Jurnal Ilmiah Cahaya Hukum : Jurnal Ilmu Hukum
Program Studi Magister Ilmu Hukum Universitas Mathla'ul Anwar
Volume 3. Nomor.2, Juli 2024

KOMINFO BERTANGGUNGJAWAB ATAS PERLINDUNGAN DATA PUBLIK TERKAIT SERANGAN SIBER DAN POLRI SEGERA SELIDIKI SIAPA PELAKUNYA

Penulis :

Asst Prof. Dr.H.Suhardi Somomoeljono, SH.,MH.
(Dosen MIH Pascasarjana UNMA Banten dan STIH ADHYAKSA Jakarta)

Abstrak

Peretas Sistem Pusat Data Nasional ("PDN") milik negara telah berahasil dijebol oleh pihak peretas (peretas adalah mengacu pada aktivitas intrusif[1] yang terkait dengan eksploitasi sistem komputer atau jaringan pribadi tanpa akses resmi). Sehingga sistim PDN selama lebih kurang tiga hari lumpuh dengan segala akibat yang ditimbulkannya antara lain terganggunya pelayanan publik di bandara soeta serta macetnya pelayanan publik yang dilakukan oleh imigrasi. Tentu saja kerugian-kerugian terkait lainnya secara diskriptif terutama terhadap perlindungan data pribadi milik publik berpotensi menjadi korban. UU Perlindungan Data Pribadi Kerusakan yang dialami oleh pusat data nasional kementerian komunikasi dan informatika (PSN Kominfo) bisa disebabkan oleh beberapa faktor bisa karena jaringan kelistrikan hingga serangan siber seperti DDos & Malware. Masalahnya perlindungan data pribadi milik rakyat Indonesia bisa terganggu bisa saja data pribadi itu dijual belukan di Dark Web (Dark web adalah bagian dari internet yang tidak diindeks oleh mesin pencari). Kalau sudah dicuri dan dijual belikan secara bebas dipasar gelap tentu ini menjadi tamparan keras bagi negara.Bagaimana data publik yang begitu besar bisa diakses oleh pihak yang tidak bertanggungjawab sehingga warga negara kita menjadi korbannya. Sebab identitas kita dicuri dan akan digunakan oleh pihak lain padahal mengenai hal ini telah diatur oleh UU PDP.

Keyword : Kominfo Bertanggungjawab Atas Perlindungan Data Publik Terkait Serangan Siber

[1] Asst Prof. Dr. Suhardi Somomoeljono, SH.,MH. *"Pengertian secara umum Intrusif thoughts adalah cara berpikir yang secara tiba-tiba memiliki keinginan untuk melakukan sesuatu yang tidak sejalan dengan akal sehat misal tiba-ada hasrat untuk meloncat dari sesuatu yang sangat membahayakan."*

Kejahatan Siber[2]

Dunia siber/maya (cyber space) tak dapat dipungkiri telah menjadi bagian hidup setiap manusia di era digital saat ini. Tanpa terasa dengan lahirnya internet dan kemajuan peralatan elektronik khususnya komputer telah menggiring manusia dalam pola hidup praktis, berbagai macam kegiatan dapat dieksekusi dari ujung jari saja secara virtual. Ya, dari mulai bebelanja berbagai kebutuhan barang, transaksi perbankan, permohonan dokumen kependudukan seperti Kartu Tanda Penduduk (KTP) dan Paspor, pola bekerja, tiket perjalanan serta berbagai jasa kebutuhan lainnya semuanya dapat diperolah dari aplikasi telepon seluler masing-masing.

Namun literasi dunia siber yang tidak merata di semua lini telah disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab untuk mengeruk keuntungan pribadi secara ilegal dari kondisi ini yang dikenal dengan istilah kejahatan siber (cyber crime). Sebagaimana dunia fisik dengan berbagai ragam kejahatannya dunia siber juga tidak luput dari tangan-tangan jahat yang berbekal literasi digital lebih dari pengetahuan kalangan masyarakat umum apalagi hari ini semua transaksi perbankan contohnya pembukaan rekening, gaji pegawai, transfer uang, pengelolaan tabungan semuanya telah dikelola melalui aplikasi berbasis internet. Oleh karena peningkatan literasi di bidang siber yang telah menjadi bagian kehidupan manusia dan seluk beluk keamanannya secara praktis adalah sebuah keniscayaan, tidak terkecuali anda.

Menurut National Institute of Standards and Technology (NIST), sebuah agensi dari Departemen Perdagangan Amerika Serikat yang misinya adalah untuk mempromosikan inovasi dan daya saing industri Amerika Serikat, definisi cyberspace (yang telah di-Indonesia-kan dalam Kamus Besar Bahasa Indonesia (KBBI) menjadi "siber" bermakna sistem komputer dan informasi/dunia maya) dunia siber/ruang siber adalah Jaringan infrastruktur teknologi informasi yang saling bergantung yang meliputi Internet, jaringan telekomunikasi, sistem computer, prosessor, dan sistem kontrol industri (Sumber : NIST SP 800-30 Rev. 1 under Cyberspace from CNSSI 4009 dan NIST SP 800-39 under Cyberspace from CNSSI 4009).

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 merupakan representasi grafis dari data yang diabstraksi dari bank setiap komputer dalam sistem manusia.

[2] Irfan Fanasafa. (2022, 14 Desember). Kenali Dunia Siber, Waspadai Kejahatannya! (Bagian I). Di akses pada 2 https://www.djkn.kemenkeu.go.id/artikel/baca/15712/Kenali-Dunia-Siber-Waspadai-Kejahatannya-Bagian-I.html5 Juni 2024.

Secara Sejarah, Istilah "cyberspace" pertama kali muncul dalam seni visual pada akhir 1960-an, ketika seniman Denmark Susanne Ussing (1940-1998) dan rekan arsiteknya Carsten Hoff membentuk diri mereka sebagai Atelier Cyberspace. Di bawah nama ini keduanya membuat serangkaian instalasi dan gambar berjudul "ruang sensorik" yang didasarkan pada prinsip sistem terbuka yang dapat beradaptasi dengan berbagai pengaruh, seperti gerakan manusia dan perilaku material baru.

Atelier Cyberspace bekerja pada saat Internet tidak ada dan komputer kurang lebih terlarang bagi seniman dan keterlibatan kreatif. Dalam wawancara tahun 2015 dengan majalah seni Skandinavia Kunstkritikk, Carsten Hoff mengenang, bahwa meskipun Atelier Cyberspace mencoba mengimplementasikan komputer, mereka tidak tertarik pada ruang virtual seperti itu.

Karya-karya Atelier Cyberspace awalnya ditampilkan di sejumlah tempat di Kopenhagen dan kemudian dipamerkan di Galeri Nasional Denmark di Kopenhagen sebagai bagian dari pameran "What's Happening?". Istilah "ruang maya" pertama kali muncul dalam fiksi pada 1980-an dalam karya penulis fiksi ilmiah cyberpunk William Gibson, pertama dalam cerita pendeknya tahun 1982 "Burning Chrome" dan kemudian dalam novelnya tahun 1984 Neuromancer. Dalam beberapa tahun berikutnya, kata tersebut menjadi jelas diidentifikasi dengan jaringan komputer online.

Selain itu, Don Slater menggunakan metafora untuk mendefinisikan dunia maya, menggambarkan "rasa dari pengaturan sosial yang ada murni dalam ruang representasi dan komunikasi itu ada sepenuhnya dalam ruang komputer, didistribusikan di jaringan yang semakin kompleks dan lancar." Istilah "Cyberspace" mulai menjadi sinonim de facto untuk Internet, dan kemudian World Wide Web, selama tahun 1990-an, terutama di kalangan akademis dan komunitas aktivis.

Pelaku Cyber Crime

Pelaku kejahatan siber dikenal sebagai *hacker* atau *cybercriminal* yang dijalankan secara individu atau tergabung dalam sebuah organisasi. Beberapa pelaku *cyber crime* memiliki *skill* mumpuni dan menggunakan teknik canggih sehingga mampu membobol *website* atau aplikasi dengan tingkat keamanan tinggi sekali pun.

Serangan Cyber Itu Apa Saja[3]

Kejahatan siber atau kerap dikenal dengan cyber crime merupakan tindak perilaku kejahatan berbasis komputer dan jaringan internet. Pelaku dari kejahatan siber biasanya akan

[3] Rini Pertiwi. (2021). Kenali 4 Jenis Kejahatan Siber. Di akses pada 25 Juni 2024 https://kominfo.kotabogor.go.id/index.php/post/single/740

meretas sistem untuk memperoleh data korban yang bersifat privasi. Terdapat berbagai jenis tindak kejahatan siber. Berikut empat jenis tindak kejahatan siber:

1. Penipuan Phising
   Seperti namanya, phising yang dapat diartikan pelaku "memancing" para korbannya untuk memberikan identitas dan informasi pribadi. Banyak orang yang tak sadar sedang terkena penipuan phising karena pelaku yang pintar berbicara dengan "memancing" pertanyaan-pertanyaan jebakan kepada korban.
2. Peretasan
   Peretasan merupakan upaya menyusup kepada sistem komputer tanpa izin. Beberapa hal yang biasa dilakukan para peretas yaitu membobol sistem, mencuri data pribadi, dan data keuangan.
3. Cyber Stalking
   Cyber Stalking atau Penguntitan siber merupakan penggunaan internet dan teknologi lainnya untuk menguntit atau meneror korban. penguntit akan melakukan sesuatu secara berulang-ulang. Selain membuat korban merasa terganggu, perilaku penguntit tersebut dapat pula membahayakan nyawa korban.
4. Cyber Bullying
   Cyber Bullying merupakan perundungan atau penindasan yang dilakukan secara online melalui internet dan teknologi lainnya. Biasanya hal ini terjadi pada kolom komentar di berbagai media sosial.

Banyaknya jenis kejahatan siber yang ada, membuat kita harus lebih waspada serta bijak dalam menggunakan media internet. Terlebih pelaku kejahatan siber tidak pandang bulu, sehingga siapa saja dapat menjadi korban kejahatan siber.

Jenis-jenis Cyber Crime yang Mengancam Keamanan Komputer[4]

Kejahatan siber dilakukan dalam berbagai macam aktivitas yang menyerang keamanan komputer atau *website* Anda. Namun, ada sebelas jenis kejahatan siber populer dan lazim dilakukan oleh *hacker* secara individu atau terorganisasi.

1. Pemalsuan Identitas
   Kejahatan siber ini sering terjadi di media sosial dan wajib diwaspadai pengguna internet. Pelaku mengambil identitas seseorang dari media sosial seperti foto, nama, dan informasi lainnya, kemudian memanfaatkannya untuk melakukan tindakan kriminal. Mereka bisa melakukan penipuan *online* dan pencucian uang berbekal identitas palsu tersebut.
2. *Phishing*

[4] Lintasarta Cloudeka. (2023,22 Mei). Ketahui 14 Jenis-Jenis Cyber Crime yang Harus Diwaspadai!. Di akses pada 25 Juni 2024. https://www.cloudeka.id/id/berita/web-sec/jenis-jenis-cyber-crime/#:~:text=Pelaku%20kejahatan%20siber%20dikenal%20sebagai,tingkat%20keamanan%20tinggi%20sekali%20pun.

Kejahatan ini dilakukan dengan mencuri informasi atau data sensitif seseorang melalui pesan atau tautan (*link*) palsu yang terlihat kredibel. Pelaku menghubungi target seperti biasa dan mengaku berasal dari pihak atau instansi tertentu, kemudian mencuri data sensitif mereka. Aktivitas *phishing* berjalan lebih mulus berkat kemajuan teknologi saat ini. Contohnya iklan *banner* di *website* yang dibuat menarik, padahal terdapat formulir yang meminta data sensitif di dalamnya untuk dicuri.

3. *Cracking*
   Aktivitas ini berupa percobaan penyusupan sistem komputer dengan meretas sistem keamanan komputer, jaringan, atau software-nya. Pelaku cracking alias cracker mencuri dan memanipulasi data tersebut untuk tujuan ilegal atau kriminalitas. Kejahatan siber ini wajib diwaspadai oleh tim IT perusahaan supaya sistem komputer atau website bisnisnya tetap aman, apalagi terdapat data pelanggan atau perusahaan di dalamnya.
4. *Spoofing*
   Spoofing sebenarnya mirip seperti phishing, yakni pelaku mengaku sebagai pihak berwenang dan mencuri data pelanggan untuk tujuan ilegal. Perbedaannya, spoofing bisa mengirimkan virus atau malware berbahaya ke perangkat atau website target. Apabila website tersebut diakses oleh pengguna, besar kemungkinan virusnya bisa menyebar ke perangkat mereka.
5. Serangan DDoS
   Distributed Denial of Service (DDoS) merupakan serangan yang dikirimkan oleh *hacker* untuk melumpuhkan *server website*. Serangan DDoS membuat *traffic website* berjalan lebih lambat sehingga *server*-nya mengalami *overload* akibat tidak mampu menampung banyak *request* dalam waktu bersamaan. Banyak sekali teknik serangan DDoS, salah satunya mengirimkan *bot* yang disisipkan dalam *malware*.
6. *Carding*
   Kejahatan ini menargetkan data atau informasi sensitif dari kartu kredit target, terutama nomor kartu dan PIN. Pelaku memanfaatkan data tersebut untuk mencuri saldo limit kartu atau melakukan transaksi secara ilegal. *Carding* dilakukan melalui dua cara, yaitu lewat *card skimmer* pada mesin EDC atau menggunakan media *online* seperti *e-mail phishing* atau *hacking*.
7. Pemalsuan Data
   Target serangan siber ini adalah data atau informasi dari dokumen penting yang tidak disimpan dengan proses enkripsi di internet. Dokumen tersebut disimpan dalam situs berbasis *web database* yang bisa diakses siapa pun, termasuk pelaku *cyber crime* itu sendiri. Contohnya, pemalsuan informasi alamat di surat undangan wawancara kerja suatu instansi sehingga korban memasukkan data pribadi untuk mendaftar lowongan kerja tersebut.
8. SIM Swap
   SIM Swap adalah jenis kejahatan siber di mana penjahat mencuri nomor telepon milik korban dengan mengganti kartu SIM korban yang sah dengan kartu SIM milik penjahat.

Setelah berhasil memasang kartu SIM tersebut, penjahat dapat mengakses akun *online* yang menggunakan verifikasi dua faktor (2FA) melalui nomor telepon korban.

Dengan mengambil alih nomor telepon korban, penjahat dapat mereset kata sandi dan mengakses akun korban, seperti akun media sosial, layanan perbankan, hingga dapat melakukan peretasan situs dan email.

SIM Swap sering kali membutuhkan banyak informasi pribadi yang dikumpulkan dari berbagai sumber, sehingga dapat menjadi upaya kejahatan siber yang rumit dan terorganisir.

9. Botnet

   Botnet adalah jaringan perangkat komputer yang dibajak yang digunakan untuk melakukan berbagai penipuan dan serangan siber. Istilah "botnet" terbentuk dari kata "robot" dan "*network*".

   Botnet menggunakan perangkat orang lain (perangkat yang dibajak) untuk menipu orang lain atau menyebabkan gangguan, dan semuanya dilakukan secara ilegal.

10. *Cyberstalking*

    Cyberstalking adalah salah satu kejahatan dunia maya yang dilakukan melalui media sosial, email, pesan teks, atau *platform* komunikasi *online* lainnya dengan tujuan mengintimidasi, menakut-nakuti, atau mempersekusi seseorang secara online. *Cyberstalking* biasanya dilakukan oleh seseorang yang memiliki motif untuk merugikan, mengintimidasi, atau membahayakan korban.

    Contoh perilaku *cyberstalking* antara lain mengirimkan pesan yang mengancam, memposting informasi pribadi korban, mengikuti dan memantau aktivitas korban di media sosial, atau bahkan melakukan serangan DDoS ke situs web atau akun korban.

11. Penipuan OTP

    Kejahatan ini dijalankan dengan cara mengirimkan pesan palsu berupa permintaan OTP untuk verifikasi aplikasi atau website. One Time-Password (OTP) merupakan rangkaian kode numerik dan digunakan sebagai password sekali pakai untuk proses verifikasi di aplikasi atau website. Biasanya, OTP tersebut digunakan ketika melakukan transaksi keuangan atau jual-beli secara ilegal.

12. Injeksi SQL

    Serangan ini memanfaatkan celah keamanan pada basis data aplikasi agar bisa disusupi kode yang berbahaya. Injeksi SQL terjadi karena developer aplikasi tidak menerapkan sistem keamanan yang ketat, yaitu penggunaan filter beberapa metakarakter dalam sintaks SQL. Akibatnya, hacker dapat memasukkan metakarakter di dalamnya supaya database aplikasi tersebut bisa diakses.

13. Cyber Espionage

    Jenis kejahatan siber ini berada di level tertinggi karena pelaku memanfaatkan sistem komputer untuk memata-matai target mereka. Organisasi hacker biasanya melakukan cyber espionage karena alasan politis dan menargetkan orang penting yang memiliki data

rahasia dalam sistem komputernya. Hacker menyusupkan spyware, yakni software untuk memantau aktivitas targetdalam komputer korban sehingga mereka bisa mengintai aktivitas dan data penting di dalamnya.

14. Serangan Malware
    Rata-rata kejahatan siber di atas memanfaatkan serangan malware untuk mencuri data korban serta melumpuhkan sistem komputernya. Namun, apakah serangan malware itu? Malware adalah program, software, atau file yang bisa membahayakan keamanan komputer. Software ini ditanamkan oleh hacker untuk meretas komputer target, kemudian mencuri data yang ada di dalamnya. Malware berasal dari mana saja, termasuk situs yang tidak menggunakan sertifikat SSL/TLS.

Sanksi Bagi Pelanggar Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi[5]

Secara garis besar dalam Udang-Undang No. 27 Tahun 2022 tentang Perilindungan Data Pribadi (UU PDP) tersebut, antara lain, diatur mengenai Lembaga Pelindungan Data Pribadi (PDP). Selain itu, juga diatur mengenai sanksi atau hukuman untuk pelanggaran UU PDP. Sanksi berlaku bagi penyelenggara sistem elektronik (PSE), baik pemerintah (publik) maupun swasta (privat), perseorangan, serta korporasi.

Disebutkan, UU PDP mengamanatkan pembentukan Lembaga PDP berada di bawah presiden dan bertanggung jawab kepada presiden. Mengenai Lembaga PDP diatur dalam Pasal 58 dan 60 UU PDP.

Lembaga PDP memiliki sejumlah fungsi dan tugas, di antaranya, merumuskan dan menetapkan kebijakan serta strategi PDP, pengawasan penyelenggaraan PDP, penegakan hukum administratif terhadap pelanggaran UU PDP, dan memfasilitasi penyelesaian sengketa di luar pengadilan (out of court) terkait pelindungan data pribadi di ranah digital.

Secara spesifik, terkait dengan lembaga PDP, nanti akan berada di bawah presiden dan bertanggung jawab kepada presiden sebagai pengejawantahan sistem pemerintahan presidensial di Indonesia.
Dalam draf UU PDP, terdapat dua jenis sanksi bagi pelanggar data pribadi. Jenis pertama, bagi pengendali atau pemroses data pribadi jika melanggar ketentuan UU PDP. Di antaranya, tidak memproses data pribadi sesuai tujuannya dan tidak mencegah akses data tidak sah.

Sanksi hukum terdiri dari empat jenis, yaitu pertama, sanksi administratif dalam Pasal 57 UU PDP berupa peringatan tertulis; kedua, penghentian sementara kegiatan pemrosesan

[5] Kominfo.go.id. (2022, 24 September). Mengenal Sanksi Pelanggar Data Pribadi. Di akses pada 25 Juni 2024. https://www.kominfo.go.id/content/detail/44680/mengenal-sanksi-pelanggar-data-pribadi/0/artikel#:~:text=Untuk%20pelanggaran%20UU%20PDP%20memalsukan,atau%20denda%20sebesar%20Rp60%20miliar.

data pribadi; ketiga, penghapusan atau pemusnahan data pribadi; dan/atau keempat, denda administratif/paling tinggi dua persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

Jenis kedua, bagi orang perseorangan atau korporasi yang melakukan perbuatan terlarang. Di antaranya, mengumpulkan data pribadi yang bukan miliknya untuk menguntungkan diri sendiri atau orang lain mengungkapkan data pribadi yang bukan miliknya dan memalsukan data pribadi untuk keuntungan yang mengakibatkan kerugian bagi orang lain dapat dikenakan Pasal 67 sampai dengan 73 UU PDP.

Adapun ketentuan pidana diatur dalam UU sebagai berikut pertama pidana denda maksimal Rp4 miliar hingga Rp6 miliar, dan kedua, pidana penjara maksimal 4 tahun hingga 6 tahun.

Selain sanksi yang sudah disebutkan di atas, Pasal 69 mengatur pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian. Jika tindak pidana dilakukan oleh korporasi, menurut Pasal 70 UU PDP, dapat dikenakan hukuman denda sebesar 10 kali lipat dari yang pidana asli beserta penjatuhan pidana tambahan tertentu lainnya.

Untuk pelanggaran UU PDP memalsukan data pribadi dapat dipidana 6 tahun dan atau denda sebesar Rp60 miliar. Jika menjual atau membeli data pribadi akan dipidana 5 tahun atau denda sebesar Rp50 miliar. Korporasi yang kedapatan melanggar undang-undang ini dapat dikenakan pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan/pembekuan seluruh atau sebagian usaha korporasi sampai dengan pembubaran korporasi.

Faktor penyebab terjadinya kejahatan siber[6]

Kejahatan siber atau cyber crime merupakan sebuah tindak kejahatan yang dilakukan secara online. Jenis kejahatan ini biasanya tidak mengenal waktu maupun target sehingga siapapun bisa menjadi target. Oleh karenanya Anda harus waspada.

Tujuan dari kejahatan cyber ini cukup beragam. Ada yang hanya sekedar iseng dan ada juga yang masuk ke dalam kategori kejahatan serius hingga merugikan korbannya secara finansial. Dalam prakteknya kejahatan ini dapat dilakukan oleh individu maupun kelompok orang.

Para pelakunya tentu merupakan orang yang ahli dalam berbagai teknik hacking. Bahkan seringkali aksi kejahatan cyber ini dilakukan dari berbagai tempat yang berbeda namun di

[6] Indonet Team. (2024,30 Januari). Faktor yang menyebabkan Kejahatan Siber Mudah Terjadi. Di akses pada 25 Juni 2024. https://indonet.co.id/id/12-faktor-penyebab-kejahatan-siber-mudah-terjadi/

waktu yang bersamaan. Ada beberapa faktor yang dapat menyebabkan kejahatan siber menjadi lebih mudah terjadi.

Beberapa faktor tersebut tentunya sangat beragam sehingga memungkinkan serangan terjadi. Berikut adalah beberapa faktor yang dapat mempermudah terjadinya kejahatan siber:

1. Kerentanan Sistem Keamanan
   Kejahatan siber sering terjadi karena adanya kerentanan atau celah dalam sistem keamanan. Apalagi tak semua orang menjadikan keamanan sebagai prioritas. Bahkan ada juga yang mengabaikan sistem keamanan dan tidak memperbaharuinya secara teratur. Jika perangkat lunak atau sistem operasi tidak diperbarui secara teratur, kelemahan keamanan tertentu bisa dieksploitasi oleh penjahat siber. Akibatnya kejahatan siber menjadi sulit untuk dihindari.
2. Kurangnya Kesadaran Keamanan
   Sampai saat ini masih banyak orang yang belum menyadari dan memahami bahaya dunia digital. Kurangnya pemahaman dan kesadaran mengenai praktik keamanan digital dapat membuat individu atau organisasi mengabaikan masalah keamanan dasar seperti memperbarui kata sandi. Tak jarang banyak individu maupun organisasi asal klik tautan yang muncul meski mencurigakan tanpa memahami resiko keamanannya. Individu seperti inilah yang biasanya lebih rentan mengalami kejahatan siber. Hal ini karena tanpa sadar telah memudahkan para penjahat siber melakukan aksinya.
3. Kemajuan Teknologi
   Kemajuan teknologi memang semakin pesat. Keuntungan yang bisa diberikan oleh kemajuan ini juga sangat signifikan. Sayangnya meskipun teknologi memberikan banyak keuntungan, kemajuan teknologi juga dapat membuka pintu bagi penjahat siber. Perkembangan dalam kecerdasan buatan dan teknologi lainnya dapat digunakan untuk mengembangkan serangan yang lebih canggih dan sulit dideteksi. Terlebih jika tidak diiringi dengan pengembangan cara mengatasi serangan tersebut maka kejahatan siber bisa jadi akan semakin berkembang.
4. Anonimitas di Internet
   Anonimitas yang diberikan oleh internet dapat memotivasi penjahat siber untuk melakukan tindakan tanpa takut terkena sanksi hukum. Kemampuan untuk menyembunyikan identitas para ini membuatnya sulit untuk dilacak. Bahkan untuk menangkap pelaku kejahatan siber tergolong hampir mustahil. Jika bisa pun sudah pasti akan memerlukan waktu yang sangat lama.
5. Eksploitasi Manusia (Social Engineering)
   Penjahat siber sering menggunakan teknik sosial untuk memanipulasi individu atau karyawan agar memberikan informasi rahasia atau mengakses sistem yang aman. Kurangnya kesadaran terhadap teknik social engineering dapat membuat serangan semacam itu lebih berhasil dan mudah dilakukan.
6. Kurangnya Hukuman yang Tegas

Faktor penyebab kejahatan siber semakin mudah dan marak terjadi tentunya tak lepas dari lemahnya hukum yang ada. Memang seperti di Indonesia sendiri sudah ada pasal tersendiri mengenai kejahatan ini. Namun dalam prakteknya penanganan tentang kasus ini masih terbilang kurang. Inilah yang akhirnya membuat penjahat siber untuk terus melakukan serangan tanpa takut ditangkap atau dihukum.

7. Ketergantungan pada Teknologi
   Semakin banyaknya organisasi dan individu yang bergantung pada teknologi digital meningkatkan potensi serangan siber. Ketergantungan ini membuat banyak target yang menarik bagi penjahat siber yang mencari keuntungan finansial atau ingin menciptakan kerusakan.
8. Identitas Pengguna
   Faktor penyebab cyber crime lainnya adalah terkait identitas pengguna. Fitur-fitur yang mempermudah manipulasi privasi di platform media sosial seringkali dimanfaatkan oleh pengguna dengan niat yang tidak baik. Tidak hanya itu, data pengguna lain juga rentan terhadap pencurian memberikan peluang bagi pelaku kejahatan siber untuk melakukan manipulasi maupun kejahatan terhadap korban.
9. Replikasi Aset Informasi
   Pengguna media sosial dengan mudah dapat mereplika atau menggandakan aset informasi sehingga memberi peluang terjadinya kejahatan siber. Hal ini biasanya terjadi karena fitur penghapusan atau yang dikenal sebagai 'delete button' di dunia internet tidak tersedia. Oleh karena itu dalam bermain atau menggunakan media sosial Anda harus bijak. Jagalah dengan baik informasi pribadi yang sekiranya penting dan bisa menimbulkan kerugian atau kejahatan siber.
10. Lokasi
    Faktor selanjutnya yang bisa memicu munculnya ancaman serangan kejahatan siber adalah lokasi Anda bisa dideteksi dengan mudah di media sosial. Hal ini sama saja dengan memberi kemudahan untuk pemalsuan dan menjadi awal terjadinya kejahatan siber. Dengan lokasi ini orang asing bisa dengan mudah mengetahui lokasi hingga Alamat rumah Anda. Informasi lokasi tersebut kemudian bisa disalahgunakan untuk melakukan kejahatan siber.
11. Motivasi Finansial
    Motivasi Finansial juga bisa menjadi faktor penyebab kejahatan siber. Hal ini karena banyak sekali serangan siber dilakukan dengan tujuan mendapatkan keuntungan finansial. Untuk itulah pelaku kejahatan siber ini sampai nekat melakukan pencurian data pribadi, peretasan rekening bank, atau ransomware. Pelaku kejahatan siber ini bahkan tidak akan peduli pada kerugian yang dialami korbannya asalkan mendapat keuntungan finansial. Inilah kenapa kejahatan siber bisa menjadi kerugian yang sangat besar untuk para korbannya.

12. Kondisi Lingkungan Digital yang Dinamis
    Lingkungan digital yang terus berkembang dan berubah dengan cepat memberikan peluang bagi penjahat siber untuk mengeksploitasi celah keamanan yang baru muncul. Inilah yang kemudian membuat kejahatan siber semakin meningkat dan sulit dihentikan.

Kesimpulan

Dapat diduga kemungkinan telah terjadi kerentanan sistem adalah kelemahan perangkat lunak atau perangkat keras pada server atau klien yang dapat dieksploitasi oleh penyusup untuk mendapatkan akses atau mematikan jaringan keamanan menyebabkan sering terjadinya kejaharan siber karena adanya kerentanan atau celah dalam sistem keamanan yang tidak menjadikan sistem keamanan sebagai prioritas sehingga sistem keamanan terabaikan lebih-lebih jika tidak dilakukan update untuk memperbaruhinya secara teratur.

Sehingga secara teoritik asumsinya secara hukum pidana pihak korban dapat dilakukan penyelidikan siapa saja subjek hukumnya dan siapa pihak pelaku yang melakukan peretasan dan / atau memberikan peluang kesempatan sehingga memungkinkan pihak yang melakukan perbuatan peretasan baik langsung maupun tidak langsung menjalankan perbuatannya sehingga menyebabkan jebolnya server sistem Pusat Data Nasional ("PDN") milik Negara Kesatuan Republik Indonesia.

Daftar Pustaka

- Asst Prof. Dr. Suhardi Somomoeljono, SH.,MH. *"Pengertian secara umum Intrusif thoughts adalah cara berpikir yang secara tiba-tiba memiliki keinginan untuk melakukan sesuatu yang tidak sejalan dengan akal sehat misal tiba-ada hasrat untuk meloncat dari sesuatu yang sangat membahayakan."*

- Irfan Fanasafa. (2022, 14 Desember). Kenali Dunia Siber, Waspadai Kejahatannya! (Bagian I). Di akses pada 2 https://www.djkn.kemenkeu.go.id/artikel/baca/15712/Kenali-Dunia-Siber-Waspadai-Kejahatannya-Bagian-I.html5 Juni 2024.

- Rini Pertiwi. (2021). Kenali 4 Jenis Kejahatan Siber. Di akses pada 25 Juni 2024 https://kominfo.kotabogor.go.id/index.php/post/single/740

- Lintasarta Cloudeka. (2023,22 Mei). Ketahui 14 Jenis-Jenis Cyber Crime yang Harus Diwaspadai!. Di akses pada 25 Juni 2024. https://www.cloudeka.id/id/berita/web-sec/jenis-jenis-cyber-crime/#:~:text=Pelaku%20kejahatan%20siber%20dikenal%20sebagai,tingkat%20keamanan%20tinggi%20sekali%20pun.

- Kominfo.go.id. (2022, 24 September). Mengenal Sanksi Pelanggar Data Pribadi. Di akses pada 25 Juni 2024. https://www.kominfo.go.id/content/detail/44680/mengenal-sanksi-pelanggar-data-pribadi/0/artikel#:~:text=Untuk%20pelanggaran%20UU%20PDP%20memalsukan,atau%20denda%20sebesar%20Rp60%20miliar.

- Indonet Team. (2024,30 Januari). Faktor yang menyebabkan Kejahatan Siber Mudah Terjadi. Di akses pada 25 Juni 2024. https://indonet.co.id/id/12-faktor-penyebab-kejahatan-siber-mudah-terjadi/