanan siber menjadi sangat penting karena tingginya ancaman *cyber crime*, dimana setiap tahunterjadi peningkatan *cyber attack*. Selain itu akibat negatif *cyber crime* sendiri negara dan korban personal menanggung kerugian finansial yang sangat besar. Karena bahayanya dari kejahatan *cyber* ini, maka keamanan *cyber* menjadi sangat penting.

Berikut manfaat dari cyber security yaitu :

- Dapat mencegah penggunaan yang tidak sah untuk masuk dan menggunakan *system* computer
- Dapat mempercepat perbaikan atau *recovery* setelah adanya serangan siber kedala sistem computer
- Dapat meningkatkan kepercayaan pelanggan jika perusahaan menerapkan *cyber security*. Sehingga membuat pelanggan merasa aman ketika berkomunikasi dengan kita atau produk perusahaan

Faktor-faktor yang mempengaruhi terjadinya *Cybercrime* ada 3 (tiga) faktor, yaitu :

1. Faktor Politik
2. Faktor Ekonomi
3. Faktor Sosial dan Budaya

Pelaku *cybercrime* yang sempat tertangkap kebanyakan remaja, bahkan beberapa pelaku terhitung masih anak-anak. Tentu mereka belum menduduki jabatan penting di masyarakat. Para pelaku ini juga jauh dari profil anak jalanan. Jarang terlibat kenakalan remaja. Mereka berawal dari keluarga baik-baik, dan rata-rata cerdas. Sejauh ini belum ada penelitian yang komprehensif tentang pelaku tindak pidana cybercrime modus operandi *cybercrime*, sulit dimengerti oleh orang-orang yang tidak menguasai pengetahuan Teknologi Informasi. Sebab, salah satu karakter pokok *cybercrime* adalah penggunaan Teknologi Informasi. Sifat inilah yang membuat *cybercrime* berbeda dengan tindak pidana lainnya.

METODE PENELITIAN

Penelitian ini mencoba mencari tahu kendala yang dihadapi perusahaan-perusahaan panas bumi/geothermal sebagai objek vital negara dalam *menghadapi* cyber *attackt*.Untuk mencari tahu jawaban penelitian tersebut, maka diperoleh teori *cyber*, jenis-jenis cyber dan metode *cyber attack* yang sering digunakan oleh para pelaku. Teori *cyber* menjelaskan bahwa definisi *cyber* didalam proses sehari-hari yang dijalani oleh perusahaan.

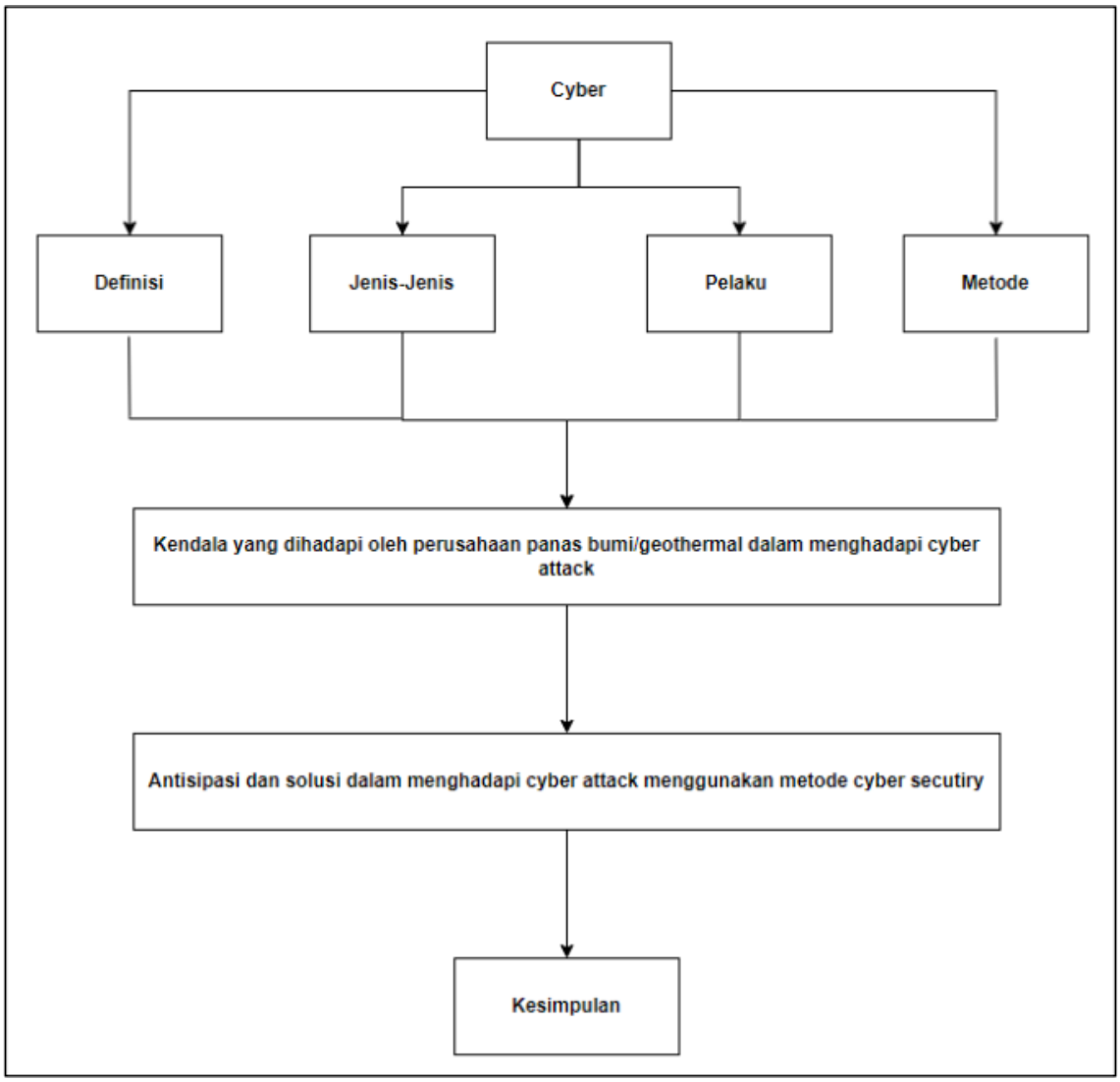
Penelitian *Cyber Security* secara deskriptif pada perusahaan panas bumi/geothermal dilakukan dari Universitas Bhayangkara Jakarta Raya tahun 2022. Riset ini termasuk penelitian deskriptif kualitatif karena mendeskripsikan hasil riset penelitian fenomena atau peristiwa yang terjadi pada perusahaan

geothermal atas *cyber attack*. Riset di atas menggunakan metode penelitian deskriptif kualitatif untuk menganalisis data primer maupun sekunder dengan cara mendeskripsikan, menjelaskan, dan memvalidasi temuan-temuan riset.

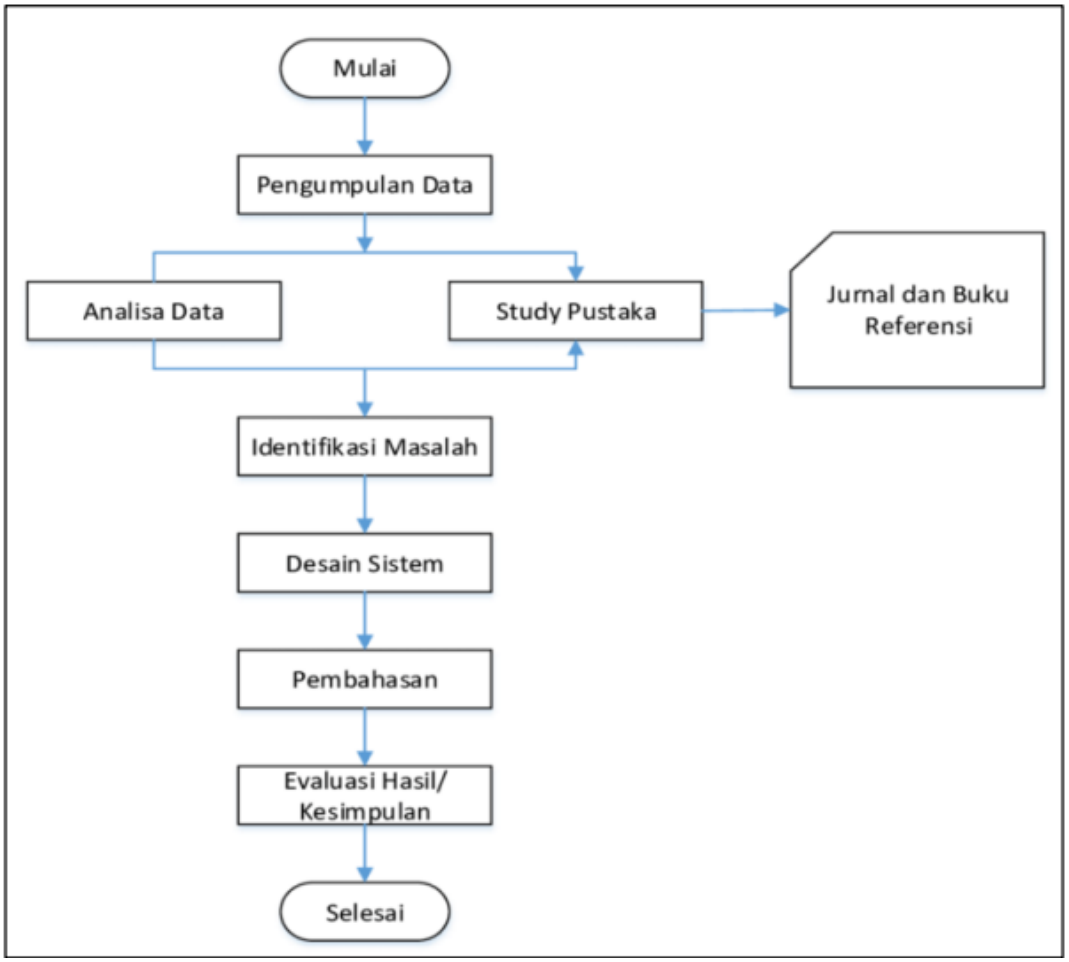
Adapun tahapan penelitan yang dilakukan adalah pengumpula data-data seperti *cyber attack* yang terjadi pada perusahaan geothermal dan dampak yang diakibatkan pada seluruh proses system keseluruhan perusahaan *geothermal*. Selanjutkan dilakukan analisa data dan studi pustaka melalui jurnal dan buku referensi. Kemudian mengindentifikasi masalah sebagai dasar untuk melakukan antisipasi dan solusi menghadapi *cyber attack* melalui desain *system* dan pembahasan. Langkah terakhir adalah kesimpulan penelitan.

Penelitian dilakukan pada salah satu perusahaan *geothermal* yang telah beroperasi sejak tahun 2000 silam yaitu perusahaan X yang berlokasi di Kecamatan Pangalengan, Kabupaten Bandung Selatan, Jawa Barat. Sementara untuk waktu penelitan dilakukan pada bulan Mei 2023.

Untuk melakukan penelitian tentang keamanan *cyber* di era digital, berikut adalah metodologi yang dapat digunakan :



Gambar 1. Kerangka Penelitian



Gambar 2. Tahapan Penelitian

HASIL DAN PEMBAHASAN

Berdasarkan data yang telah dikumpulkan, bahwa serangan *cyber* yang paling sering terjadi pada perusahaan panas bumi/*geothermal* adalah *ransomware, craking, pishing,* dan *hacking* dimana serangan tersebut terjadi pada *system* perusahaan maupun karyawan melalui e-mail perusahaan yang sering di bajak dan kehilangan seluruh data yang telah di *compile*. Sehingga *system* pada perusahaan mengalami kelumpuhan total dan tidak dapat beroperasi semestinya. Hal ini menjadi salah satu perhatian utama, dimana *control room power plant* menggunakan computer yang saling terhubung akan menghambat proses *generation* ketika ada *cyber attack*. Begitu juga dengan *database* data yang dibutuhkan sewaktu-waktu untuk mengatasi/menyelesaikan masalah yang terdapat pada sumur atau fasilitas *power plant*. Hal ini menjadi salah satu perhatian utama oleh perusahaan untuk meningkatkan *cyber security* secara massive terhadap berbagai aspek terumata pada *system* informasi dan teknologi milik perusahaan.

Dengan melakukan improvisasi pada *cyber security* perusahaan mampu menjalankan kegiatan operationalnya dengan efisien dan berkelanjutan yang saling terintegrasi satu dengan lain dalan mempermudah load job pekerjaan para karyawan pada berbagai divisi. Perusahaan sebelumnya menggunakan *Frakas* sebagai *system database* dimana terdapat beberapa kelemahan seperti *maintenance* dan *backup* data yang cukup lama sehingga dapat mengganggu proses operasional *power plant* begitu juga dengan tim yang bekerja di kantor. Namun, dengan adanya pembaharuan pada *system* dimana menggunakan aplikasi *system* yang saat ini digunakan, isu-isu tersebut sudah dapat terselesaikan dengan baik sehingga kegiatan operation menjadi lebih efisien dan efektif. Kemudian masalah *ransomware, craking, pishing, dan hacking* juga dapat terselesaikan dengan baik dan maksimal dengan menggunakan *system* yang terbaru tersebut.

Biaya untuk membangun dan mengelola infrastruktur TI pada perusahaan *geothermal* ini cukup tinggi terutama untuk biaya infrastruktur *networking* dan *server*. Hal yang terpenting perusahaan panas bumi ini biasanya tidak bersifat tetap dan jangka panjang, dikarenakan menunggu hasil dari produksi dimana jika tidak berhasil dalam pengeboran maka ada kemungkinan perusahaan akan berhenti kegiatan operasionalnya/ditutup . Dari ulasan diatas penulis mengusulkan untuk menggunakan *Co-location server* yang difasilitasi oleh satu provider *data center* untuk mengelola infrastruktur TI untuk *networking* dan pengelolaan *server* sehingga mendapatkan biaya yang minimal.

Seiring meningkatnya pertumbuhan *Data Center* data-data layanan data yang digunakan bersama (shared resources) dalam suatu pusat data dengan menggunakan jaringan/*networking*. *Co-location server* adalah sebuah layanan yang menyediakan tempat untuk menyimpan atau menitipkan server yang dimilikinya ke sebuah *data center*. *Data center* yang menyediakan layanan ini memiliki standar keamanan fisik dan infrastruktur yang mendukung. Selain itu, penyedia layanan ini harus memastikan dalam kestabilitan arus listrik, suhu, UPS, akses internet, *power generator, flooring*, dan CCTV. Selain itu, dari segi keamanan juga harus tinggi penjagaannya. Pada layanan ini, *server* akan diletakkan dan disimpan di dalam rak atau kabinet khusus server. Kelebihan dari layanan ini adalah biaya yang dikeluarkan tidak bergantung dengan spesifikasi *server* yang dititipkan karena yang dikenakan kepada pengguna adalah biaya sewa tempat tersebut di *data center*. Namun, kekurangannya adalah pengguna yang menyewa tempat di *data center* tersebut harus bertanggung jawab penuh terhadap servernya sendiri, termasuk apabila terjadi kerusakan di dalamnya.

Co-location server pada *data center* merupakan teknologi yang memanfaatkan layanan menggunakan pusat server yang disediakan oleh suatu *data center* dan bersifat virtual dengan tujuan pemeliharaan data dan aplikasi. Selain itu *Co-location server* menjadi trend teknologi informasi yang significant dalam meningkatkan kecepat transfer/lalu lintas data dan meminimalkan penggunaan biaya operasi pengolahan data. Perusahaan panas bumi yang memiliki user atau pengguna yang cukup banyak sehingga sangat sesuai menggunakan teknologi komputasi awan terutama untuk lalu lintas data dan mempercepat hantaran layanan data, fungsi pengolahan data dan penyimpanan data. Perusahaan tersebut yang membutuhkan *resource* yang besar dalam penggunaan e-mail, website , *hosting files* dalam bentuk gambar , suara , video. Selain itu Perusahaan tidak perlu mengeluarkan biaya untuk melakukan pengembangan dan pemeliharaan *server* karena fasilitas ini sudah banyak yang ditawarkan oleh beberapa *Data Center*.

Organisasi menggunakan *co-location server* dan pemeliharaan data pada *data center* untuk memberikan kemampuan pengolahan data secara terpusat diseluruh perusahaan. *Data center* menyimpan dan mengelola sejumlah besar data yang bersifat *mission-critical*. Lima elemen utama yang penting untuk fungsi dasar dari sebuah data center adalah aplikasi, *database*, *server* dan *operating system*, jaringan dan *storage*. *Data center* dapat diklasifikasikan menjadi beberapa *Tier*. *Tier* 1 merupakan model data center yang paling sederhana dan biasanya dapat disebut juga ruang server. Tier 4 merupakan model *data center* paling ketat dan lengkap dimana *data center Tier* 4 dirancang khusus untuk menampung sistem komputer yang bersifat kritikal. *Tier* 4 ini, dilengkapi dengan komponen *redundant*. Perusahan ini tidak perlu membangun infrastuktur seperti membangun jaringan (*network*) , membuat aplikasi dan server. Dimana sebagian besar perusahan migas dapat beroperasi dalam waktu jangka pendek tergantung kontrak kerja dengan pemerintah. Dibawah ini adalah gambaran dari konfigurasi /topologi dari perusahaan eksplorasi panas bumi.

Pada tulisan ini dilakukan analisa biaya dan keuntungan dengan menggunakan sehingga dapat diketahui penggunaan *co-location server* dapat meminimalkan penggunaan biaya operasi pengolahan dan komputasi data. Selain itu perusahaan eksplorasi migas ada yang keberadaannya perusahaannya tidak berlangsung lama tergantung dari hasil reservoir atau cadangan yang ada dan kontrak kerja. Ada beberapa aplikasi yang yang disimpan dan di jalankan di beberapa *server* yang terpisah seperti JDE (*Finance*), *Human Resource* (HRIS) , *HSE Portal*, *Production* (SOT) , E-mail dll.

Antisipasi yang dapat dilakukan oleh perusahaan geothermal dalam menghadapi *cyber attack* adalah :

1. Memodifikasi dan memperbarui keamanan siber
   Cara mencegah *cyber attack* pada sektor migas selanjutnya adalah dengan melakukan pembaruan *Operating System*, instalasi *software* ICS, dan pemeriksaan rutin. Hal tersebut dilakukan untuk memastikan antivirus dan *software* keamanan lainnya berfungsi dengan baik. Selain itu, perusahaan juga perlu memantau *remote access point* dan port *Remote Desktop Protocol* yang tidak digunakan.

2. Melakukan Enkripsi
   Perlu adanya *end-to-end encryption* dan keamanan yang tersemat pada setiap perangkat. Selain itu, dalam beberapa kasus juga diperlukan adanya sertifikat SSL untuk menghindari perangkat palsu. Hal ini juga akan melindungi dari side channel attack yang dapat membahayakan kunci enkripsi.

3. Menerapkan Prosedur Otentikasi Dan Akses Kontrol
   Perusahaan haruslah menerapkan prosedur autentikasi dan otorisasi yang ketat untuk karyawan dan semua perangkat lunak. perusahaan dapat mengembangkan langkah-langkah kontrol akses untuk mencegah akses yang tidak sah ke sistem *cyber*.

4. Melakukan Pengujian Penetrasi Dan Audit Internal
   Semua fasilitas di lingkungan industri *geothermal* haruslah menerapkan penilaian kerentanan yang ketat, serta audit pengujian penetrasi secara teratur untuk memastikan analisis sistem operasional yang berkelanjutan.

5. Menyediakan Pelatihan Kesadaran Karyawan
   Semua karyawan yang bekerja pada sistem kritis harus memiliki pelatihan atau sertifikasi yang tepat untuk mendukung tingkat ancaman yang lebih tinggi dari posisi mereka. Mereka juga perlu membangun kesadaran untuk mencegah serangan *cyber* seperti *phising*, serta menerapkan *cyber hygiene* yang tepat untuk memastikan keamanan yang efektif.

6. Melakukan *Backup Data*
   Lakukan pencadangan data penting dan buatlah salinan cadangan yang dilindungi kata sandi secara *offline*. Perusahaan juga dapat memastikan jika salinan data penting tidak dapat diakses untuk modifikasi atau penghapusan dari sistem tempat data berada.

7. Membuat Rencana Pemulihan
   Setelah mengupayakan cara mencegah *cyber attack* pada *geothermal*, dapat membuat rencana pemulihan dengan menyimpan salinan data dari *server* sensitif dan eksklusif di lokasi yang aman, tersegmentasi, dan terpisah secara fisik. Lokasi tersebut termasuk *hard drive*, perangkat penyimpanan, dan *cloud*.

8. Memastikan Keamanan Kata Sandi
   Pastikan perusahaan menggunakan kata sandi yang kuat. Jika memungkinkan, Anda juga dapat memanfaatkan *Multi-Factor Authentication* (MFA). Jangan lupa untuk memperbarui kata sandi secara teratur untuk sistem dan akun jaringan, serta hindari penggunaan kembali kata sandi yang sama untuk banyak akun.

9. Keamanan Email
   Pertimbangkan untuk menambahkan spanduk email ke pesan yang berasal dari luar organisasi dan nonaktifkan *hyperlink* di email yang diterima.

KESIMPULAN DAN SARAN

Kesimpulan dari penelitan ini adalah bahwa serangan *cyber* yang paling sering terjadi pada perusahaan panas bumi/*geothermal* adalah *ransomware, craking, pishing, dan hacking* dimana serangan tersebut terjadi pada *system* perusahaan maupun karyawan melalui e-mail perusahaan yang sering di bajak dan kehilangan seluruh data yang telah di *compile*. Hal ini menjadi salah satu perhatian utama, dimana *control room power plant* menggunakan computer yang saling terhubung akan menghambat proses generation ketika ada *cyber attack*. Begitu juga dengan *database* data yang dibutuhkan sewaktu-waktu untuk mengatasi/menyelesaikan masalah yang terdapat pada sumur atau fasilitas *power plant*. Dengan melakukan improvisasi pada *cyber security* perusahaan mampu menjalankan kegiatan operationalnya dengan efisien dan berkelanjutan yang saling terintegrasi satu dengan lain dalan mempermudah *load job* pekerjaan para karyawan pada berbagai divisi. *Co-location server* menjadi trend teknologi informasi yang significant dalam meningkatkan kecepat transfer/lalu lintas data dan meminimalkan penggunaan biaya operasi pengolahan data. Perusahaan panas bumi yang memiliki user atau pengguna yang cukup banyak sehingga sangat sesuai menggunakan teknologi komputasi awan terutama untuk lalu lintas data dan mempercepat hantaran layanan data, fungsi pengolahan data dan penyimpanan data. Perusahaan tersebut yang membutuhkan resource yang besar dalam penggunaan *e-mail*, *website* , *hosting files* dalam bentuk gambar, suara, video.

Penelitian ini jauh dari sempurna dan perkembangan ancaman *cyber* semakin meluas dan sulit untuk dibendung, untuk itu kiranya ada penelitian yang lebih teknis dalam penguatan *cyber security* untuk menghadapi tantangan dunia global di masa yang akan datang.

UCAPAN TERIMA KASIH

Bagian ini disediakan bagi penulis untuk menyampaikan ucapan terima kasih, baik kepada pihak penyandang dana penelitian, pendukung fasilitas, atau bantuan ulasan naskah. Bagian ini juga dapat digunakan untuk memberikan pernyataan atau penjelasan, apabila artikel ini merupakan bagian dari skripsi/tesis/disertasi/makalah konferensi/hasil penelitian.

DAFTAR PUSTAKA

2004, Keputusan Presiden RI No 63 Tahun 2004 tentang Pengamanan Objek Vital Nasional. Jakarta, Sekretariat Negara.

2005, Surat Keputusan kapolri No.Pol. : Skep/738/X/2005 tanggal 13 Oktober 2005 tentang Pedoman Sistem Pengamanan Objek Vital.

Cakrawala, Apa Itu Cyber security? Mengapa Cyber security Kini Makin Penting? https://infokomputer.grid.id/read/122710604/apa-itu-cyber-security-mengapa- cyber-security-kini-makinpenting?page=all (Diakses tanggal 29 May 2023)

Dasep Lukiman, Cyber security: Apa Itu Cyber security?, https://wakool.id/blog/582-cyber- security-apa-itucyber-security (Diakses tanggal 29 May 2023)

Maskun. (2013) Kejahatan Siber, Cybercrime : Suatu Pengantar. Jakarta, Kencana Prenada Media Group. Jakarta

Sutarman. (2007). Cybercrime: Modus Operandi dan Penanggulangannya. Jogjakarta, LaksBangPRESSindo.