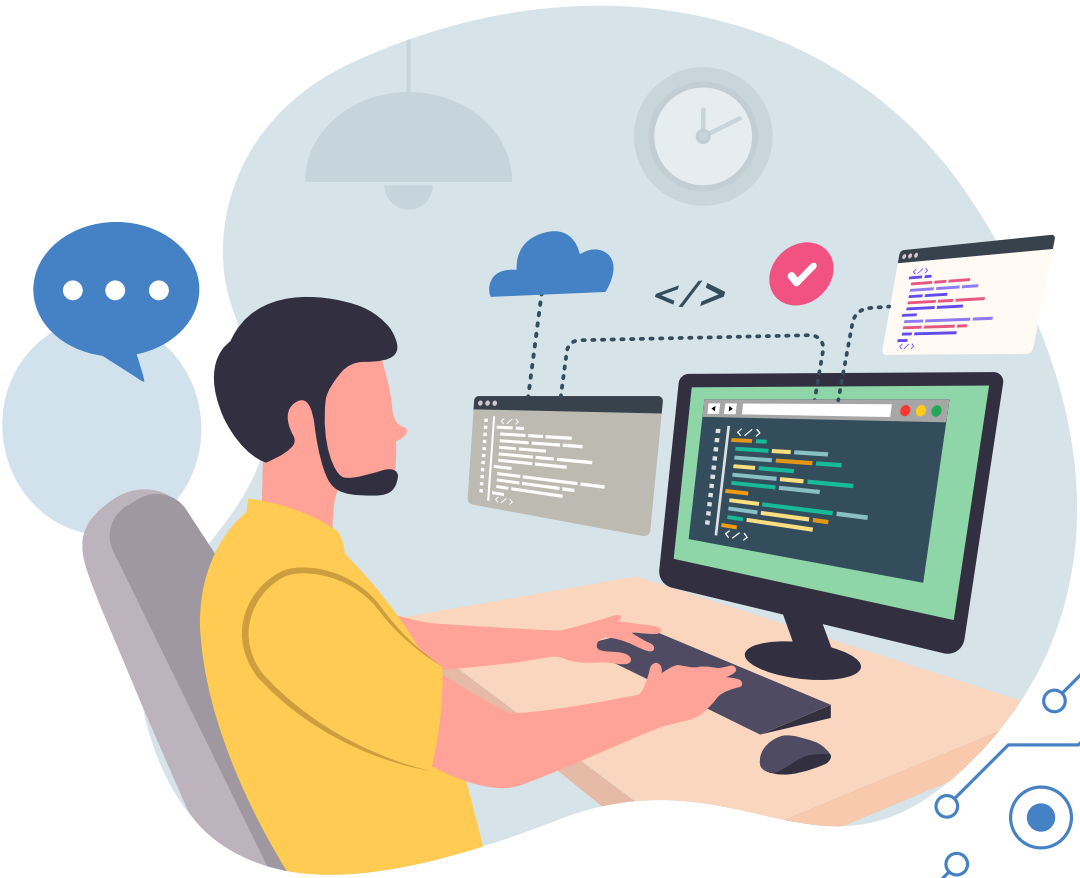
ISBN 978-623-125-444-3

KEAMANAN INFORMASI DAN PRIVASI DALAM TEKNOLOGI KOMPUTER



Penulis :
Deddy Rudhistiar, Muhammad Irwan Syahib,
Yendi Putra, Addin Aditya

KEAMANAN INFORMASI DAN PRIVASI DALAM TEKNOLOGI KOMPUTER

Deddy Rudhistiar
Muhammad Irwan Syahib
Yendi Putra
Addin Aditya

GET PRESS INDONESIA

KEAMANAN INFORMASI DAN PRIVASI DALAM TEKNOLOGI KOMPUTER

Penulis :
Deddy Rudhistiar
Muhammad Irwan Syahib
Yendi Putra
Addin Aditya

ISBN : 978-623-125-444-3

Editor : Diana Purnama Sari., S.E., M.E
Penyunting : Ari Yanto., M.Pd
Desain Sampul dan Tata Letak : Atyka Trianisa, S.Pd

Penerbit : GET PRESS INDONESIA
Anggota IKAPI No. 033/SBA/2022

Redaksi :
Jln. Palarik Air Pacah No 26 Kel. Air Pacah
Kec. Koto Tangah Kota Padang Sumatera Barat
Website : www. getpress.co.id
Email : adm.getpress@gmail.com

Cetakan pertama, Oktober 2024

KATA PENGANTAR

Segala Puji dan syukur atas kehadirat Allah SWT dalam segala kesempatan. Sholawat beriring salam dan doa kita sampaikan kepada Nabi Muhammad SAW. Alhamdulillah atas Rahmat dan Karunia-Nya penulis telah menyelesaikan Keamanan Informasi Dan Privasi Dalam Teknologi Komputer ini.

Buku ini membahas Keamanan Informasi Dan Privasi Dalam Teknologi Komputer, Kriptografi Dan Pengamanan Jaringan, Privasi Dan Kepatuhan Regulasi, Tantangan Terkini Dalam Keamanan Informasi.

Proses penulisan buku ini berhasil diselesaikan atas kerjasama tim penulis. Demi kualitas yang lebih baik dan kepuasan para pembaca, saran dan masukan yang membangun dari pembaca sangat kami harapkan.

Penulis ucapkan terima kasih kepada semua pihak yang telah mendukung dalam penyelesaian buku ini. Terutama pihak yang telah membantu terbitnya buku ini dan telah mempercayakan mendorong, dan menginisiasi terbitnya buku ini. Semoga buku ini dapat bermanfaat bagi masyarakat Indonesia.

Padang, Oktober 2024

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1
KEAMANAN INFORMASI DAN PRIVASI DALAM TEKNOLOGI KOMPUTER

Oleh Deddy Rudhistiar

1.1 Pendahuluan

Informasi pada umumnya adalah sebuah data atau gabungan beberapa data yang telah diproses terlebih dahulu sehingga dapat dapat memberikan makna yang berarti bagi penggunanya. Proses yang terjadi didalamnya membuat data yang awalnya merupakan data mentah menjadi hal penting baik itu untuk keperluan analisis dalam pengambilan keputusan, dalam berbagai sektor, seperti bisnis, pendidikan hingga pemerintahan. Sehingga dalam hal ini, informasi adalah aset penting bagi semua orang sehingga dibutuhkan keamanan yang serius. Dengan mempertimbangkan bahwa saat ini merupakan era digital yang dinamis, dimana data dengan mudah dapat menyebar luas.

Sebuah informasi tentunya mempunyai sebuah objek yang menjadi perhatian khusus bagi penggunanya, sehingga secara garis besar, informasi dikategorikan ke dalam dua kategori utama yaitu informasi ranah umum dan informasi ranah pribadi. Informasi yang termasuk dalam ranah umum biasanya tidak terdapat batasan-batasan karen bersifat terbuka sehingga dapat diakses oleh siapa saja. Contohnya informasi umum ini mencakup data statistik populasi, berita publik, atau informasi yang dipublikasikan secara luas di media sosial. Karena dengan sifatnya yang memang dirancang untuk konsumsi publik maka Informasi umum ini sering kali tidak menimbulkan risiko besar terkait privasi.

Informasi dalam ranah pribadi memiliki perlakuan khusus karena informasi pribadi mencakup data yang lebih sensitif, seperti identitas seseorang, data keuangan, riwayat medis, hingga kebiasaan pengguna di internet. Dalam hal ini undang-undang privasi dan regulasi perlindungan data digunakan untuk melidungi

informasi dengan mempertimbangkan dampak signifikan yang dapat terjadi apabila data ini jatuh ke orang lain yang berpotensi menyalah gunakan data, terutama dalam hal ini adalah data yang bersifat pribadi atau privat. Dan hal ini mengakibatkan informasi pribadi menjadi semakin penting seiring dengan meningkatnya ancaman keamanan siber, termasuk peretasan, pencurian identitas, dan pelanggaran data (Kaufman dkk., 2023).

Beberapa kasus besar tentang keamanan informasi dan privasi mencakup peretasan Yahoo (2013-2014), di mana 3 miliar akun pengguna dicuri, peretasan Equifax (2017) yang mengekspos data pribadi 147 juta orang, dan skandal Cambridge Analytica (2018), di mana data 87 juta pengguna Facebook digunakan tanpa izin untuk mempengaruhi pemilihan presiden AS. Ketiga kasus ini menyoroti kerentanan data pribadi di dunia digital, dengan perusahaan-perusahaan besar seperti Yahoo, Equifax, dan Facebook menghadapi sanksi hukum dan kehilangan kepercayaan pengguna karena gagal melindungi privasi mereka (Hammouchi dkk., 2019).

Dengan pemahaman yang mendalam tentang pentingnya melindungi informasi, baik yang bersifat publik maupun pribadi, kita dapat merumuskan pendekatan yang lebih tepat dalam penerapan keamanan dan privasi dalam teknologi komputer. Pemisahan informasi berdasarkan sifat dan tingkat sensitivitasnya menjadi landasan bagi pengembangan kebijakan dan prosedur yang lebih spesifik dan efektif. Hal ini memastikan bahwa dalam penanganan informasi bukan hanya menitik beratkan aspek teknis, tetapi juga memperhitungkan dimensi etika dan hukum yang harus dipatuhi oleh seluruh pihak yang berperan dalam pengelolaan data. Keamanan informasi, dengan demikian, menjadi tanggung jawab bersama yang melibatkan semua elemen organisasi dan masyarakat.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi adalah regulasi yang dirancang untuk memberikan perlindungan hukum terhadap pengelolaan data pribadi di Indonesia. Undang-undang ini penting untuk menjawab kebutuhan akan perlindungan privasi individu, terutama di era digital yang perkembangannya bisa terjadi perubahan yang cukup signifikan. Dalam konteks ini, data pribadi didefinisikan sebagai semua

informasi yang terkait dengan individu, baik secara langsung maupun tidak langsung, yang memungkinkan seseorang dapat diidentifikasi. Pengelolaan data ini mencakup pengumpulan, penyimpanan, pemrosesan, dan distribusi data oleh berbagai entitas seperti perusahaan swasta, instansi pemerintah, atau pihak lain yang memiliki kepentingan terkait.

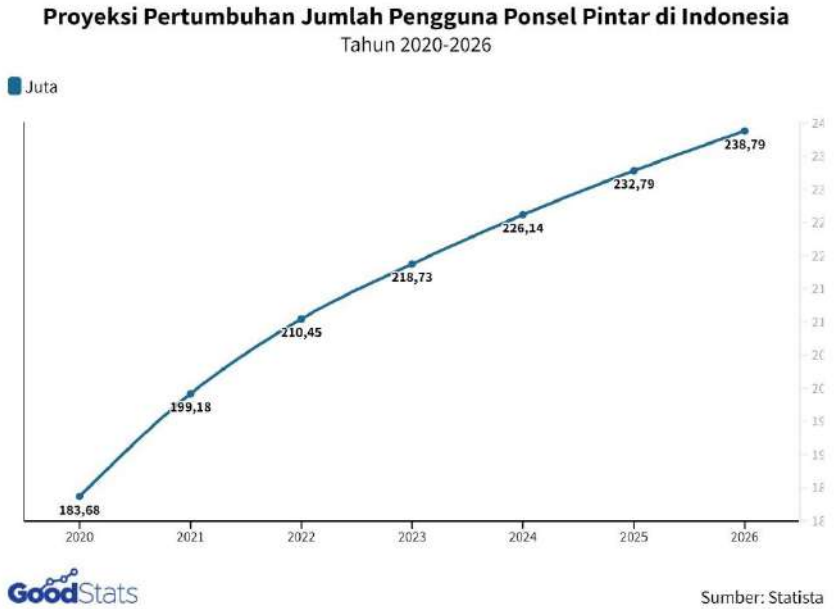
Keamanan informasi dalam dunia komputer adalah upaya untuk melindungi informasi dari berbagai ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data. Keamanan informasi mencakup perlindungan terhadap data sensitif, baik saat data tersebut disimpan maupun saat data sedang ditransmisikan melalui jaringan komputer. Berikut adalah penjelasan mengenai beberapa upaya sederhana yang dapat dilakukan untuk menjaga keamanan informasi, beserta keterbatasan-keterbatasannya: 1. Menggunakan Kata Sandi yang Kuat dan Unik. 2. Secara berkala mengganti Kata Sandi yang digunakan. 3. Tidak menggunakan Kata Sandi yang berhubungan dengan data pribadi.

1.2 Informasi dan Privasi di Era Digital

Transformasi ke arah Era Digital telah membawa perubahan yang signifikan dalam cara seseorang berinteraksi, mengakses informasi serta penyimpanan data. Dengan pertumbuhan pesat teknologi informasi, penggunaan internet, perangkat pintar, serta platform media sosial, privasi dan keamanan informasi menjadi dua aspek yang sangat penting. Dalam konteks ini, tantangan baru muncul, terutama dalam melindungi data pribadi dari akses yang tidak sah serta penyalahgunaan. Kejadian seperti bocornya data pribadi menjadi peringatan tentang betapa rentannya informasi kita di dunia digital.

Data pribadi yang tidak dilindungi dengan baik dapat dengan mudah diakses, dikumpulkan, dan disalahgunakan oleh pihak yang tidak bertanggung jawab. Salah satu contoh nyata adalah insiden Byorka yang mengguncang Indonesia pada tahun 2022. Hacker yang dikenal dengan nama Byorka berhasil mengakses dan membocorkan data pribadi beberapa pejabat tinggi Indonesia, serta mengklaim memiliki akses terhadap informasi rahasia pemerintah.

Kejadian ini menunjukkan betapa lemahnya perlindungan privasi dan keamanan informasi di beberapa sektor, serta betapa berbahayanya jika data jatuh ke tangan yang salah . Dampaknya tidak hanya menyentuh ranah privasi individu, namun juga keamanan nasional. Menurut laporan CNBC Indonesia, insiden ini menggambarkan ketidakmampuan sistem keamanan dalam menjaga data sensitif (Bestari, 2022) .



Gambar 1.1. Pertumbuhan jumlah pengguna ponsel pintar di Indonesia
(Sumber : Siahaan, 2023)

Selain insiden Byorka, kasus Pangkalan Data Nasional (PDN) juga menunjukkan kelemahan dalam pengelolaan data di sektor publik. Kebocoran informasi dalam sistem PDN yang melibatkan data strategis Indonesia menjadi alarm penting terkait kurangnya infrastruktur keamanan yang memadai. Kasus ini juga menyoroti pentingnya pengelolaan privasi yang ketat, terutama dalam menangani informasi yang bersifat sensitif dan strategis. Sebagaimana dilaporkan oleh *Kompas*, kasus PDN menunjukkan

bagaimana serangan siber bisa mengekspos kelemahan dalam sistem digital pemerintah (Hardiansyah, 2024).

Peristiwa-peristiwa ini menggambarkan bagaimana transformasi digital yang pesat harus diiringi dengan penguatan regulasi, kebijakan keamanan, serta kesadaran masyarakat tentang pentingnya menjaga privasi di dunia maya. Di era digital ini, informasi telah menjadi salah satu aset paling berharga, dan tanpa pengamanan yang memadai, informasi tersebut dapat dimanipulasi atau dicuri dengan mudah . Menurut David Solove dalam *Understanding Privacy*, privasi tidak hanya soal kerahasiaan, tetapi juga kontrol atas siapa yang memiliki akses ke data kita dan bagaimana data tersebut digunakan .

1.3 Aspek Keamanan Informasi Dan Privasi

Keamanan informasi mencakup serangkaian prinsip yang dirancang untuk melindungi data dari akses yang tidak sah, perubahan, atau gangguan. Dalam dunia digital, ada beberapa aspek penting yang menjadi pilar utama dalam menjaga keamanan informasi dan privasi, yaitu *Confidentiality* (Kerahasiaan), *Integrity* (Keaslian), *Availability* (Ketersediaan), dan *Authentication* (Autentikasi). Masing-masing aspek ini memainkan peran kunci dalam menjaga data agar tetap aman dan terpercaya.

1.3.1 *Confidentiality* (Kerahasiaan)

Kerahasiaan adalah konsep yang memastikan bahwa informasi hanya dapat diakses oleh individu atau entitas yang berwenang. Prinsip ini dirancang untuk mencegah kebocoran data kepada pihak yang tidak berkepentingan. Penggunaan enkripsi dan kebijakan akses terbatas adalah beberapa metode yang umum digunakan untuk menjaga kerahasiaan.

Insiden peretasan oleh Byorka pada tahun 2022 di Indonesia adalah contoh bagaimana pelanggaran terhadap kerahasiaan dapat menyebabkan kerugian besar. Dalam kasus ini, hacker tersebut berhasil mengakses dan membocorkan informasi pribadi beberapa pejabat tinggi negara, yang semestinya dijaga kerahasiaannya oleh sistem yang lebih kuat.

1.3.2 *Integrity* (Keaslian)

Keaslian atau integritas adalah prinsip yang memastikan bahwa informasi tidak diubah atau dirusak oleh pihak yang tidak berwenang. Data yang otentik harus tetap utuh dan tidak dimodifikasi tanpa persetujuan dari pihak yang berwenang. Sistem harus memastikan bahwa jika ada perubahan, perubahan tersebut terdeteksi dan dilaporkan.

Kasus manipulasi data keuangan dalam serangan ransomware adalah contoh pelanggaran terhadap prinsip integritas. Dalam serangan ini, hacker tidak hanya mencuri informasi tetapi juga memodifikasi data yang ada. Sebagai contoh, serangan ransomware WannaCry pada tahun 2017 mempengaruhi banyak institusi besar, termasuk lembaga kesehatan, yang tidak hanya menghadapi kehilangan akses terhadap data tetapi juga data yang diubah oleh hacker.

1.3.3 *Availability* (Ketersediaan) – Aplikasi BSI tidak bisa dipakai

Ketersediaan mengacu pada prinsip bahwa data dan sistem informasi harus selalu dapat diakses oleh pengguna yang berwenang kapan pun dibutuhkan. Ini mencakup langkah-langkah seperti perlindungan dari serangan *Distributed Denial of Service* (DDoS), pemeliharaan sistem, dan redundansi untuk memastikan bahwa layanan tidak terganggu.

Serangan DDoS pada 2020 terhadap beberapa bank besar di Indonesia adalah contoh bagaimana prinsip ketersediaan dapat dilanggar. Dalam serangan ini, layanan perbankan online terhenti karena server dibanjiri oleh permintaan palsu yang dibuat oleh hacker, sehingga pengguna yang sah tidak dapat mengakses layanan tersebut. Dampaknya sangat besar karena banyak pengguna yang tidak bisa melakukan transaksi penting dalam waktu yang cukup lama.

1.3.4 *Autentication* (Autentikasi)

Autentikasi adalah proses verifikasi identitas pengguna sebelum memberikan akses ke data atau sistem. Proses ini melibatkan penggunaan kata sandi, biometrik, atau autentikasi

multi-faktor (MFA) untuk memastikan bahwa hanya individu yang berhak yang dapat mengakses informasi tertentu.

Pelanggaran terhadap autentikasi terjadi dalam kasus peretasan akun-akun media sosial selebriti di Indonesia, di mana hacker berhasil membobol akun-akun tersebut melalui teknik serangan *phishing* dan eksploitasi kelemahan dalam sistem autentikasi. Contoh lain adalah penggunaan kata sandi yang lemah, yang memungkinkan hacker masuk ke dalam sistem dan mencuri informasi pribadi

1.4 Tindakan pelanggaran Keamanan

Dalam dunia digital komputer, pelanggaran keamanan informasi merupakan ancaman yang signifikan dan beragam, sehingga pada pada individu dan organisasi dapat menyebabkan kerusakan serius. Seiring dengan meningkatnya ketergantungan kita pada teknologi dan internet, risiko keamanan semakin kompleks dan meresahkan. Berbagai tindakan pelanggaran keamanan, seperti phishing, hacking, dan malware, dapat mengekspos data pribadi, merusak sistem, atau mengakibatkan pencurian informasi yang berharga. Upaya peretasan, kebocoran data, dan serangan yang melibatkan teknik manipulasi psikologis atau eksploitasi kerentanan perangkat lunak merupakan contoh nyata dari ancaman yang dihadapi dalam lingkungan digital saat ini. Dari tindakan pelanggaran keamanan yang sudah disebutkan, terdapat beberapa yang menjadi perhatian utama bagi tiap individu. Phishing, Hacking dan Malware memiliki dampak yang dapat menyebabkan kerusakan serius, tidak jarang hal ini diakibatkan oleh kelalaian pengguna dalam memanfaatkan teknologi informasi.

Phishing adalah salah satu bentuk tindak pelanggaran informasi di mana peretas mencoba mendapatkan informasi sensitif, seperti kata sandi atau nomor kartu kredit, dengan berpura-pura sebagai entitas yang sah. Serangan ini biasanya dilakukan melalui email atau pesan teks yang tampak resmi, mengarahkan korban untuk mengklik tautan berbahaya atau membuka lampiran yang dapat menginstal malware. Situs web palsu yang digunakan dalam serangan ini sering kali dirancang menyerupai halaman login resmi dari organisasi terpercaya, seperti bank atau layanan online,

untuk menipu korban agar memasukkan kredensial mereka. Dengan teknik manipulasi psikologis, pesan phishing mendorong korban untuk bertindak cepat, sering kali dengan ancaman atau peringatan palsu. Akibatnya, korban bisa kehilangan akses ke akun pribadi, mengalami pencurian identitas, kerugian finansial, atau bahkan infeksi malware pada perangkat mereka. Phishing yang sukses tidak hanya dapat mencuri data pribadi, tetapi juga menimbulkan dampak jangka panjang pada keamanan dan reputasi korban.

Hacking adalah tindakan ilegal yang dilakukan oleh peretas untuk mencoba memasuki sistem komputer atau jaringan tanpa izin dengan tujuan mengakses, mencuri, atau merusak data. Peretas menggunakan berbagai teknik, seperti eksploitasi kerentanan perangkat lunak, serangan brute force, atau rekayasa sosial, untuk mendapatkan akses ke sistem yang dilindungi. Serangan ini dapat berdampak serius pada individu maupun organisasi, termasuk pencurian informasi pribadi, data finansial, dan rahasia perusahaan. Selain itu, peretas dapat memanipulasi sistem, mengubah atau menghapus data, dan bahkan menyebabkan kerusakan infrastruktur digital yang mengakibatkan gangguan operasi bisnis atau layanan penting. Serangan hacking yang berhasil tidak hanya mengakibatkan kerugian finansial, tetapi juga bisa merusak reputasi, melumpuhkan operasional, dan memerlukan biaya besar untuk pemulihan sistem serta keamanan.

Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak, mencuri, atau mengganggu fungsi sistem komputer tanpa sepengetahuan pengguna. Malware dapat mengambil berbagai bentuk, seperti **virus**, yang menyebar dengan menginfeksi file atau program lain, merusak data, dan memperlambat kinerja perangkat. **Trojan** berpura-pura sebagai program yang sah, tetapi ketika diinstal, mereka memberikan akses kepada peretas untuk mengendalikan sistem dari jarak jauh. **Ransomware**, jenis malware yang semakin sering ditemui, mengenkripsi data penting pengguna dan menuntut tebusan untuk memulihkan akses, sering kali disertai ancaman bahwa data akan hilang atau dibocorkan. **Spyware** bekerja dengan diam-diam memantau aktivitas pengguna, mencatat informasi sensitif seperti kata sandi, informasi keuangan, atau data

pribadi. Dampak dari malware sangat merugikan, karena dapat mengakibatkan hilangnya data, pencurian informasi pribadi, dan bahkan pemerasan melalui tebusan. Selain itu, malware dapat menghancurkan infrastruktur sistem, mengganggu operasional, dan menyebabkan kerugian finansial yang besar serta rusaknya reputasi organisasi atau individu.

Memahami berbagai bentuk pelanggaran keamanan informasi dan dampaknya menjadi langkah krusial dalam upaya melindungi data dan sistem di era digital. Setiap jenis pelanggaran, mulai dari serangan phishing, hacking, hingga infeksi malware, membawa risiko yang signifikan terhadap integritas, kerahasiaan, dan ketersediaan informasi. Tanpa pemahaman yang mendalam, organisasi dan individu rentan terhadap ancaman yang dapat mengakibatkan hilangnya data, pencurian identitas, gangguan operasional, dan kerugian finansial yang besar. Dengan mengenali pola serangan dan memahami metode yang digunakan oleh penyerang, langkah-langkah perlindungan yang lebih efektif dapat diimplementasikan. Ini mencakup penerapan kebijakan keamanan yang ketat, penggunaan teknologi yang tepat, serta edukasi pengguna mengenai risiko keamanan. Pada akhirnya, kesadaran dan kesiapan yang baik dalam menghadapi ancaman ini akan memastikan bahwa informasi tetap aman, rahasia, dan tersedia saat dibutuhkan, menjaga kelangsungan bisnis dan kepercayaan pengguna di dunia yang semakin terhubung secara digital.

1.5 Upaya Peningkatan Keamanan dengan pendekatan Teknologi komputer

Untuk menghadapi berbagai ancaman keamanan informasi di era digital, upaya peningkatan keamanan melalui pendekatan teknologi komputer menjadi sangat penting. Salah satu langkah utama adalah dengan menerapkan enkripsi pada data sensitif, baik saat data tersebut disimpan maupun saat dikirimkan melalui jaringan. Enkripsi memastikan bahwa meskipun data diakses secara tidak sah, isinya tetap terlindungi dan sulit dibaca tanpa kunci dekripsi. Selain itu, autentikasi dua faktor (2FA) juga semakin banyak digunakan untuk menambahkan lapisan perlindungan tambahan pada proses login, sehingga meskipun kata sandi bocor,

penyerang tetap memerlukan kode verifikasi tambahan untuk mendapatkan akses. Firewall dan sistem deteksi serta pencegahan intrusi (IDS/IPS) juga dapat digunakan untuk memonitor lalu lintas jaringan dan mendeteksi aktivitas yang mencurigakan atau serangan yang sedang berlangsung. Pembaruan perangkat lunak secara berkala adalah langkah lain yang tidak boleh diabaikan, karena pengembang perangkat lunak secara rutin merilis patch untuk memperbaiki kerentanan keamanan. Virtualisasi dan segmentasi jaringan juga dapat membantu dalam membatasi akses penyerang ke bagian-bagian penting dari jaringan, sehingga jika terjadi serangan, dampaknya dapat diminimalkan. Dengan pendekatan teknologi yang tepat dan terus berkembang, organisasi dapat memperkuat pertahanan mereka dan mengurangi risiko dari ancaman digital yang semakin kompleks.

Dalam menghadapi ancaman digital yang terus berkembang, penting bagi organisasi untuk menerapkan strategi keamanan informasi yang komprehensif dan berlapis. Langkah-langkah seperti enkripsi data, baik saat penyimpanan maupun transmisi, memainkan peran penting dalam menjaga kerahasiaan informasi dari akses tidak sah. Ditambah dengan penerapan autentikasi dua faktor (2FA), risiko kebocoran informasi akibat pencurian kata sandi dapat diminimalkan, karena penyerang tetap membutuhkan verifikasi tambahan untuk mendapatkan akses. Penggunaan firewall dan sistem deteksi serta pencegahan intrusi (IDS/IPS) memungkinkan pemantauan lalu lintas jaringan secara real-time untuk mendeteksi aktivitas yang mencurigakan atau ancaman yang berpotensi merusak dan pembaruan perangkat lunak, sangat penting untuk menjaga integritas dan kerahasiaan informasi. Implementasi strategi keamanan yang komprehensif ini harus didukung oleh kebijakan keamanan yang jelas serta kesadaran yang tinggi dari setiap pengguna dalam mematuhi praktik terbaik dalam keamanan siber. Dengan pendekatan proaktif dan berkelanjutan, organisasi dapat lebih siap menghadapi tantangan keamanan yang terus berkembang dan memastikan perlindungan optimal bagi aset digital mereka.

DAFTAR PUSTAKA

Bestari, N.P. (2022) *Hacker Bjorka Tantang Pemerintah RI: Saya Menunggu Digerebek!*, *CNBC Indonesia*. Available at: https://www.cnbcindonesia.com/tech/20221226135118-37-400166/hacker-bjorka-tantang-pemerintah-ri-saya-menunggu-digerebek (Accessed: 10 September 2024).

Hammouchi, H. *et al.* (2019) 'Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time', *Procedia Computer Science*, 151, pp. 1004–1009. Available at: https://doi.org/10.1016/j.procs.2019.04.141.

Hardiansyah, Z. (2024) *Kronologi Serangan Ransomware ke PDN dan Penanganannya yang Tak Kunjung Usai*, *Kompas Indonesia*. Available at: https://tekno.kompas.com/read/2024/07/10/12350077/kronologi-serangan-ransomware-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai.

Kaufman, C. *et al.* (2023) *Network Security: Private Communications in a Public World, 3rd edition*. 3rd edn. Pearson.

Siahaan, M. (2023) *Smartphone users in Indonesia 2018-2028*. Available at: https://www.statista.com/forecasts/266729/smartphone-users-in-indonesia.

BAB 2
KRIPTOGRAFI DAN PENGAMANAN JARINGAN

Oleh Muhammad Irwan Syahib

2.1 Pendahuluan

Kriptografi adalah ilmu yang mempelajari tentang teknik-teknik matematika untuk mengamankan informasi. Sederhananya, kriptografi adalah seni dan ilmu untuk menyembunyikan pesan agar hanya pihak yang berwenang yang dapat memahaminya. Bayangkan kita ingin mengirim pesan rahasia kepada teman kita. Agar pesan tersebut tidak dibaca oleh orang lain, kita bisa mengacak huruf-huruf dalam pesan tersebut sehingga menjadi tidak terbaca. Proses pengacakan ini disebut enkripsi, dan proses mengembalikan pesan ke bentuk semula disebut dekripsi.

Berdasarkan definisi diatas maka bisa disimpulkan bahawa tujuan utama dari kriptografi adalah melindungi data dari akses yang tidak sah, manipulasi, dan penyalahgunaan. Secara spesifik, kriptografi bertujuan untuk mencapai empat hal utama:

1. Kerahasiaan: mencegah orang yang tidak berwenang membaca informasi, artinya hanya pihak yang berwenang yang dapat membaca informasi yang dikirimkan.
2. Integritas: menjamin bahwa data yang diterima sama persis dengan data yang dikirimkan, tanpa adanya perubahan atau kerusakan selama proses transmisi.
3. Autentikasi: memastikan identitas pengirim dan penerima pesan, sehingga dapat dipastikan bahwa komunikasi terjadi antara pihak yang benar.
4. Non-Repudiasi: mencegah pengirim pesan menyangkal bahwa ia telah mengirim pesan tersebut, sehingga memberikan jaminan legal atas transaksi atau komunikasi yang terjadi.

Kriptografi telah menjadi bagian integral dari peradaban manusia sejak zaman kuno. Awalnya, kriptografi digunakan untuk tujuan militer dan diplomasi, di mana pesan-pesan rahasia perlu disembunyikan dari mata musuh. Pada masa Mesir Kuno dan Mesopotamia, simbol-simbol tertentu sudah digunakan untuk menyembunyikan makna suatu pesan. Yunani Kuno mengembangkan alat bernama *Scytale*, sebuah silinder yang digunakan untuk mengenkripsi pesan dengan cara melilitkan pita berisi pesan di sekelilingnya. Sementara itu, Romawi Kuno terkenal dengan sandi Caesar, sebuah teknik sederhana yang menggeser huruf dalam alfabet.

Selama Abad Pertengahan, ilmuwan Muslim seperti Al-Kindi mengembangkan teknik-teknik kriptografi yang lebih kompleks, termasuk analisis frekuensi untuk memecahkan kode. Pada masa Renaissance, kriptografi semakin banyak digunakan, namun masih terbatas pada kalangan tertentu. Seiring dengan perkembangan teknologi, kriptografi juga mengalami evolusi yang signifikan. Pada Perang Dunia, mesin Enigma yang digunakan oleh Jerman menjadi simbol kompleksitas mesin enkripsi pada masa itu.

Pasca Perang Dunia, kriptografi mengalami perkembangan pesat. Munculnya komputer memungkinkan pengembangan algoritma enkripsi yang jauh lebih kompleks. Kriptografi simetris seperti DES (*Data Encryption Standard*) menjadi standar untuk enkripsi data, sementara kriptografi asimetris seperti RSA memungkinkan komunikasi yang lebih aman dengan menggunakan kunci publik dan privat.

Perkembangan terbaru dalam kriptografi mencakup kriptografi kuantum yang menawarkan tingkat keamanan yang jauh lebih tinggi, serta penerapan kriptografi dalam berbagai bidang seperti mata uang kripto, keamanan jaringan, dan e-commerce. Singkatnya, sejarah kriptografi adalah perjalanan panjang dari teknik sederhana hingga menjadi ilmu yang sangat kompleks dan mendasar dalam era digital saat ini.

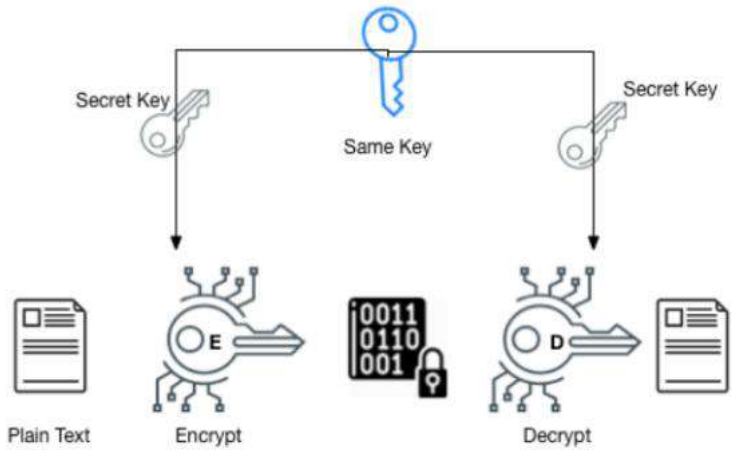
2.2 Konsep Dasar Kriptografi

2.2.1 Algoritma Kriptografi

Algoritma kriptografi adalah sekumpulan aturan atau instruksi matematis yang digunakan untuk mengubah data teks biasa menjadi bentuk yang tidak dapat dipahami teks cipher atau sebaliknya. Secara sederhana, algoritma kriptografi seperti sebuah resep rahasia untuk mengacak dan menyusun ulang data sehingga hanya pihak yang memiliki "kunci" yang tepat dapat memahaminya. Di tengah derasnya arus informasi yang kita hadapi saat ini, data pribadi, komunikasi, dan transaksi *online* menjadi sangat rentan terhadap ancaman. Algoritma kriptografi berperan krusial dalam melindungi informasi sensitif seperti nomor kartu kredit, kata sandi, informasi kesehatan, serta mengamankan komunikasi digital seperti email dan panggilan video. Dengan menggunakan algoritma kriptografi, kita dapat memastikan bahwa data kita tetap aman dan terjaga kerahasiaannya, sehingga kita dapat melakukan aktivitas online dengan lebih tenang dan percaya diri. Ada dua jenis algoritma kriptografi dalam sistem keamanan data, yaitu algoritma simetris dan asimetris.

1. **Algoritma simetris**

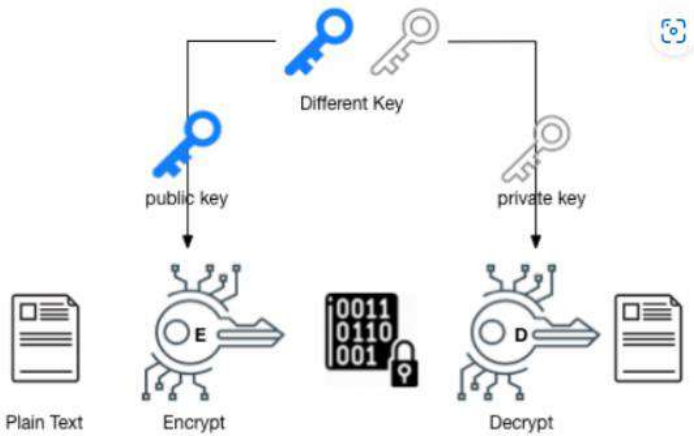
   Algoritma simetris adalah algoritma yang menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi data. Kunci ini harus dirahasiakan dan didistribusikan secara aman kepada semua pihak yang berwenang. Kelebihan dari algoritma simetris adalah proses enkripsi dan dekripsi umumnya lebih cepat dibandingkan dengan algoritma asimetris sehingga hanya membutuhkan komputasi yang lebih rendah dalam prosesnya. Contoh algoritma simetris yaitu, DES (*Data Encryption Standard*), AES (*Advanced Encryption Standard*), Blowfish, dan Twofish.



Gambar 2.1. Algoritma simetris
(Sumber : https://socs.binus.ac.id/)

2. Algoritma asimetris

Algoritma asimetris adalah algoritma yang menggunakan sepasang kunci yang berbeda untuk proses enkripsi dan dekripsi data, yang disebut juga kunci publik dan kunci privat. Kunci publik dapat didistribusikan secara bebas, sedangkan kunci privat harus dirahasiakan.



Gambar 2.2. Algoritma asimetris
(Sumber : https://socs.binus.ac.id/)

Kelebihan dari algoritma asimetris adalah lebih mudah dalam mendistribusikan kunci publik, sehingga cocok untuk sistem dengan banyak pengguna serta dapat digunakan untuk otentikasi dan tanda tangan digital. Contoh algoritma asimetris yaitu, RSA (*Rivest-Shamir-Adleman*), ECC (*Elliptic Curve Cryptography*), dan Diffie-Hellman.

2.2.2 Fungsi Hash

Fungsi hash adalah sebuah algoritma matematis yang mengambil data dengan ukuran berapa pun dan mengubahnya menjadi sebuah string dengan panjang yang tetap. String hasil olahan ini disebut *hash* atau *digest*. Proses perubahan ini bersifat satu arah, artinya tidak mungkin untuk menghitung kembali data asli dari hash yang dihasilkan.

Fungsi hash memainkan peran krusial dalam menjaga keamanan data. Prinsip kerjanya yang mengubah data apa pun menjadi string karakter dengan panjang tetap hash membuatnya sangat berguna dalam berbagai aplikasi. Dalam verifikasi integritas data, hash digunakan sebagai semacam sidik jari unik. Jika data asli diubah sedikit saja, hash yang dihasilkan akan sangat berbeda, sehingga memungkinkan kita untuk mendeteksi adanya manipulasi data. Penerapan lain yang umum adalah dalam penyimpanan kata sandi. Alih-alih menyimpan kata sandi dalam bentuk aslinya plaintext yang mudah diretas, sistem akan menyimpan hash-nya. Ketika pengguna ingin masuk, kata sandi yang dimasukkan akan di-hash dan dibandingkan dengan hash yang tersimpan. Tanda tangan digital juga memanfaatkan fungsi hash untuk memverifikasi keaslian pesan dan identitas pengirim. Pesan akan dienkripsi menggunakan kunci pribadi pengirim dan kemudian di-hash. Penerima dapat memverifikasi keaslian pesan dengan membandingkan hash yang diterima dengan hash yang dihasilkan dari pesan yang telah didekripsi. Konsep ini juga menjadi fondasi teknologi blockchain, di mana setiap blok dalam rantai berisi hash dari blok sebelumnya, menciptakan struktur data yang sangat aman dan transparan. Dengan demikian, fungsi hash tidak hanya melindungi data dari modifikasi yang tidak sah, tetapi juga berperan

penting dalam memastikan integritas dan keamanan sistem informasi secara keseluruhan.

Fungsi hash memiliki beberapa jenis dengan karakteristik dan keunggulan masing-masing. MD5, salah satu pionir dalam bidang ini, meskipun populer di masa lalu, kini dianggap kurang aman karena rentan terhadap serangan yang dapat menghasilkan hash yang sama untuk data yang berbeda. SHA merupakan keluarga algoritma hash yang lebih modern dan aman, dengan SHA-256 menjadi salah satu varian yang paling banyak digunakan saat ini. Keccak, algoritma yang menjadi dasar SHA-3, dirancang dengan arsitektur yang lebih kuat dan efisien, menjadikannya pilihan yang lebih baik untuk aplikasi keamanan modern. Setiap jenis fungsi hash memiliki kekuatan dan kelemahannya sendiri, sehingga pemilihan jenis yang tepat sangat bergantung pada kebutuhan keamanan spesifik dari suatu sistem.

2.2.3 Digital Signature

Digital Signature adalah metode otentikasi elektronik yang digunakan untuk memverifikasi identitas pengirim pesan atau dokumen digital, serta memastikan integritas data tersebut. Sederhananya, tanda tangan digital adalah versi digital dari tanda tangan basah yang kita gunakan sehari-hari, namun dengan tingkat keamanan yang jauh lebih tinggi.

Proses tanda tangan digital melibatkan beberapa langkah:

1. Pembuatan Hash
   Dokumen atau pesan yang akan ditandatangani diubah menjadi representasi numerik yang unik, yang disebut *hash*. Hash ini bertindak sebagai sidik jari digital dari dokumen tersebut. Perubahan sekecil apapun pada dokumen akan menghasilkan hash yang sangat berbeda.
2. Enkripsi dengan Kunci Privat
   Hash yang dihasilkan kemudian dienkripsi menggunakan *kunci privat* dari si pengirim. Kunci privat ini adalah kunci rahasia yang hanya dimiliki oleh pemiliknya.

3. Penyerahan Tanda Tangan
   Hasil enkripsi tanda tangan digital ini kemudian ditambahkan ke dokumen asli dan dikirimkan kepada penerima.
4. Verifikasi dengan Kunci Publik
   Penerima akan menggunakan *kunci publik* dari pengirim untuk mendekripsi tanda tangan digital. Kunci publik ini adalah pasangan dari kunci privat dan dapat didistribusikan secara bebas. Penerima kemudian menghitung kembali hash dari dokumen yang diterima. Jika hash yang dihitung sama dengan hash yang didapatkan dari mendekripsi tanda tangan digital, maka dokumen tersebut dianggap asli dan belum pernah diubah.

2.3 Pengamanan Jaringan

2.3.1 Ancaman Keamanan Jaringan

Ancaman keamanan jaringan adalah segala bentuk upaya yang bertujuan untuk mengganggu, merusak, atau mencuri data dan layanan yang ada dalam suatu jaringan. Ancaman ini bisa berasal dari berbagai sumber, mulai dari individu, kelompok, hingga negara. Berikut adalah beberapa jenis ancaman keamanan jaringan yang umum terjadi:

1. Serangan *Denial-of-Service* dan *Distributed Denial-of-Service*
   Serangan DoS (*Denial-of-Service*) dan DDoS (*Distributed Denial-of-Service*) adalah jenis serangan siber yang bertujuan untuk membuat sebuah layanan atau jaringan tidak dapat diakses dengan cara membanjiri sistem dengan permintaan yang berlebihan. Perbedaan dari keduannya adalah; Serangan DoS melibatkan hanya satu sumber yang mengirimkan sejumlah besar permintaan palsu ke target sedangkan serangan DDoS dilakukan dari banyak sumber yang berbeda secara bersamaan.
2. Injeksi SQL
   Injeksi SQL adalah salah satu jenis serangan siber yang memanfaatkan celah keamanan dalam aplikasi web untuk memanipulasi database. Serangan ini memungkinkan

penyerang untuk memasukkan kode SQL berbahaya ke dalam input data yang kemudian dieksekusi oleh database.

3. *Phishing*
   Phishing adalah jenis serangan siber yang memanfaatkan teknik manipulasi psikologis untuk menipu pengguna agar menyerahkan informasi pribadi mereka secara sukarela. Para pelaku phishing biasanya menyamar sebagai entitas yang terpercaya, seperti bank, perusahaan teknologi, atau lembaga pemerintah, untuk meyakinkan korban.
4. *Malware*
   Malware adalah singkatan dari malicious software atau perangkat lunak berbahaya. Ini adalah program komputer yang dirancang secara khusus untuk menyusup ke sistem komputer tanpa izin pemiliknya. Tujuan utama malware adalah untuk merusak sistem, mencuri data, atau mendapatkan kendali atas komputer yang terinfeksi.
5. *Man-in-the-Middle Attack*
   Serangan *Man-in-the-Middle* adalah jenis serangan siber di mana seorang penyerang secara diam-diam menyisipkan dirinya di antara dua pihak yang sedang berkomunikasi. Penyerang ini kemudian dapat menyadap, memodifikasi, atau bahkan mengalihkan komunikasi tersebut tanpa diketahui oleh kedua pihak yang sah.
6. *Social Engineering*
   Social engineering adalah teknik manipulasi psikologis yang digunakan oleh pelaku kejahatan siber untuk meyakinkan seseorang agar memberikan informasi sensitif atau melakukan tindakan yang menguntungkan pelaku. Sederhananya, ini adalah seni memanipulasi manusia untuk mendapatkan apa yang diinginkan.
7. *Zero-Day Exploit*
   Serangan *Zero-Day Exploit* adalah jenis serangan siber yang memanfaatkan celah keamanan dalam perangkat lunak, sistem operasi, atau perangkat keras yang belum diketahui atau belum ada tambalan keamanannya. Istilah "*Zero-Day*" mengacu pada fakta bahwa pengembang perangkat lunak

tidak memiliki waktu nol hari untuk memperbaiki celah keamanan tersebut sebelum diserang.

2.3.2 *Firewall*

Firewall adalah sistem keamanan jaringan yang bertindak sebagai perisai antara jaringan internal Anda (misalnya, jaringan rumah atau kantor) dengan jaringan eksternal seperti internet. *Firewall* berfungsi untuk memantau lalu lintas jaringan yang masuk dan keluar, serta memblokir lalu lintas yang dianggap mencurigakan atau berbahaya.

Firewall bertindak sebagai penjaga gerbang yang melindungi jaringan kita dari ancaman eksternal. Fungsi utamanya adalah memblokir akses tidak sah dari pihak yang tidak berwenang, sehingga menjaga keamanan sistem dan data kita dari serangan siber seperti peretasan, virus, dan *malware*. Selain itu, *firewall* juga berfungsi sebagai filter yang cerdas, memungkinkan Anda mengontrol lalu lintas jaringan secara granular berdasarkan berbagai kriteria seperti alamat IP, *port*, protokol, dan jenis aplikasi. Dengan demikian, kita dapat memblokir lalu lintas yang dianggap mencurigakan atau tidak perlu, serta mencegah kebocoran data sensitif. Selain meningkatkan keamanan, firewall juga dapat berkontribusi pada peningkatan kinerja jaringan dengan membatasi lalu lintas yang tidak relevan, sehingga memaksimalkan *bandwidth* yang tersedia.

2.3.3 *Intrusion Detection System*

IDS (*Intrusion Detection System*) adalah sistem keamanan jaringan yang dirancang untuk mendeteksi aktivitas mencurigakan atau serangan yang terjadi pada suatu jaringan komputer. IDS bekerja dengan memantau lalu lintas jaringan dan aktivitas sistem, kemudian membandingkannya dengan pola serangan yang telah diketahui atau perilaku yang dianggap abnormal.

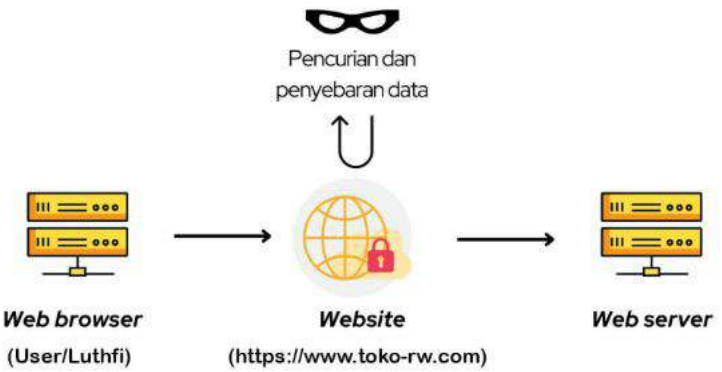
Intrusion Detection System bekerja dengan cara mengumpulkan data lalu lintas jaringan dari berbagai sumber seperti log server, switch, dan router. Data ini kemudian dianalisis secara mendalam menggunakan berbagai teknik, termasuk membandingkan dengan database tanda tangan serangan yang

sudah diketahui (*signature-based detection*), mendeteksi aktivitas yang menyimpang dari pola normal (*anomaly-based detection*), serta menggunakan analisis statistik dan aturan heuristik untuk mengidentifikasi perilaku mencurigakan. Jika IDS menemukan aktivitas yang dianggap sebagai ancaman, sistem akan segera mengirimkan peringatan kepada administrator jaringan melalui berbagai metode seperti email, log, atau tampilan pada konsol manajemen. Dengan demikian, IDS berperan sebagai penjaga mata yang terus-menerus memantau jaringan dan memberikan peringatan dini terhadap potensi serangan.

2.4 Kriptografi dalam Pengamanan Jaringan

2.4.1 Kriptografi dalam Protokol Komunikasi

Kriptografi pada protokol HTTPS adalah sebagai kunci utama yang menjaga keamanan komunikasi data antara perangkat Anda (misalnya, komputer, ponsel) dan server web. HTTPS adalah singkatan dari *Hypertext Transfer Protocol Secure,* yang berarti protokol transfer hiperteks yang aman.



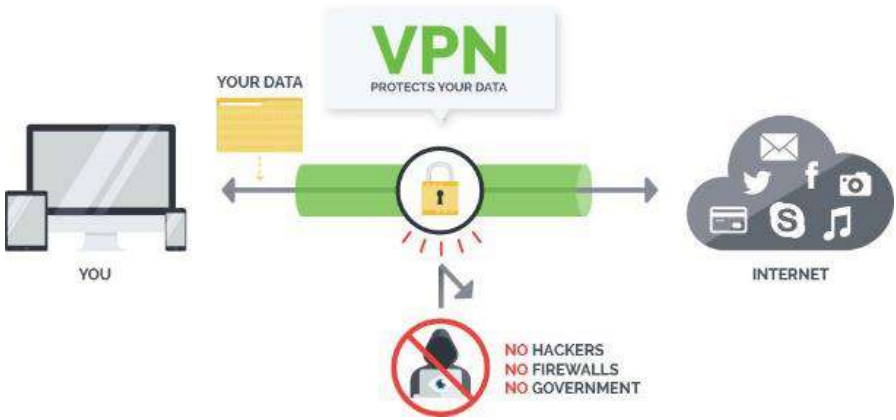
Gambar 2.3. Penggunaan HTTPS
(Sumber : https://blog.rumahweb.com)

Cara kerja Kriptografi dalam HTTPS adalah Setiap situs web yang menggunakan HTTPS memiliki sepasang kunci kriptografi, yaitu kunci publik dan kunci pribadi. Saat kita mengakses situs tersebut, server akan mengirimkan kunci publiknya kepada kita.

Kita kemudian akan menggunakan kunci publik ini untuk mengenkripsi data yang kita kirimkan, seperti kata sandi atau informasi pembayaran. Setelah itu, server akan menggunakan kunci pribadinya (yang dirahasiakan) untuk mendekripsi data tersebut. Selain itu, kita dan server akan menghasilkan sebuah kunci rahasia yang juga dienkripsi untuk meningkatkan keamanan komunikasi. Dengan cara ini, data yang kita kirimkan antara kita dan server akan tetap aman dan rahasia, terhindar dari ancaman penyadapan.

2.4.2 Kriptografi dalam VPN

Kriptografi dalam VPN (*Virtual Private Network*) digunakan untuk mengamankan data yang dikirimkan antara perangkat pengguna dan server VPN melalui jaringan publik, seperti internet. VPN menciptakan koneksi terenkripsi, sering disebut sebagai "tunnel", yang melindungi privasi dan memastikan integritas data.



Gambar 2.4. *Virtual Private Network*
(Sumber : https://cdn3.geckoandfly.com)

Didalam cara kerjanya VPN menggunakan berbagai protokol kriptografi untuk membangun koneksi yang aman dan terenkripsi antara perangkat pengguna dan server VPN. Salah satu protokol yang umum digunakan adalah IPsec (*Internet Protocol Security*), yang memanfaatkan enkripsi simetris dan asimetris untuk mengamankan data di tingkat IP. Protokol ini memastikan bahwa sumber data diverifikasi dan mencegah perubahan data selama

transmisi. Selanjutnya, OpenVPN adalah protokol VPN yang sangat populer dan aman karena menggunakan pustaka OpenSSL untuk enkripsi, sering kali dalam kombinasi dengan TLS atau SSL sebagai lapisan tambahan guna memperkuat keamanan. Protokol ini sangat fleksibel dan banyak digunakan dalam lingkungan VPN komersial. Selain itu, WireGuard adalah protokol VPN yang lebih baru, dikenal karena desainnya yang ringan serta fokus pada kecepatan dan keamanan. WireGuard menggunakan algoritma modern yang efisien, menjadikannya pilihan yang ideal bagi pengguna yang menginginkan performa optimal dengan tetap menjaga privasi data.

Pada proses selanjutnya adalah enkripsi data, enkripsi data memegang peranan penting dalam menjaga kerahasiaan dan integritas informasi yang dikirimkan. Setelah koneksi VPN berhasil dibentuk, data yang ditransmisikan antara perangkat pengguna dan server dienkripsi menggunakan enkripsi simetris dengan algoritma seperti AES (*Advanced Encryption Standard*). Enkripsi simetris ini cepat dan efisien, dan kunci yang digunakan hanya diketahui oleh klien dan server, sehingga memastikan bahwa pihak ketiga tidak dapat membaca atau mengakses data tersebut. Namun, sebelum data dapat dienkripsi secara simetris, terlebih dahulu terjadi proses enkripsi asimetris selama tahap negosiasi, atau *handshake*. Dalam proses ini, enkripsi asimetris dengan kunci publik dan kunci privat digunakan untuk bertukar kunci enkripsi simetris secara aman. Kunci publik, yang dapat dibagikan secara bebas, digunakan untuk mengenkripsi kunci sesi simetris, sementara kunci privat, yang dirahasiakan, digunakan untuk mendekripsi kunci tersebut. Dengan cara ini, kunci sesi hanya diketahui oleh klien dan server, memastikan komunikasi yang aman di seluruh durasi koneksi.

Selain enkripsi, integritas data juga merupakan aspek penting dalam keamanan VPN. VPN tidak hanya memastikan bahwa data yang dikirim melalui jaringan terenkripsi, tetapi juga menjamin bahwa data tersebut tidak dapat diubah tanpa terdeteksi. Ini penting untuk mencegah manipulasi data oleh pihak yang tidak berwenang selama transmisi. Untuk memverifikasi keaslian dan integritas pesan, VPN biasanya menggunakan mekanisme seperti HMAC (*Hash-based Message Authentication Code*). HMAC menghasilkan hash unik dari data yang dikirim, dan jika ada

perubahan atau manipulasi dalam data tersebut, hash yang dihasilkan akan berbeda dari yang diharapkan, sehingga menunjukkan bahwa data telah dirusak. Dengan cara ini, VPN tidak hanya melindungi kerahasiaan informasi, tetapi juga menjaga keutuhan dan keaslian data yang dikirim.

2.4.3 Kriptografi dalam Email

Kriptografi dalam email digunakan untuk melindungi kerahasiaan, integritas, dan otentikasi pesan yang dikirim melalui email, memastikan bahwa hanya penerima yang dimaksud dapat membaca pesan, pesan tersebut tidak diubah selama transmisi, dan pengirim pesan dapat diverifikasi.

Dalam kriptografi email, enkripsi *end-to-end* memainkan peran penting dalam melindungi data yang dikirim. Enkripsi simetris dapat digunakan untuk mengenkripsi data email dengan algoritma seperti AES. Namun, tantangan utama enkripsi simetris adalah bagaimana membagikan kunci secara aman antara pengirim dan penerima. Sebaliknya, enkripsi asimetris lebih umum digunakan, di mana setiap pengguna memiliki sepasang kunci: kunci publik dan kunci privat. Pengirim menggunakan kunci publik penerima untuk mengenkripsi email, dan hanya penerima dengan kunci privat yang sesuai yang dapat mendekripsinya. Dua protokol enkripsi email yang populer, PGP (*Pretty Good Privacy*) dan S/MIME (*Secure/Multipurpose Internet Mail Extensions*), menggunakan enkripsi asimetris untuk menjaga kerahasiaan pesan. Enkripsi, tanda *digital signature* juga merupakan komponen penting dalam kriptografi email. Dengan *digital signature*, pengirim dapat membuktikan bahwa dia adalah pemilik asli alamat email tersebut, dan bahwa pesan yang dikirim tidak diubah selama transmisi. *Digital signature* dihasilkan menggunakan kunci privat pengirim, dan penerima menggunakan kunci publik pengirim untuk memverifikasi keaslian tanda tangan dan pesan. Untuk menjaga integritas pesan, algoritma hashing seperti SHA-256 digunakan. Hash ini berfungsi sebagai sidik jari dari pesan yang dikirim. Jika pesan mengalami perubahan selama transmisi, nilai hash yang dihasilkan dari pesan yang diterima akan berbeda dari hash asli, menandakan bahwa pesan tersebut telah dimodifikasi. Dengan

demikian, hashing memastikan bahwa isi pesan tetap utuh dari pengirim hingga penerima.

PGP (*Pretty Good Privacy*) adalah salah satu contoh implementasi kriptografi dalam email yang menggabungkan enkripsi simetris dan asimetris untuk memastikan keamanan komunikasi. Dalam PGP, pesan email dienkripsi menggunakan kunci simetris karena efisiensinya dalam mengenkripsi data. Namun, untuk mengamankan kunci simetris itu sendiri, digunakan enkripsi asimetris. Kunci simetris dienkripsi dengan kunci publik penerima, sehingga hanya penerima yang memiliki kunci privat yang sesuai dapat mendekripsi kunci tersebut dan kemudian menggunakan kunci simetris untuk membaca pesan. Dengan pendekatan ini, PGP memberikan lapisan keamanan ganda dengan menjaga kerahasiaan data melalui enkripsi simetris dan keamanan distribusi kunci melalui enkripsi asimetris.

Sementara itu, S/MIME (*Secure/Multipurpose Internet Mail Extensions*) adalah standar lain untuk enkripsi email yang menggunakan sertifikat digital untuk memberikan keamanan tambahan. S/MIME menggunakan sertifikat digital yang dikeluarkan oleh otoritas sertifikat (CA) untuk memastikan bahwa pengirim pesan adalah entitas yang tepercaya. Selain mengenkripsi konten email, S/MIME juga menjamin otentikasi pengirim dan integritas pesan, memastikan bahwa email yang dikirim tidak diubah selama transmisi dan benar-benar berasal dari pengirim yang sah.

DAFTAR PUSTAKA

Forouzan, B. A., & Mukhopadhyay, D. (2015). *Cryptography and network security* (2nd ed.). McGraw-Hill Education.

Kaufman, C., Perlman, R., & Speciner, M. (2010). *Network security: Private communication in a public world* (2nd ed.). Prentice Hall.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson Education.

BAB 3
PRIVASI DAN KEPATUHAN REGULASI

Oleh Yendi Putra

3.1 Pendahuluan

Dalam era digital yang semakin terhubung, privasi dan kepatuhan terhadap regulasi keamanan siber telah menjadi dua pilar penting yang harus diperhatikan oleh organisasi dan individu. Seiring dengan semakin pesatnya adopsi teknologi informasi, ancaman terhadap privasi pribadi dan data organisasi juga meningkat. Privasi berkaitan dengan hak individu untuk mengontrol informasi pribadinya, sementara kepatuhan regulasi mengacu pada kewajiban yang harus dipenuhi oleh entitas untuk melindungi data tersebut sesuai dengan undang-undang yang berlaku. Di banyak negara, kerangka hukum yang ada terus berkembang seiring dengan munculnya ancaman baru, seperti *General Data Protection Regulation* (GDPR) di Uni Eropa dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia. Pengabaian terhadap privasi dan regulasi ini dapat menimbulkan konsekuensi serius, baik dari sisi reputasi maupun finansial.

Di dalam konteks keamanan siber, privasi tidak hanya berbicara tentang melindungi informasi pribadi, tetapi juga mencakup bagaimana informasi tersebut dikumpulkan, digunakan, dan disimpan. Setiap perusahaan yang mengelola data pelanggan memiliki tanggung jawab besar untuk memastikan bahwa data tersebut diproses sesuai dengan prinsip-prinsip privasi yang telah ditetapkan. Penerapan kebijakan privasi yang kuat menjadi syarat mutlak, terutama ketika teknologi seperti cloud computing dan kecerdasan buatan (AI) semakin banyak digunakan. Namun, seringkali organisasi menghadapi tantangan dalam menyeimbangkan kebutuhan operasional dengan perlindungan privasi. Ketika privasi diabaikan, kerentanan terhadap serangan siber meningkat, yang

pada akhirnya dapat mengakibatkan pelanggaran data yang besar. kepatuhan terhadap regulasi keamanan siber merupakan kewajiban hukum yang dirancang untuk melindungi data dan menjaga kepercayaan publik. Regulasi seperti GDPR, California Consumer Privacy Act (CCPA), dan UU PDP mengharuskan organisasi untuk mematuhi standar tertentu dalam mengelola data. Tidak mematuhi regulasi tersebut dapat mengakibatkan denda yang sangat besar dan kerusakan reputasi yang tidak ternilai (Ziqra et al., 2021). Di dalam dunia yang semakin diatur oleh regulasi yang kompleks, organisasi harus memastikan bahwa mereka memiliki sistem kepatuhan yang tepat, termasuk audit internal dan ekternal, serta kebijakan keamanan yang diperbarui secara berkala. Dalam konteks global, tantangan lainnya adalah memastikan kepatuhan lintas negara, terutama bagi organisasi yang beroperasi di berbagai yurisdiksi (Rawat, 2021).

Ancaman terhadap privasi dan regulasi terus berkembang seiring dengan meningkatnya teknologi yang digunakan untuk mengakses dan memanipulasi data. Dengan berkembangnya *Internet of Things* (IoT), mobile computing, dan teknologi blockchain, semakin banyak celah yang dapat dieksploitasi oleh penyerang siber (H. Saputra, 2024). Hal ini mengharuskan perusahaan untuk beradaptasi dengan cepat terhadap perubahan lanskap ancaman. Kegagalan dalam menjaga privasi dan kepatuhan regulasi tidak hanya berimplikasi pada denda dan sanksi hukum, tetapi juga pada hilangnya kepercayaan konsumen. Oleh karena itu, strategi keamanan siber yang komprehensif harus melibatkan perlindungan privasi dan mekanisme kepatuhan yang kuat. privasi dan kepatuhan regulasi bukanlah sekadar tanggung jawab hukum, tetapi juga bagian integral dari strategi keamanan siber yang berkelanjutan. Organisasi harus terus memperbarui kebijakan keamanan mereka agar sesuai dengan regulasi yang ada dan siap menghadapi ancaman baru yang mungkin muncul. Di tengah lingkungan digital yang cepat berubah, perusahaan yang berhasil mempertahankan kepercayaan konsumen adalah mereka yang mampu menjaga integritas data melalui kebijakan

privasi yang kuat dan kepatuhan terhadap regulasi yang ketat. Masa depan keamanan siber sangat bergantung pada bagaimana organisasi menyeimbangkan antara inovasi teknologi dan perlindungan privasi serta kepatuhan regulasi.

3.1.1 Privasi

Privasi adalah hak fundamental individu untuk menjaga dan mengontrol informasi pribadi mereka agar tidak diakses, digunakan, atau disebarluaskan tanpa persetujuan. Dalam konteks digital, privasi mencakup perlindungan terhadap data pribadi yang dihasilkan melalui aktivitas online, seperti informasi identitas, lokasi, riwayat penelusuran, serta komunikasi pribadi. Setiap individu memiliki hak untuk menentukan sejauh mana informasi pribadi mereka dapat diungkapkan kepada pihak lain, termasuk pemerintah, perusahaan, dan organisasi. Pentingnya privasi semakin meningkat seiring dengan perkembangan teknologi, yang memungkinkan pengumpulan, penyimpanan, dan analisis data dalam skala besar, sehingga menimbulkan risiko terhadap kebocoran data, penyalahgunaan informasi, dan pelanggaran hak privasi individu(Fauzi et al., 2024).

Konsep privasi juga mencakup perlindungan terhadap intrusi atau gangguan dalam kehidupan pribadi, baik secara fisik maupun digital. Dalam lingkup ini, berbagai regulasi dan kebijakan telah diterapkan untuk melindungi hak privasi, seperti GDPR di Uni Eropa dan UU Perlindungan Data Pribadi di Indonesia, yang bertujuan mengatur bagaimana data pribadi harus dikumpulkan, diproses, dan diamankan. Privasi bukan hanya masalah teknis, tetapi juga terkait dengan kepercayaan masyarakat terhadap entitas yang mengelola informasi pribadi mereka. Pada akhirnya, menjaga privasi menjadi tanggung jawab bersama antara individu, pemerintah, dan perusahaan untuk memastikan keamanan informasi pribadi di era digital.

3.1.2 Kepatuhan Regulasi

Kepatuhan regulasi adalah upaya yang dilakukan oleh organisasi, perusahaan, atau individu untuk memastikan bahwa

operasi dan aktivitas mereka sesuai dengan hukum, aturan, dan standar yang berlaku di wilayah tempat mereka beroperasi. Ini mencakup berbagai aspek, mulai dari hukum perburuhan, lingkungan, kesehatan dan keselamatan kerja, hingga perlindungan data dan keamanan siber. Kepatuhan terhadap regulasi tidak hanya mencakup pengetahuan tentang aturan yang berlaku, tetapi juga implementasi kebijakan dan prosedur yang memastikan bahwa semua aktivitas organisasi berjalan sesuai dengan ketentuan hukum yang telah ditetapkan. Dengan semakin kompleksnya regulasi, kepatuhan ini menjadi lebih penting untuk menghindari sanksi hukum, denda finansial, atau kerusakan reputasi.

Di dunia digital, khususnya dalam konteks keamanan siber dan perlindungan data, kepatuhan regulasi semakin menjadi sorotan. Banyak negara memberlakukan undang-undang yang mengatur bagaimana data pribadi dikumpulkan, disimpan, dan dilindungi. Contohnya adalah *General Data Protection Regulation* (GDPR) di Uni Eropa, yang mewajibkan perusahaan untuk mendapatkan persetujuan pengguna sebelum mengumpulkan data pribadi mereka. GDPR juga menuntut perusahaan untuk melaporkan pelanggaran data dalam waktu 72 jam sejak kejadian. Pelanggaran terhadap GDPR dapat mengakibatkan denda hingga 20 juta Euro atau 4% dari pendapatan tahunan perusahaan, mana yang lebih besar. Di Indonesia, Undang-Undang Perlindungan Data Pribadi (UU PDP) juga mengatur pengelolaan data pribadi dan mewajibkan perusahaan untuk memastikan data pengguna dilindungi dengan baik(Romansky, 2022).

Salah satu contoh nyata pentingnya kepatuhan regulasi dapat dilihat dari kasus *Cambridge Analytica* yang melibatkan Facebook. Pada tahun 2018, terungkap bahwa data pribadi puluhan juta pengguna Facebook telah digunakan tanpa izin untuk tujuan kampanye politik. Ketidakpatuhan Facebook terhadap regulasi privasi di Amerika Serikat dan Uni Eropa mengakibatkan denda besar serta hilangnya kepercayaan publik. Kasus ini juga memicu perdebatan global tentang pentingnya regulasi yang lebih ketat terkait penggunaan data

pribadi, serta menunjukkan dampak serius dari ketidakpatuhan regulasi dalam konteks perlindungan privasi. Di sektor lain, perusahaan teknologi harus mematuhi berbagai regulasi terkait hak kekayaan intelektual, anti-monopoli, dan keamanan siber. Misalnya, perusahaan cloud computing seperti Amazon Web Services (AWS) atau Microsoft Azure diharuskan untuk memastikan infrastruktur mereka memenuhi standar keamanan global, seperti ISO 27001 dan kepatuhan terhadap Payment Card Industry Data Security Standard (PCI DSS) untuk melindungi informasi kartu kredit. Kegagalan dalam mematuhi standar ini dapat mengakibatkan hilangnya sertifikasi yang dibutuhkan untuk menjalankan bisnis secara global, atau bahkan tuntutan hukum(Informatika et al., 2023).

Dengan adanya berbagai regulasi di tingkat nasional dan internasional, organisasi harus membangun sistem kepatuhan yang kuat. Ini melibatkan pemantauan rutin terhadap perubahan regulasi, pelatihan karyawan, serta audit internal dan eksternal. Kepatuhan bukan hanya tentang mengikuti aturan demi menghindari sanksi, tetapi juga untuk menjaga reputasi dan memastikan integritas operasional. Organisasi yang patuh cenderung mendapatkan kepercayaan lebih dari pelanggan, mitra bisnis, dan pemangku kepentingan lainnya, karena mereka dianggap lebih dapat diandalkan dalam menjaga keamanan dan privasi.

3.2 Kepatuhan Regulasi dalam Keamanan Siber

Kepatuhan terhadap regulasi dalam keamanan siber adalah elemen penting dalam upaya melindungi data dan informasi dari risiko yang ditimbulkan oleh ancaman dunia maya. Kepatuhan (*compliance*) tidak hanya bertujuan untuk mengamankan informasi dari serangan siber, tetapi juga memastikan bahwa organisasi mematuhi peraturan hukum yang berlaku, menjaga hak-hak individu terkait privasi data, serta meminimalkan risiko hukum dan finansial yang bisa terjadi akibat pelanggaran data.

3.2.1 Definisi Kepatuhan (*Compliance*)

Kepatuhan dalam konteks keamanan siber merujuk pada proses dan kebijakan yang harus diikuti oleh organisasi untuk memastikan bahwa mereka memenuhi semua persyaratan yang ditetapkan oleh hukum, regulasi, dan standar industri terkait keamanan data dan privasi. Kepatuhan ini mencakup berbagai bidang, mulai dari pengelolaan data pribadi hingga perlindungan infrastruktur digital organisasi. Kepatuhan terhadap regulasi sering kali melibatkan audit internal dan eksternal, pelatihan karyawan tentang kebijakan keamanan, serta penerapan langkah-langkah teknis dan administratif untuk melindungi data dari akses yang tidak sah, pencurian, atau kerusakan. Tujuannya adalah untuk memastikan bahwa organisasi tidak hanya melindungi aset digital mereka tetapi juga mematuhi standar yang telah ditetapkan oleh pemerintah atau badan regulasi.

3.2.2 Pentingnya Kepatuhan Terhadap Regulasi

Kepatuhan terhadap regulasi dalam keamanan siber penting karena berbagai alasan:

1. Perlindungan Data Pribadi

   Peraturan seperti GDPR dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia menekankan pentingnya melindungi data pribadi. Organisasi yang tidak mematuhi regulasi ini dapat menghadapi denda yang besar dan kehilangan kepercayaan dari pelanggan (Sautunnida et al., 2018).
2. Meminimalkan Risiko Hukum

   Ketidakpatuhan terhadap regulasi bisa mengakibatkan tuntutan hukum, baik dari pemerintah maupun dari individu yang dirugikan oleh pelanggaran data. Organisasi yang lalai melindungi data pelanggan dapat dituntut atas pelanggaran privasi atau kelalaian.
3. Mengurangi Risiko Reputasi

   Ketika sebuah organisasi mengalami pelanggaran data atau gagal mematuhi regulasi keamanan siber, reputasi mereka di mata publik dapat rusak. Dalam dunia yang sangat kompetitif, kepercayaan pelanggan adalah aset yang

sangat berharga, dan kehilangan kepercayaan ini dapat berakibat pada hilangnya peluang bisnis.

4. Meningkatkan Efisiensi Operasional

   Mematuhi standar keamanan dan privasi sering kali memaksa organisasi untuk meningkatkan sistem dan infrastruktur teknologi informasi mereka. Hal ini dapat meningkatkan efisiensi operasional, meningkatkan kemampuan dalam mengelola risiko, serta mengurangi kemungkinan insiden keamanan siber.

3.2.3 Dampak Ketidakpatuhan Terhadap Regulasi

Ketidakpatuhan terhadap regulasi keamanan siber dapat menimbulkan dampak yang sangat serius bagi organisasi, baik dari sisi finansial, reputasi, maupun operasional. Dalam lingkungan bisnis yang semakin bergantung pada data dan teknologi, ketidakpatuhan bukan lagi sekadar risiko yang dapat diabaikan. Berbagai regulasi seperti GDPR, CCPA, dan UU PDP Indonesia mengharuskan organisasi untuk mematuhi standar perlindungan data yang ketat. Ketika standar ini dilanggar, konsekuensinya bisa menghancurkan.

Berikut adalah beberapa dampak utama dari ketidakpatuhan terhadap regulasi keamanan siber:

1. Sanksi Hukum dan Denda Finansial

   Salah satu dampak paling langsung dari ketidakpatuhan terhadap regulasi adalah sanksi hukum berupa denda finansial yang bisa sangat besar. Beberapa peraturan, seperti GDPR dan CCPA, memiliki ketentuan denda yang besar bagi organisasi yang melanggar peraturan tersebut.

   a. Pelanggaran GDPR

      GDPR menetapkan denda yang sangat ketat. Untuk pelanggaran berat, denda bisa mencapai hingga 20 juta euro atau 4% dari pendapatan tahunan global organisasi, mana yang lebih tinggi. Contohnya, pada tahun 2021, perusahaan teknologi Amazon didenda sebesar €746 juta oleh otoritas perlindungan data Luxembourg atas dugaan pelanggaran privasi pelanggan berdasarkan GDPRni menunjukkan betapa

besarnya dampak finansial dari ketidakpatuhan terhadap regulasi data (Hanifa Salsabila, 2024).

b. Pelanggaran CCPA
   Di Amerika Serikat, pelanggaran California Consumer Privacy Act (CCPA) juga membawa konsekuensi finansial yang besar. Perusahaan yang gagal melindungi data konsumen sesuai ketentuan CCPA dapat dikenakan denda hingga $7.500 per pelanggaran. Ini berarti bahwa jika ribuan catatan pelanggan disusupi, denda kumulatif bisa mencapai jutaan dolar(Hanifa Salsabila, 2024).
c. Pelanggaran UU PDP Indonesia
   Di Indonesia, Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada tahun 2022 juga mengatur sanksi bagi pelanggaran privasi data. Selain denda administratif, pelanggaran serius terhadap UU PDP dapat menyebabkan sanksi pidana berupa denda hingga miliaran rupiah dan ancaman hukuman penjara bagi para pelanggar.

2. Kerugian Reputasi
   Kerugian reputasi mungkin menjadi salah satu dampak jangka panjang paling merusak dari ketidakpatuhan terhadap regulasi keamanan siber. Ketika data pribadi pelanggan bocor atau diakses tanpa izin, kepercayaan publik terhadap organisasi dapat langsung tergerus. Membangun reputasi sebagai organisasi yang dapat dipercaya dalam hal keamanan data membutuhkan waktu bertahun-tahun, tetapi kerusakan reputasi akibat satu insiden bisa terjadi dalam hitungan hari atau bahkan jam. Beberapa contoh nyata dampak reputasi adalah:
   a. Kasus Pelanggaran Data Facebook (*Cambridge Analytica*)
      Skandal *Cambridge Analytica* pada tahun 2018, di mana data pribadi jutaan pengguna Facebook digunakan tanpa persetujuan mereka, merusak reputasi Facebook secara global. Meskipun Facebook tidak secara langsung

melanggar GDPR karena peristiwa ini terjadi sebelum regulasi tersebut diterapkan, dampaknya sangat besar terhadap citra publik mereka. Pengguna menjadi lebih waspada dalam membagikan informasi pribadi di platform media sosial dan banyak yang memilih untuk menghapus akun mereka. Selain itu, Facebook menghadapi gugatan hukum besar-besaran dan denda miliaran dolar di AS dan negara-negara lainnya.

b. Pelanggara Data Equifax
Pada 2017, Equifax, salah satu biro kredit terbesar di dunia, mengalami pelanggaran data besar-besaran yang mempengaruhi lebih dari 143 juta konsumen di AS. Data yang dicuri termasuk nomor jaminan sosial, nomor kartu kredit, dan informasi pribadi lainnya. Meskipun Equifax menerima denda finansial, dampak reputasi yang lebih parah adalah hilangnya kepercayaan konsumen. Orang-orang merasa tidak aman menyerahkan informasi pribadi mereka kepada perusahaan besar yang seharusnya menjaga keamanan data tersebut(Manajemen et al., 2024).
Setelah terjadi pelanggaran besar seperti itu, banyak konsumen yang ragu untuk melanjutkan hubungan dengan organisasi tersebut. Mereka mungkin beralih ke pesaing, sehingga mengurangi pangsa pasar dan mempengaruhi pendapatan jangka panjang.

3. Kerugian Finansial Langsung dan Tidak Langsung
Selain denda dan kerugian reputasi, ketidakpatuhan terhadap regulasi keamanan siber juga dapat menyebabkan kerugian finansial langsung dan tidak langsung lainnya. Dampak ini bisa berasal dari berbagai sumber, seperti:
   a. Biaya Litigasi
   Ketidakpatuhan yang mengakibatkan pelanggaran data dapat memicu tuntutan hukum dari individu atau kelompok yang merasa dirugikan. Di Amerika Serikat, perusahaan sering kali harus menghadapi class action lawsuits yang berujung pada kompensasi bernilai jutaan

dolar. Biaya hukum, kompensasi kepada korban, dan penyelesaian litigasi dapat menambah beban finansial yang sangat besar.

b. Penurunan Nilai Saham
   Perusahaan publik yang mengalami pelanggaran data besar sering kali melihat penurunan signifikan dalam harga saham mereka. Hal ini terjadi karena investor kehilangan kepercayaan pada kemampuan manajemen untuk melindungi data penting dan memenuhi regulasi. Penurunan nilai saham ini bisa menyebabkan miliaran dolar kerugian kapitalisasi pasar. Contoh nyata terjadi pada Yahoo setelah pelanggaran data besar-besaran yang mengungkapkan informasi pribadi lebih dari 3 miliar akun pengguna. Nilai perusahaan turun drastis setelah insiden tersebut terungkap.
c. Biaya Perbaikan dan Pemulihan Sistem
   Setelah insiden pelanggaran keamanan, organisasi sering kali harus menginvestasikan dana besar untuk memperbaiki kerusakan. Ini mencakup peningkatan infrastruktur teknologi, penerapan langkah-langkah keamanan tambahan, dan melakukan investigasi forensik untuk menemukan akar penyebab pelanggaran. Biaya ini bisa menjadi beban finansial yang signifikan bagi organisasi, terutama jika infrastruktur teknologi mereka perlu diganti atau diperbarui secara besar-besaran.

4. Disrupsi Operasional
   Ketidakpatuhan terhadap regulasi keamanan siber sering kali menyebabkan disrupsi besar pada operasi bisnis sehari-hari. Ketika sebuah perusahaan mengalami pelanggaran data atau serangan siber, mereka mungkin harus menghentikan operasi selama beberapa waktu untuk menangani insiden tersebut. Hal ini dapat berdampak serius pada produktivitas dan aliran pendapatan.

a. Shutdown Sistem
   Dalam beberapa kasus, pelanggaran data atau ketidakpatuhan bisa memaksa perusahaan untuk menghentikan sementara layanan mereka untuk memperbaiki masalah. Misalnya, pada 2021, Colonial Pipeline, perusahaan energi terbesar di AS, harus menutup operasi selama beberapa hari akibat serangan ransomware. Akibatnya, pasokan bahan bakar di sebagian besar Pantai Timur AS terganggu, menyebabkan kerugian ekonomi yang sangat besar(Golden & Extortion, n.d.).
b. Kehilangan Pelanggan Bisnis
   Selain disrupsi operasional, ketidakpatuhan bisa menyebabkan hilangnya pelanggan utama atau kontrak bisnis yang penting. Perusahaan yang tidak mematuhi standar keamanan siber mungkin kehilangan kontrak dengan klien besar yang mengharuskan vendor mereka memiliki kepatuhan yang ketat. Hal ini dapat berdampak langsung pada pendapatan dan prospek bisnis di masa depan.

5. Peningkatan Pengawasan Regulasi
   Organisasi yang pernah melanggar regulasi keamanan siber sering kali berada di bawah pengawasan yang lebih ketat oleh badan-badan pengatur. Ini dapat menyebabkan peningkatan audit, inspeksi, dan tuntutan administrasi yang lebih tinggi dari regulator. Biaya untuk mematuhi audit tambahan dan memenuhi persyaratan administrasi ini bisa sangat signifikan, terutama bagi perusahaan yang beroperasi di berbagai yurisdiksi yang memiliki regulasi berbeda.

6. Kehilangan Kepercayaan dari Mitra Bisnis dan Investor
   Ketidakpatuhan terhadap regulasi keamanan siber dapat berdampak pada hubungan organisasi dengan mitra bisnis dan investor. Mitra bisnis yang mengandalkan sistem keamanan kuat dari rekanan mereka mungkin merasa

khawatir jika terjadi pelanggaran, dan hal ini dapat memicu penghentian kerjasama. Di sisi lain, investor yang telah menanamkan modal juga dapat kehilangan kepercayaan, menyebabkan hilangnya peluang pendanaan atau penurunan nilai saham secara drastis. Dalam dunia bisnis yang semakin terkoneksi, banyak perusahaan bekerja dalam ekosistem yang bergantung pada integritas data. Ketika salah satu komponen dalam ekosistem tersebut mengalami pelanggaran, risiko penyebaran masalah ke seluruh rantai pasokan menjadi sangat nyata. Misalnya, perusahaan yang bergerak dalam industri keuangan atau kesehatan mungkin dipaksa menghentikan kerja sama dengan vendor atau partner yang tidak mematuhi standar keamanan data. Akibatnya, perusahaan tersebut bisa kehilangan proyek atau kontrak bernilai tinggi.

Bagi investor, ketidakpatuhan yang mengakibatkan pelanggaran data atau denda regulasi dapat menjadi indikator bahwa perusahaan tidak dikelola dengan baik. Hal ini dapat menyebabkan penurunan nilai saham, dan dalam kasus yang lebih serius, mengakibatkan investor menarik dana mereka. Penurunan modal ini dapat mempengaruhi stabilitas jangka panjang perusahaan, mengurangi kemampuan untuk berkembang atau bersaing di pasar.

7. Biaya Pemulihan Reputasi dan Komunikasi Krisis

   Setelah pelanggaran data atau ketidakpatuhan terhadap regulasi, organisasi sering kali harus mengalokasikan sumber daya yang signifikan untuk memulihkan reputasi mereka. Langkah-langkah pemulihan ini mencakup strategi komunikasi krisis, penanganan keluhan pelanggan, dan perbaikan sistem yang rusak.

   a. Strategi Komunikasi Krisis

      Sebuah organisasi yang mengalami pelanggaran data perlu merespons cepat dengan rencana komunikasi krisis yang baik. Hal ini melibatkan pengumuman publik tentang insiden, pemberitahuan kepada pihak yang terkena dampak, dan penjelasan tentang langkah-

langkah yang diambil untuk memitigasi dampak tersebut. Biaya untuk menyewa konsultan PR dan pakar komunikasi, serta untuk kampanye media yang bertujuan memulihkan citra perusahaan, bisa sangat tinggi.

b. Pemberitahuan kepada Pihak yang Terkena Dampak
   Beberapa regulasi, seperti GDPR, mewajibkan organisasi untuk memberi tahu pihak yang terkena dampak pelanggaran data dalam jangka waktu tertentu. Proses pemberitahuan ini sering kali membutuhkan teknologi khusus untuk mendeteksi dan menginformasikan kepada individu yang terkena dampak secara tepat. Misalnya, dalam kasus pelanggaran data pelanggan yang melibatkan jutaan orang, biaya untuk menghubungi setiap individu dan memberikan rincian tentang pelanggaran tersebut bisa sangat besar.
c. Kompensasi dan Dukungan kepada Pelanggan
   Selain biaya komunikasi, organisasi mungkin perlu menawarkan kompensasi kepada pelanggan yang terkena dampak pelanggaran data. Kompensasi ini bisa berupa layanan pemantauan kredit gratis untuk memastikan tidak ada penyalahgunaan data pribadi, atau bahkan ganti rugi finansial bagi mereka yang dirugikan secara langsung. Semua langkah ini memerlukan anggaran tambahan, yang pada akhirnya menambah beban biaya pemulihan dari pelanggaran.

3.3 Kerangka Kerja Regulasi Global dalam Keamanan

Kerangka kerja regulasi global berfungsi sebagai panduan dan standar untuk mengelola risiko keamanan siber dan memastikan bahwa perusahaan di seluruh dunia mematuhi persyaratan kepatuhan yang relevan. Dalam konteks globalisasi dan digitalisasi yang semakin cepat, organisasi harus memahami berbagai regulasi yang berlaku di wilayah operasi mereka, serta

bagaimana kerangka kerja ini diimplementasikan untuk melindungi data dan privasi.

3.3.1 Prinsip-Prinsip Utama dalam Kerangka Kerja Global

Sebagian besar kerangka kerja regulasi keamanan siber berbagi prinsip-prinsip dasar yang serupa. Prinsip-prinsip ini menekankan perlindungan data pribadi, transparansi dalam pemrosesan data, serta hak konsumen atau pengguna terkait data mereka. Beberapa prinsip utama adalah:

1. Perlindungan Data Pribadi Setiap regulasi keamanan siber mengedepankan perlindungan terhadap data pribadi, memastikan bahwa data tidak digunakan atau diakses tanpa izin pemiliknya.
2. Transparansi dan Kejujuran Organisasi harus transparan tentang bagaimana data dikumpulkan, digunakan, dan disimpan. Ini termasuk pemberitahuan kepada konsumen mengenai tujuan pengumpulan data dan pihak ketiga yang memiliki akses ke data tersebut.
3. Kebebasan Pemilik Data Pengguna berhak meminta akses, perbaikan, atau penghapusan data pribadi mereka. Mereka juga dapat menarik persetujuan yang sebelumnya diberikan untuk pemrosesan data.
4. Kewajiban Keamanan Organisasi diwajibkan untuk menerapkan langkah-langkah teknis dan organisasi yang sesuai untuk melindungi data pribadi dari kebocoran, pencurian, atau akses tidak sah.
5. Pemberitahuan Insiden Keamanan Banyak kerangka kerja mengharuskan organisasi melaporkan insiden keamanan dalam batas waktu tertentu untuk meminimalkan dampak pelanggaran data.

3.3.2 Kerangka Kerja Regulasi Global

1. **GDPR: *General Data Protection Regulation* (Uni Eropa)**
   General Data Protection Regulation (GDPR) adalah peraturan privasi data yang paling komprehensif dan ketat di dunia, diadopsi oleh Uni Eropa dan mulai berlaku sejak 25 Mei 2018. Regulasi ini bertujuan untuk memberikan

perlindungan terhadap data pribadi warga negara Uni Eropa serta mengatur bagaimana perusahaan dan organisasi mengumpulkan, menyimpan, dan memproses informasi pribadi (Kubben, n.d.). GDPR tidak hanya berlaku bagi entitas yang berbasis di Uni Eropa, tetapi juga bagi perusahaan di luar Uni Eropa yang memproses data warga Uni Eropa, menjadikannya salah satu regulasi keamanan siber yang paling luas cakupannya secara global(Ziqra et al., 2021).

Gambar 3.1. *General Data Protection Regulation* (GDPR)
Sumber: https://wqa-apac.com

a. Cakupan dan Ruang Lingkup GDPR

GDPR berlaku untuk semua organisasi yang memproses data pribadi warga Uni Eropa, baik organisasi tersebut beroperasi di dalam Uni Eropa maupun di luar wilayahnya. Definisi "data pribadi" dalam GDPR mencakup segala informasi yang dapat mengidentifikasi individu secara langsung atau tidak langsung, seperti nama, alamat email, data lokasi, serta informasi identifikasi online (alamat IP). Peraturan ini dirancang untuk memperkuat hak-hak individu atas data mereka, memberikan kontrol lebih besar terkait bagaimana informasi pribadi mereka dikelola oleh organisasi.

GDPR mengharuskan semua organisasi untuk memiliki kebijakan dan prosedur yang jelas untuk mengelola data pribadi dan untuk memastikan kepatuhan terhadap hak-hak individu yang diatur oleh peraturan ini.

b. Prinsip-Prinsip Utama GDPR

GDPR didasarkan pada enam prinsip utama yang menjadi panduan dalam pengelolaan data pribadi(Carmi et al., 2023):

1) **Keabsahan, Keadilan, dan Transparansi**
   Data pribadi harus diproses secara sah, adil, dan transparan. Individu harus diberi tahu secara jelas tentang bagaimana data mereka akan digunakan dan tujuan pengumpulannya.
2) **Pembatasan Tujuan**
   Data hanya boleh dikumpulkan untuk tujuan yang telah ditentukan dengan jelas dan tidak boleh digunakan untuk tujuan lain yang tidak terkait.
3) **Minimalisasi Data**
   Hanya data pribadi yang relevan dan diperlukan yang boleh dikumpulkan. GDPR menekankan pentingnya meminimalkan jumlah data yang diproses untuk mencapai tujuan yang sah.
4) **Keakuratan**
   Data pribadi harus akurat dan, jika diperlukan, diperbarui. Langkah-langkah yang wajar harus diambil untuk memastikan bahwa data yang tidak akurat dihapus atau diperbaiki segera.
5) **Pembatasan Penyimpanan**
   Data pribadi tidak boleh disimpan lebih lama dari yang diperlukan untuk tujuan pemrosesan. GDPR menuntut organisasi untuk menetapkan kebijakan penyimpanan data yang jelas dan memastikan penghapusan data jika tidak lagi relevan.

6) **Integritas dan Kerahasiaan**
   Data pribadi harus diproses dengan cara yang menjamin keamanan yang sesuai, termasuk perlindungan dari pemrosesan yang tidak sah atau melanggar hukum, kehilangan, kerusakan, atau kehancuran.

c. Hak-Hak Individu di Bawah GDPR

GDPR memberikan serangkaian hak yang kuat kepada individu, memungkinkan mereka memiliki kontrol penuh atas data pribadi mereka. Beberapa hak penting tersebut meliputi:

1) **Hak untuk Mengakses (*Right to Access*)**: Individu berhak mengetahui apakah data mereka diproses dan berhak meminta salinan data pribadi mereka yang sedang diproses oleh organisasi.
2) **Hak untuk Dihapus (*Right to be Forgotten*)**: Individu dapat meminta organisasi untuk menghapus data pribadi mereka dalam keadaan tertentu, terutama ketika data tersebut tidak lagi relevan atau ketika individu menarik persetujuan mereka.
3) **Hak untuk Memperbaiki (*Right to Rectification*)**: Jika data yang disimpan tidak akurat atau tidak lengkap, individu dapat meminta agar data mereka diperbarui atau diperbaiki.
4) **Hak untuk Membatasi Pemrosesan (*Right to Restriction of Processing*)**: Individu dapat meminta pembatasan pemrosesan data mereka dalam situasi tertentu, misalnya ketika data dianggap tidak akurat atau diproses secara ilegal.
5) **Hak atas Portabilitas Data (*Right to Data Portability*)**: Individu berhak meminta data mereka dalam format yang dapat dipindahkan dan dapat mengirimkannya ke pengendali data lain.
6) **Hak untuk Menolak Pemrosesan (*Right to Object*)**: Individu dapat menolak pemrosesan data

pribadi mereka untuk tujuan tertentu, seperti pemasaran langsung(G. Data & Regulation, 2024).

d. Kewajiban Organisasi di Bawah GDPR

Organisasi yang memproses data pribadi diharuskan mematuhi sejumlah kewajiban yang ketat di bawah GDPR. Beberapa kewajiban ini mencakup:

1) **Penunjukan Data *Protection Officer* (DPO)**: Organisasi yang memproses data dalam skala besar harus menunjuk seorang DPO yang bertanggung jawab untuk memastikan kepatuhan terhadap GDPR.
2) **Penilaian Dampak Perlindungan Data (*Data Protection Impact Assessment* - DPIA)**: Organisasi harus melakukan DPIA ketika melakukan pemrosesan data yang dapat menimbulkan risiko tinggi terhadap hak-hak dan kebebasan individu.
3) **Pemberitahuan Pelanggaran Data**: Dalam hal terjadi pelanggaran data, organisasi diharuskan melaporkan insiden tersebut kepada otoritas perlindungan data dalam waktu 72 jam setelah kejadian, serta memberitahukan subjek data jika pelanggaran tersebut berisiko tinggi.
4) **Konsentrat Eksplisit**: GDPR mewajibkan organisasi untuk memperoleh persetujuan eksplisit dari individu sebelum memproses data pribadi mereka, terutama dalam kasus pemrosesan data sensitif.

e. Sanksi dan Denda di Bawah GDPR

GDPR menetapkan denda yang sangat berat bagi pelanggaran regulasi, dengan dua tingkatan denda:

1) Denda maksimum **10 juta euro atau 2% dari pendapatan tahunan global**, mana yang lebih besar, untuk pelanggaran administratif seperti kurangnya catatan yang sesuai atau gagal melaporkan pelanggaran data tepat waktu.

2) Denda maksimum **20 juta euro atau 4% dari pendapatan tahunan global**, mana yang lebih besar, untuk pelanggaran yang lebih berat, seperti gagal mendapatkan persetujuan yang sah untuk pemrosesan data atau gagal menghormati hak-hak individu di bawah GDPR.
Pemberlakuan sanksi ini bertujuan untuk mendorong perusahaan menjaga standar keamanan yang tinggi dalam pengelolaan data pribadi, serta memastikan bahwa hak-hak individu dihormati dengan baik(G. Data & Regulation, 2024).

f. Dampak GDPR pada Perusahaan Global

Penerapan GDPR tidak hanya berdampak pada perusahaan yang berbasis di Uni Eropa, tetapi juga bagi organisasi di seluruh dunia yang memproses data warga Uni Eropa. Hal ini memaksa banyak perusahaan global untuk merevisi kebijakan privasi mereka, memperkuat protokol keamanan, dan mengadopsi pendekatan privasi sejak awal (*privacy by design*). Perusahaan besar seperti Google dan Facebook telah dikenai denda signifikan karena pelanggaran GDPR, yang menyoroti pentingnya kepatuhan yang ketat terhadap regulasi ini. Selain itu, penerapan GDPR juga memicu reformasi regulasi privasi di negara-negara lain, termasuk di Amerika Serikat dan Asia, yang mulai mengadopsi kerangka kerja privasi yang lebih ketat.

2. *California Consumer Privacy Act* (CCPA)

California Consumer Privacy Act (CCPA) adalah salah satu undang-undang privasi data paling signifikan yang diimplementasikan di Amerika Serikat, yang berlaku mulai 1 Januari 2020. Undang-undang ini bertujuan untuk meningkatkan hak privasi dan perlindungan data bagi warga negara bagian California. CCPA sering dibandingkan dengan *General Data Protection Regulation* (GDPR) yang diterapkan oleh Uni Eropa, karena keduanya memberikan

hak yang kuat kepada individu terkait data pribadi mereka, meskipun terdapat perbedaan mendasar dalam ruang lingkup dan penerapan(Wong, 2023).

CCPA memberikan wewenang kepada konsumen California untuk mengontrol informasi pribadi mereka dan mewajibkan perusahaan untuk transparan dalam bagaimana data dikumpulkan, diproses, dan dijual. Undang-undang ini dipandang sebagai langkah awal Amerika Serikat menuju undang-undang privasi data yang lebih komprehensif di tingkat federal(Ehimuan et al., 2024).

Gambar 3.2. Ilustrasi California Consumer Privacy Act (CCPA)
Sumber: https://dropsuite.com/

a. Cakupan dan Ruang Lingkup CCPA

CCPA berlaku untuk perusahaan yang beroperasi di California atau yang memproses data warga California, dan memenuhi salah satu dari tiga kriteria berikut:

1) Memiliki pendapatan tahunan lebih dari $25 juta,
2) Memproses data pribadi lebih dari 50.000 konsumen, rumah tangga, atau perangkat,
3) Mendapatkan lebih dari 50% pendapatan tahunannya dari penjualan data konsumen.

Dengan cakupan ini, CCPA tidak hanya berlaku bagi perusahaan besar, tetapi juga bagi bisnis yang sangat bergantung pada data konsumen dalam kegiatan komersialnya. Data pribadi yang dicakup

oleh CCPA meliputi informasi yang mengidentifikasi, berhubungan, menjelaskan, atau mampu dikaitkan dengan individu tertentu, seperti nama, alamat, alamat IP, dan informasi perilaku online.

b. Hak-Hak Konsumen di Bawah CCPA

CCPA memberikan serangkaian hak penting kepada konsumen California terkait data pribadi mereka. Hak-hak ini bertujuan untuk memberikan kontrol yang lebih besar kepada individu atas informasi mereka dan memaksa perusahaan untuk bertindak lebih transparan dan bertanggung jawab dalam menangani data. Beberapa hak utama yang diatur oleh CCPA antara lain(Satria & Yusuf, 2024):

1) **Hak untuk Mengetahui (*Right to Know*)**: Konsumen memiliki hak untuk mengetahui kategori dan jenis data pribadi yang dikumpulkan oleh perusahaan, sumber data tersebut, tujuan pengumpulan, dan dengan siapa data tersebut dibagikan atau dijual.
2) **Hak untuk Menghapus (*Right to Delete*)**: Konsumen dapat meminta perusahaan untuk menghapus data pribadi mereka. Namun, ada beberapa pengecualian untuk permintaan ini, seperti ketika data dibutuhkan untuk menyelesaikan transaksi, mematuhi kewajiban hukum, atau digunakan untuk tujuan penelitian ilmiah atau statistik yang sah.
3) **Hak untuk Menolak Penjualan Data (*Right to Opt-Out*)**: Konsumen dapat meminta agar data pribadi mereka tidak dijual kepada pihak ketiga. Bagi konsumen di bawah usia 16 tahun, CCPA mewajibkan persetujuan eksplisit dari individu (atau orang tua/wali jika di bawah 13 tahun) sebelum data mereka dapat dijual.

4) **Hak untuk Tidak Didiskriminasi (*Right to Non-Discrimination*)**: Perusahaan tidak boleh mendiskriminasi konsumen yang menggunakan hak-hak mereka di bawah CCPA. Misalnya, perusahaan tidak dapat menolak layanan, membebankan harga berbeda, atau memberikan kualitas produk atau layanan yang lebih rendah hanya karena konsumen menggunakan hak mereka untuk menolak penjualan data.

c. Kewajiban Perusahaan di Bawah CCPA

CCPA mewajibkan perusahaan untuk mengambil langkah-langkah tertentu guna memastikan kepatuhan terhadap regulasi, termasuk:

1) **Pemberitahuan kepada Konsumen**: Perusahaan diwajibkan untuk memberikan pemberitahuan kepada konsumen sebelum atau pada saat pengumpulan data, yang menjelaskan kategori data yang dikumpulkan dan tujuan penggunaannya.
2) **Penjualan Data**: Jika perusahaan menjual data konsumen, mereka harus memberikan link bertuliskan "Do Not Sell My Personal Information" di situs web mereka yang memungkinkan konsumen untuk menolak penjualan data.
3) **Penyediaan Akses Data**: Perusahaan harus memberikan cara bagi konsumen untuk mengakses dan mendapatkan salinan data pribadi mereka. Ini harus dilakukan tanpa biaya kepada konsumen, kecuali dalam kasus di mana permintaan dianggap berlebihan atau berulang.

d. Sanksi dan Denda di Bawah CCPA

Perusahaan yang melanggar ketentuan CCPA dapat dikenakan denda hingga $2.500 per pelanggaran tidak disengaja dan hingga $7.500 per pelanggaran yang disengaja. Selain itu, CCPA memberikan hak kepada konsumen untuk mengambil tindakan hukum secara

langsung terhadap perusahaan dalam kasus-kasus tertentu, seperti dalam hal terjadinya pelanggaran data yang mengakibatkan data pribadi terekspos.

e. Dampak CCPA pada Perusahaan dan Konsumen

Penerapan CCPA telah memaksa banyak perusahaan untuk merevisi kebijakan privasi mereka, memperkuat langkah-langkah keamanan data, dan meningkatkan transparansi terkait praktik pengumpulan dan penggunaan data. Bagi konsumen, CCPA memberikan kontrol lebih besar atas data pribadi mereka, meskipun banyak yang berpendapat bahwa CCPA masih belum seketat GDPR dalam hal persetujuan dan perlindungan data. Meskipun CCPA hanya berlaku di California, dampaknya dirasakan oleh perusahaan di seluruh Amerika Serikat dan dunia, karena banyak perusahaan memilih untuk menerapkan kebijakan yang konsisten di seluruh negara demi efisiensi dan untuk menghindari masalah hukum di California.

CCPA adalah langkah penting menuju perlindungan privasi data yang lebih kuat di Amerika Serikat, meskipun ruang lingkupnya terbatas pada California. Undang-undang ini memberikan hak signifikan kepada konsumen terkait data pribadi mereka dan mewajibkan perusahaan untuk lebih transparan dan akuntabel dalam pengelolaan data. Dengan denda yang substansial dan kewajiban yang ketat, CCPA memaksa perusahaan untuk memperlakukan privasi data sebagai prioritas utama dalam operasi mereka, serta mendorong perkembangan regulasi serupa di negara bagian dan tingkat federal di Amerika Serikat

3. *Health Insurance Portability and Accountability Act* (HIPAA)

***Health Insurance Portability and Accountability Act* (HIPAA)** adalah undang-undang federal Amerika Serikat yang disahkan pada tahun 1996, dengan tujuan melindungi

hak-hak privasi individu terkait data kesehatan mereka. HIPAA mengatur bagaimana informasi kesehatan pribadi atau *Protected Health Information* (PHI) dapat dikumpulkan, disimpan, dan dibagikan oleh penyedia layanan kesehatan, perusahaan asuransi, serta entitas terkait lainnya. Tujuan utama dari undang-undang ini adalah untuk menjaga kerahasiaan informasi kesehatan dan memastikan perlindungan bagi pasien serta konsumen layanan Kesehatan.

HIPAA memiliki dua komponen utama: **Title I** yang berfokus pada jaminan asuransi kesehatan untuk pekerja yang berganti pekerjaan atau menganggur, serta **Title II**, yang dikenal sebagai *Administrative Simplification*, yang mengatur standar privasi dan keamanan untuk informasi kesehatan(Satria & Yusuf, 2024).

a. Cakupan dan Ruang Lingkup HIPA

HIPAA berlaku bagi apa yang disebut sebagai "*covered entities*," yaitu penyedia layanan kesehatan, perusahaan asuransi kesehatan, dan penyedia layanan pihak ketiga yang menangani data kesehatan dalam berbagai bentuk (baik fisik maupun digital). HIPAA juga berlaku untuk "*business associates*," yaitu pihak ketiga yang mengakses atau memproses PHI atas nama entitas yang tercakup. HIPAA mengatur perlindungan terhadap informasi yang berkaitan dengan kesehatan fisik atau mental seseorang, pelayanan kesehatan yang diterima, serta pembayaran atas layanan kesehatan. Undang-undang ini mengatur semua bentuk data kesehatan, termasuk catatan medis, hasil uji laboratorium, serta informasi yang diperoleh melalui konsultasi medis.

b. Komponen Utama HIPAA

HIPAA terbagi menjadi beberapa aturan penting yang menjadi dasar bagi perlindungan data kesehatan. Di antara aturan-aturan tersebut, yang paling menonjol adalah (Oakley, 2023):

1) ***Privacy Rule***: Aturan ini menetapkan hak-hak individu atas informasi kesehatan pribadi mereka, serta membatasi pengungkapan informasi kesehatan tanpa persetujuan. *Privacy Rule* mengharuskan penyedia layanan kesehatan dan perusahaan asuransi untuk memberikan pemberitahuan tertulis kepada pasien mengenai hak-hak mereka dan cara informasi akan digunakan.
2) ***Security Rule***: Aturan ini memberikan panduan tentang bagaimana data kesehatan elektronik harus dilindungi dari ancaman fisik, teknis, dan administratif. *Security Rule* mencakup langkah-langkah teknis seperti enkripsi, kontrol akses, serta audit log untuk memonitor akses ke data.
3) ***Breach Notification Rule***: Aturan ini mewajibkan entitas yang tercakup untuk memberitahukan individu yang terkena dampak jika terjadi pelanggaran data yang melibatkan PHI. Pemberitahuan tersebut harus dilakukan dalam waktu 60 hari sejak pelanggaran diketahui, dan dalam kasus-kasus tertentu, pelanggaran harus dilaporkan kepada Departemen Kesehatan dan Layanan Kemanusiaan (HHS) serta media.

c. Prinsip-Prinsip Privasi HIPAA

Prinsip utama yang diatur dalam HIPAA bertujuan untuk melindungi kerahasiaan data kesehatan pasien serta memastikan bahwa informasi tersebut hanya digunakan untuk tujuan yang sah. Beberapa prinsip penting yang diatur oleh HIPAA antara lain:

1) **Prinsip Minimization of Data**: Hanya informasi yang relevan dan diperlukan untuk tujuan tertentu yang boleh diakses dan diproses. Ini berarti bahwa penyedia layanan kesehatan tidak boleh mengumpulkan lebih banyak data dari yang diperlukan untuk menyediakan layanan kepada pasien.

2) **Kontrol Akses**: HIPAA menetapkan bahwa hanya pihak yang sah dan memiliki izin yang dapat mengakses data kesehatan pasien. Penyedia layanan kesehatan diharuskan untuk menerapkan kontrol teknis dan administratif untuk memastikan bahwa hanya staf yang berwenang dapat mengakses informasi kesehatan.
3) **Hak Individu**: HIPAA memberikan hak kepada pasien untuk mengakses, meninjau, dan memperbaiki informasi kesehatan mereka. Pasien juga memiliki hak untuk meminta pembatasan dalam penggunaan atau pengungkapan data kesehatan mereka.

d. Kewajiban Penyedia Layanan Kesehatan di Bawah HIPAA

Penyedia layanan kesehatan serta perusahaan asuransi kesehatan memiliki sejumlah kewajiban yang harus dipatuhi di bawah HIPAA, termasuk(Margaretha Peggy Pomantow, 2Rokhmat, 2023):

1) **Kewajiban untuk Melindungi Data**: HIPAA mengharuskan entitas yang tercakup untuk menerapkan langkah-langkah keamanan yang sesuai guna melindungi informasi kesehatan elektronik, termasuk perlindungan terhadap serangan siber, kehilangan data, atau akses tidak sah.
2) **Pelatihan dan Edukasi Staf**: HIPAA mengharuskan entitas yang tercakup untuk memberikan pelatihan reguler kepada staf mengenai kebijakan privasi dan keamanan informasi kesehatan. Hal ini penting agar semua pihak yang berinteraksi dengan PHI memahami kewajiban dan standar yang berlaku.
3) **Audit dan Pemantauan**: Untuk mematuhi Security Rule, entitas yang tercakup diwajibkan untuk melakukan audit berkala terhadap sistem mereka

dan memantau akses ke data guna mendeteksi potensi ancaman atau pelanggaran.

e. Penegakan dan Sanksi di Bawah HIPAA

Pelanggaran terhadap ketentuan HIPAA dapat mengakibatkan sanksi yang signifikan, baik dari segi denda maupun dampak reputasi. Denda untuk pelanggaran HIPAA tergantung pada tingkat keparahan pelanggaran, niat, dan upaya mitigasi yang dilakukan oleh entitas yang melanggar. Denda dapat mencapai:

1) Hingga **$50.000 per pelanggaran** dengan maksimum tahunan hingga **$1,5 juta**.
2) Pelanggaran yang disengaja dapat mengakibatkan denda lebih besar dan dalam beberapa kasus, termasuk hukuman pidana.

   Selain denda, pelanggaran privasi data kesehatan dapat menyebabkan kerugian reputasi yang signifikan bagi penyedia layanan kesehatan, yang berdampak pada kepercayaan pasien dan masyarakat terhadap institusi tersebut.

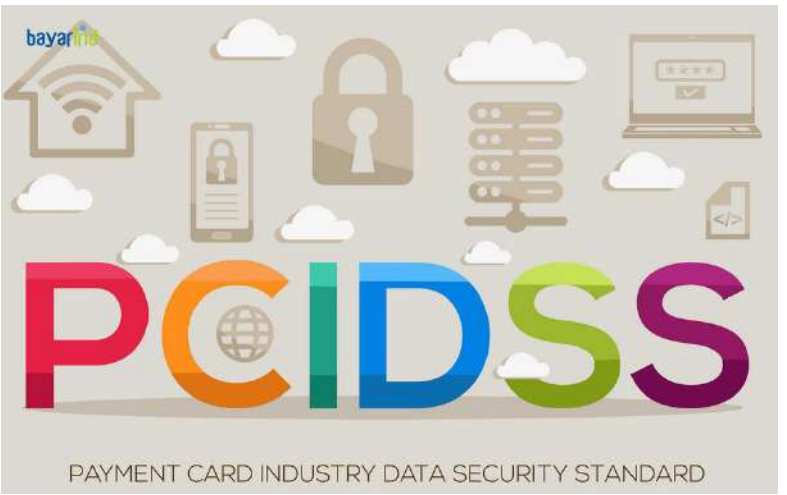
f. Dampak HIPAA pada Industri Kesehatan

HIPAA telah memberikan dampak yang luas terhadap industri layanan kesehatan, terutama dalam hal peningkatan kesadaran dan komitmen terhadap keamanan data. Penyedia layanan kesehatan dan entitas lain yang terkait dengan industri kesehatan telah berinvestasi besar-besaran dalam infrastruktur keamanan digital, termasuk penerapan sistem informasi kesehatan elektronik yang lebih aman. Namun, meskipun HIPAA telah berhasil meningkatkan perlindungan data di Amerika Serikat, masih terdapat tantangan dalam hal penerapan standar yang konsisten di seluruh penyedia layanan kesehatan, khususnya di institusi-institusi kecil yang mungkin memiliki sumber daya terbatas untuk memenuhi semua persyaratan regulasi.

4. ***Payment Card Industry Data Security Standard* (PCI DSS)**

Payment Card Industry Data Security Standard (PCI DSS) adalah standar keamanan informasi yang dirancang untuk memastikan bahwa semua perusahaan yang menerima, memproses, menyimpan, atau mentransmisikan informasi kartu kredit tetap menjaga lingkungan data yang aman. PCI DSS pertama kali diperkenalkan pada tahun 2004 oleh konsorsium utama kartu kredit, termasuk Visa, MasterCard, American Express, JCB, dan Discover, yang kemudian membentuk *Payment Card Industry Security Standards Council (PCI SSC)* untuk mengelola dan mengawasi kepatuhan terhadap standar ini (Margaretha Peggy Pomantow, 2Rokhmat, 2023).

PCI DSS berlaku secara global dan diimplementasikan oleh semua bisnis, mulai dari pedagang kecil hingga perusahaan besar, yang menangani informasi kartu kredit. Tujuan utama PCI DSS adalah untuk mencegah pencurian data kartu kredit dan meminimalkan risiko pelanggaran keamanan data yang dapat menyebabkan kerugian finansial dan reputasi yang signifikan bagi bisnis dan pelanggan.



Gambar 3.3. *Payment Card Industry Data Security Standard* (PCI DSS)
Sumber: https://pgbayarind.id/

a. Cakupan dan Ruang Lingkup PCI DSS

PCI DSS terdiri dari serangkaian standar keamanan yang harus dipatuhi oleh entitas yang menangani data kartu pembayaran. Standar ini berlaku untuk semua entitas yang terlibat dalam pemrosesan, penyimpanan, dan pengiriman data kartu pembayaran, baik secara langsung maupun melalui pihak ketiga. Lingkup PCI DSS mencakup perlindungan terhadap informasi sensitif kartu pembayaran, termasuk data pemegang kartu dan *Sensitive Authentication Data* (SAD), seperti PIN atau kode otorisasi. PCI DSS dibagi menjadi enam tujuan utama yang diuraikan menjadi 12 persyaratan yang harus dipenuhi oleh organisasi untuk memastikan keamanan data kartu kredit(Selatan, 2019):

b. 12 Persyaratan PCI DSS

PCI DSS mencakup 12 persyaratan utama yang dibagi menjadi enam tujuan keamanan yang lebih luas. Setiap persyaratan dirancang untuk mengatasi aspek keamanan tertentu, mulai dari pengamanan infrastruktur jaringan hingga pengelolaan kebijakan keamanan data(Selatan, 2019).

1) Membangun dan Memelihara Infrastruktur Jaringan yang Aman
   - Persyaratan 1: Menginstal dan memelihara konfigurasi firewall untuk melindungi data pemegang kartu.
   - Persyaratan 2: Jangan menggunakan kata sandi sistem dan parameter keamanan yang default.
2) Melindungi Data Pemegang Kartu
   - Persyaratan 3: Melindungi data yang disimpan dari pemegang kartu, seperti nomor kartu kredit, nama pemegang kartu, dan tanggal kedaluwarsa.
   - Persyaratan 4: Enkripsi transmisi data pemegang kartu saat melewati jaringan publik dan terbuka.

3) Mempertahankan Program Manajemen Kerentanan
    - Persyaratan 5: Melindungi semua sistem terhadap malware dan memperbarui perangkat lunak antivirus secara teratur.
    - Persyaratan 6: Mengembangkan dan memelihara aplikasi dan sistem yang aman melalui patching serta pengujian kerentanan secara berkala.
4) Menerapkan Langkah-Langkah Kontrol Akses yang Kuat
    - Persyaratan 7: Batasi akses ke data pemegang kartu hanya kepada pihak-pihak yang sah.
    - Persyaratan 8: Menggunakan kontrol identitas dan otentikasi unik untuk setiap pengguna dengan akses ke sistem.
    - Persyaratan 9: Membatasi akses fisik ke data pemegang kartu.
5) Memantau dan Menguji Jaringan
    - Persyaratan 10: Melacak dan memantau semua akses ke sumber daya jaringan dan data pemegang kartu.
    - Persyaratan 11: Secara teratur menguji sistem keamanan dan proses.
6) Memelihara Kebijakan Keamanan Informasi
    - Persyaratan 12: Memelihara kebijakan yang mengatur keamanan informasi, termasuk pelatihan dan edukasi karyawan terkait keamanan data.

c. Tingkat Kepatuhan PCI DS

PCI DSS mengklasifikasikan perusahaan berdasarkan volume transaksi kartu pembayaran yang mereka proses setiap tahunnya. Berdasarkan volume ini, ada empat tingkat kepatuhan:

1) **Level 1**: Perusahaan yang memproses lebih dari 6 juta transaksi kartu kredit per tahun.

2) **Level 2**: Perusahaan yang memproses antara 1 hingga 6 juta transaksi per tahun.
3) **Level 3**: Perusahaan yang memproses antara 20.000 hingga 1 juta transaksi per tahun.
4) **Level 4**: Perusahaan yang memproses kurang dari 20.000 transaksi per tahun.

Perusahaan di Level 1 harus menjalani audit kepatuhan tahunan oleh *Qualified Security Assessor* (QSA) yang disetujui PCI SSC, sedangkan perusahaan pada level lainnya diharuskan untuk mengisi Self-Assessment Questionnaire (SAQ) setiap tahun dan menjalani pemeriksaan rutin.

d. Konsekuensi Ketidak patuhan terhadap PCI DSS

Ketidakpatuhan terhadap PCI DSS dapat menyebabkan konsekuensi yang serius, termasuk denda, biaya audit yang mahal, peningkatan biaya pemrosesan kartu, serta risiko kerugian reputasi. Denda untuk ketidakpatuhan bisa mencapai $5.000 hingga $100.000 per bulan hingga organisasi tersebut sepenuhnya mematuhi standar tersebut. Selain itu, ketidakpatuhan juga dapat menyebabkan bisnis dikeluarkan dari program penerimaan kartu kredit, yang bisa sangat merugikan operasi perusahaan. Selain denda finansial, risiko lainnya termasuk kehilangan kepercayaan konsumen dan terjadinya pelanggaran data yang bisa berdampak luas. Dalam beberapa kasus, kerugian reputasi akibat pelanggaran keamanan data bisa lebih merusak daripada sanksi finansial.

e. Dampak dan Tantangan Implementasi PCI DSS

Implementasi PCI DSS membutuhkan sumber daya yang signifikan, terutama bagi organisasi dengan infrastruktur TI yang besar atau kompleks. Tantangan utama dalam kepatuhan PCI DSS termasuk:

1) Biaya Implementasi: Untuk memenuhi semua persyaratan, perusahaan sering kali harus

berinvestasi dalam perangkat keras baru, perangkat lunak keamanan, dan layanan keamanan yang dikelola. Ini bisa menjadi beban besar bagi bisnis kecil atau menengah.

2) **Pemeliharaan Berkelanjutan**: PCI DSS bukanlah persyaratan sekali saja, tetapi membutuhkan pemantauan dan pemeliharaan keamanan secara berkelanjutan. Ini mencakup pengujian kerentanan yang berkelanjutan, audit internal, dan pelatihan staf secara berkala.
3) **Kompleksitas Teknologi**: Infrastruktur teknologi yang kompleks, termasuk banyak titik akses dan sistem yang terintegrasi, dapat membuat kepatuhan lebih sulit dicapai.

Namun, manfaat utama dari kepatuhan PCI DSS adalah peningkatan kepercayaan pelanggan terhadap perusahaan yang memproses transaksi mereka, pengurangan risiko pelanggaran data, dan penurunan potensi kerugian akibat pencurian data.

3.4 Kerangka Regulasi Keamanan Siber di Indonesia

Indonesia sedang berada di jalur yang tepat dalam memperkuat kerangka regulasi keamanan sibernya. Mengingat kemajuan teknologi yang pesat dan peningkatan transaksi digital di hampir semua sektor, upaya untuk melindungi data dan menjaga sistem siber nasional dari ancaman menjadi sangat penting. Di bawah ini adalah uraian lebih mendetail mengenai kerangka regulasi yang berlaku, serta berbagai undang-undang, peraturan, dan lembaga yang terlibat dalam pengawasan keamanan siber di Indonesia.

3.4.1 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE

Undang-Undang Nomor 11 Tahun 2008, yang kemudian direvisi oleh Undang-Undang Nomor 19 Tahun 2016, dikenal sebagai Undang-Undang Informasi dan Transaksi Elektronik (UU

ITE). UU ITE mengatur berbagai aspek penggunaan teknologi informasi di Indonesia, mulai dari transaksi elektronik, perlindungan data, hingga hukuman bagi pelanggar yang terlibat dalam kejahatan siber(D. F. Saputra, 2023)(Selatan, 2019).
Beberapa poin penting yang diatur oleh UU ITE meliputi:

1. **Transaksi Elektronik yang Aman**: UU ITE mewajibkan semua pihak yang terlibat dalam transaksi elektronik untuk memastikan bahwa transaksi tersebut dilaksanakan dengan tingkat keamanan yang memadai.
2. **Sistem Perlindungan Data**: Pengelola sistem elektronik diwajibkan untuk menjaga integritas dan kerahasiaan data yang mereka simpan dari ancaman siber.
3. **Penegakan Hukum Terhadap Kejahatan Siber**: Pelaku kejahatan siber, seperti peretasan, manipulasi data, atau distribusi malware, dapat dikenakan sanksi pidana yang berat sesuai dengan ketentuan UU ITE.
4. **Penghapusan Konten Negatif**: UU ITE juga mengatur tentang tanggung jawab penyedia platform digital dalam menangani konten yang melanggar hukum, seperti ujaran kebencian, penipuan online, dan konten pornografi.

3.4.2 Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)

Peraturan Pemerintah Nomor 71 Tahun 2019 menggantikan PP Nomor 82 Tahun 2012, dan bertujuan untuk memperbarui regulasi terkait penyelenggaraan sistem dan transaksi elektronik yang semakin kompleks di era digital
Poin-poin utama PP PSTE meliputi(D. F. Saputra, 2023):

1. **Tanggung Jawab Penyelenggara Sistem Elektronik (PSE)**: Penyelenggara Sistem Elektronik, baik itu sektor publik maupun privat, diwajibkan untuk mengamankan data yang mereka kelola dari serangan atau akses yang tidak sah.
2. **Lokalisasi Data**: Ketentuan tentang lokalisasi data yang mengharuskan data disimpan di Indonesia telah dilonggarkan, tetapi tetap ada kewajiban bahwa akses data harus tetap tersedia untuk keperluan hukum dalam yurisdiksi Indonesia.

3. **Manajemen Insiden Siber**: PSE diwajibkan untuk melaporkan insiden keamanan yang signifikan kepada otoritas dalam jangka waktu yang ditetapkan. Hal ini membantu pemerintah dalam merespons insiden siber secara cepat dan terkoordinasi.

3.4.3 Undang-Undang Perlindungan Data Pribadi (UU PDP)

UU PDP yang disahkan pada tahun 2022 merupakan tonggak penting dalam regulasi keamanan siber di Indonesia. UU ini bertujuan untuk memberikan perlindungan terhadap privasi individu serta memastikan bahwa pengumpulan dan pengelolaan data pribadi dilakukan secara sah dan aman(Niffari, 2020).
Beberapa ketentuan penting dalam UU PDP meliputi:

1. **Pengelolaan Data Pribadi**: Pengendali data diwajibkan untuk mendapatkan persetujuan eksplisit dari pemilik data sebelum memproses data mereka. Pengendali juga harus menjamin keamanan data dari pencurian atau kebocoran.
2. **Hak Subjek Data**: Subjek data memiliki hak untuk mengakses, memperbarui, mengoreksi, atau menghapus data mereka. Ini memberi kontrol yang lebih besar kepada individu atas informasi pribadi mereka.
3. **Sanksi Hukum**: Pelanggaran terhadap UU PDP, seperti penyalahgunaan data pribadi tanpa izin, dapat dikenakan sanksi administratif, denda, hingga hukuman pidana.

3.4.4 Peraturan Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) dalam Sektor Keuangan

Sektor keuangan merupakan sektor yang paling diatur secara ketat dalam hal keamanan siber karena tingginya risiko terkait data nasabah dan transaksi finansial. Beberapa peraturan utama di sektor ini adalah:

1. **Penerapan Manajemen Risiko TI oleh Bank Umum**: Baik OJK maupun BI mengeluarkan aturan yang mewajibkan bank untuk menerapkan manajemen risiko teknologi informasi yang efektif. Bank wajib menjaga integritas, kerahasiaan, dan ketersediaan sistem elektroniknya.
2. **Peraturan Tentang Pembayaran Elektronik**: BI juga menerapkan standar keamanan untuk penyelenggara

pembayaran elektronik, yang mencakup enkripsi dan otentikasi ganda guna melindungi transaksi pembayaran dari ancaman siber (Sulistianingsih et al., 2023).

Tabel 3.1. Tabel Perbandingan Regulasi Keamanan Siber di Indonesia

Regulasi	Cakupan	Fokus Utama	Tahun Penerapan	Lembaga Pengawas
UU ITE	Teknologi Informasi dan Komunikasi	Keamanan transaksi elektronik, kejahatan siber	2008, 2016 (amendemen)	Kominfo, BSSN
PP No. 71 Tahun 2019 (PSTE)	Penyelenggaraan Sistem Elektronik	Manajemen sistem elektronik, pelaporan insiden	2019	BSSN, Kominfo
UU Perlindungan Data Pribadi (PDP)	Perlindungan Data Pribadi	Hak subjek data, pengelolaan data pribadi	2022	Kementerian Kominfo, BSSN
Peraturan OJK dan BI	Sektor Keuangan	Manajemen risiko TI, keamanan pembayaran	2016, 2020	OJK, BI

3.4.5 Peran Badan Siber dan Sandi Negara (BSSN)

Badan Siber dan Sandi Negara (BSSN) merupakan lembaga pemerintah Indonesia yang memiliki mandat untuk melaksanakan tugas pengamanan siber nasional serta pengelolaan enkripsi (sandi). BSSN didirikan berdasarkan Peraturan Presiden No. 53 Tahun 2017 yang disempurnakan melalui Peraturan Presiden No. 133 Tahun 2017. Lembaga ini berfungsi sebagai garda terdepan dalam upaya menjaga keamanan siber nasional di tengah pesatnya perkembangan teknologi digital(Governance et al., 2019).

Seiring meningkatnya ancaman siber di Indonesia, BSSN memiliki peran krusial dalam memastikan keamanan infrastruktur kritis, melindungi informasi sensitif, dan mempromosikan

kesadaran keamanan siber di berbagai sektor. Berikut adalah peran utama BSSN yang dirinci dengan lebih detail:

1. **Membangun dan Menerapkan Kebijakan Keamanan Siber**

   Sebagai lembaga pengawas utama di bidang keamanan siber, BSSN bertanggung jawab dalam merumuskan dan mengimplementasikan kebijakan keamanan siber di Indonesia. Kebijakan-kebijakan ini mencakup regulasi yang mengatur tata kelola keamanan informasi, standar keamanan siber untuk sektor publik dan swasta, serta pedoman terkait pengamanan data pribadi. Kebijakan strategis BSSN meliputi(Sutra & Haryanto, 2023):

   a. Menetapkan standar keamanan informasi nasional yang harus dipatuhi oleh seluruh lembaga pemerintah dan perusahaan swasta yang mengelola infrastruktur kritis.
   b. Mengembangkan protokol keamanan yang diperlukan untuk mencegah serangan siber, baik di tingkat nasional maupun lokal.
   c. Mengkoordinasikan tanggapan terhadap insiden siber yang terjadi, termasuk menetapkan rencana mitigasi untuk insiden keamanan yang merugikan infrastruktur digital negara.

2. **Mengelola Ancaman Siber**

   BSSN bertugas untuk memantau dan mengidentifikasi potensi ancaman siber di Indonesia. Lembaga ini bekerja sama dengan sektor publik dan swasta untuk mengidentifikasi ancaman yang berkembang, baik dari dalam negeri maupun internasional. Salah satu fungsi utama BSSN adalah memastikan bahwa infrastruktur kritis nasional (seperti sektor keuangan, energi, transportasi, dan komunikasi) terlindungi dari serangan siber. Untuk menangani ancaman tersebut, BSSN memiliki beberapa program utama(Siber & Sandi, 2022):

   a. ***Cyber Threat Intelligence***: BSSN secara proaktif mengumpulkan dan menganalisis informasi terkait ancaman siber, termasuk pola serangan yang sedang

berkembang. Informasi ini kemudian digunakan untuk memperbarui kebijakan pertahanan siber nasional.

b. Sistem Deteksi Dini (*Early Warning System*): BSSN juga menerapkan sistem deteksi dini yang dirancang untuk mengidentifikasi serangan siber sebelum terjadi atau pada tahap awal, sehingga memungkinkan pemerintah dan organisasi terkait untuk merespons dengan cepat.

3. Penanggulangan Insiden Siber

BSSN bertindak sebagai pusat koordinasi untuk penanganan insiden siber nasional. Jika terjadi serangan siber besar-besaran yang berdampak pada sistem penting negara atau sektor swasta, BSSN akan mengambil peran sebagai pemimpin dalam koordinasi tanggapan insiden dan memastikan langkah-langkah mitigasi yang tepat diambil. Tugas utama dalam penanggulangan insiden meliputi:

a. Menyusun prosedur standar penanggulangan insiden siber yang harus diterapkan oleh semua sektor, termasuk tata cara pelaporan insiden.
b. Berperan sebagai pusat koordinasi antara lembaga pemerintah, perusahaan swasta, dan penyedia layanan keamanan siber dalam merespons serangan siber secara cepat dan efektif.
c. Mempersiapkan respons nasional terkoordinasi terhadap serangan siber dengan melibatkan tim respon insiden yang terlatih dan berkolaborasi dengan lembaga internasional, jika diperlukan.

4. Peningkatan Kesadaran dan Kompetensi Keamanan Siber

Selain menangani ancaman dan insiden siber, BSSN juga berperan penting dalam meningkatkan kesadaran publik mengenai pentingnya keamanan siber. BSSN secara aktif melakukan sosialisasi dan pendidikan kepada masyarakat, instansi pemerintah, dan sektor swasta untuk meningkatkan pemahaman tentang ancaman siber dan cara

untuk melindungi diri dari ancaman tersebut. Beberapa inisiatif utama di bidang ini meliputi(Sudarmadi et al., 2019):

a. **Pelatihan Keamanan Siber**: BSSN menyelenggarakan pelatihan dan seminar untuk meningkatkan keterampilan dan pengetahuan terkait keamanan siber bagi personel TI di sektor publik dan swasta.
b. **Kampanye Kesadaran Siber**: BSSN menjalankan kampanye nasional untuk mempromosikan kesadaran akan pentingnya perlindungan data pribadi, serta bagaimana menghindari serangan phishing, malware, dan ancaman lainnya yang menargetkan masyarakat umum.

5. **Sertifikasi Keamanan dan Penerapan Standar**
   BSSN bertanggung jawab untuk mengeluarkan sertifikasi terkait keamanan informasi kepada perusahaan dan organisasi yang beroperasi di Indonesia. Ini termasuk sertifikasi sistem manajemen keamanan informasi (SMKI), yang memastikan bahwa organisasi-organisasi tersebut telah menerapkan standar keamanan yang sesuai. Tugas terkait sertifikasi dan standar meliputi:
   a. Menyusun dan memperbarui standar keamanan siber nasional yang harus diterapkan oleh sektor-sektor vital, termasuk sektor keuangan, energi, dan transportasi.
   b. Menyediakan sertifikasi keamanan bagi perusahaan yang telah memenuhi persyaratan dan standar keamanan yang ditetapkan oleh BSSN.
   c. Mengawasi audit kepatuhan keamanan siber di berbagai industri, memastikan bahwa semua sektor mematuhi pedoman keamanan yang telah ditetapkan.

6. **Kerjasama Internasional**
   BSSN juga terlibat dalam kerjasama internasional terkait keamanan siber. Lembaga ini menjalin kerjasama dengan badan-badan keamanan siber di negara lain serta organisasi internasional untuk saling bertukar informasi dan strategi

dalam menangani ancaman siber global. Kerjasama ini mencakup:

a. Berpartisipasi dalam forum internasional mengenai keamanan siber, seperti ASEAN *Cybersecurity Forum*, untuk berbagi pengalaman dan teknologi dalam mengelola keamanan siber di tingkat regional dan global.
b. Berkolaborasi dengan lembaga asing dalam penelitian dan pengembangan solusi keamanan siber yang inovatif, serta dalam upaya menangani serangan siber lintas negara yang mengancam keamanan nasional.
c. Memastikan bahwa Indonesia selalu mengikuti standar internasional terkait keamanan siber, seperti ISO/IEC 27001 dalam sistem manajemen keamanan informasi.

3.4.6 Tantangan Penerapan Kerangka Regulasi Siber

Meskipun kerangka regulasi keamanan siber di Indonesia terus berkembang, beberapa tantangan masih dihadapi dalam penerapannya:

1. **Sumber Daya Terbatas**: Banyak entitas, terutama usaha kecil dan menengah, masih kurang memiliki sumber daya yang memadai untuk menerapkan standar keamanan siber yang sesuai.
2. **Kesadaran Siber**: Kesadaran masyarakat dan perusahaan akan pentingnya keamanan siber masih perlu ditingkatkan, terutama dalam hal manajemen risiko siber yang berkelanjutan.
3. **Kompleksitas Teknologi**: Teknologi yang terus berkembang, seperti *cloud computing* dan *Internet of Things* (IoT), menambah tantangan dalam pengelolaan keamanan data dan penerapan standar yang relevan.

3.5 Tantangan dan Risiko dalam Penerapan Privasi dan Kepatuhan

Penerapan privasi dan kepatuhan regulasi dalam sistem keamanan siber bukanlah proses yang sederhana. Seiring dengan kemajuan teknologi digital yang pesat, organisasi, baik sektor publik maupun swasta, menghadapi berbagai tantangan dan risiko yang

signifikan dalam melindungi data pribadi serta memastikan bahwa operasional mereka mematuhi regulasi yang berlaku. Dalam bagian ini, kita akan mengulas beberapa tantangan utama yang sering dihadapi dalam penerapan privasi dan kepatuhan regulasi, yaitu risiko keamanan data, ancaman siber yang berhubungan dengan privasi, serta kesulitan dalam mengimplementasikan regulasi.

3.4.1 Risiko Keamanan Data

Risiko keamanan data merupakan tantangan utama yang dihadapi oleh organisasi dalam penerapan privasi dan kepatuhan. Di era digital saat ini, data merupakan salah satu aset paling berharga yang dimiliki oleh perusahaan dan individu. Namun, pengelolaan dan perlindungan data ini menjadi semakin sulit karena kompleksitas jaringan serta berbagai ancaman yang semakin canggih. Beberapa risiko keamanan data yang signifikan adalah:

1. **Kebocoran Data (Data Breach)**: Kebocoran data terjadi ketika informasi pribadi atau sensitif terekspos secara tidak sengaja atau dicuri oleh pihak yang tidak berwenang. Dalam beberapa tahun terakhir, kebocoran data yang terjadi di perusahaan besar, seperti bank, layanan kesehatan, atau platform e-commerce, telah merugikan jutaan pengguna. Insiden semacam ini tidak hanya menyebabkan kerugian finansial, tetapi juga merusak reputasi organisasi yang bersangkutan.
2. **Serangan Malware dan Ransomware**: Serangan melalui perangkat lunak berbahaya, seperti malware dan ransomware, merupakan ancaman yang signifikan bagi keamanan data. Ransomware, misalnya, mengenkripsi data organisasi dan menuntut tebusan untuk memulihkan akses. Ketika terjadi serangan seperti ini, data pribadi dan penting menjadi tidak dapat diakses dan bisa hilang jika tidak ada cadangan yang memadai.
3. **Kurangnya Kontrol Akses**: Banyak organisasi tidak memiliki sistem yang memadai untuk mengelola akses ke data sensitif. Tanpa kontrol akses yang tepat, data bisa diakses oleh pihak-pihak yang tidak berwenang, baik dari dalam maupun luar organisasi. Ini meningkatkan risiko kebocoran dan penyalahgunaan data.

Untuk mengatasi risiko ini, organisasi harus mengadopsi protokol keamanan data yang kuat, seperti penggunaan enkripsi, autentikasi dua faktor (*two-factor authentication*), dan implementasi manajemen akses berbasis peran (*role-based access control*). Selain itu, pelatihan dan kesadaran karyawan tentang pentingnya menjaga keamanan data harus ditingkatkan.

3.4.2 Ancaman Cyber yang Berhubungan dengan Privasi

Privasi data pribadi merupakan salah satu aspek terpenting dalam keamanan siber. Ancaman terhadap privasi semakin berkembang seiring dengan maraknya penggunaan teknologi digital dan internet. Beberapa ancaman yang signifikan terhadap privasi antara lain(Rima et al., 2023):

1. **Phishing**: Phishing adalah teknik yang digunakan oleh penjahat siber untuk mengelabui individu agar memberikan informasi pribadi mereka, seperti kata sandi atau nomor kartu kredit. Penipuan phishing sering kali dilakukan melalui email, pesan teks, atau situs web palsu yang dibuat seolah-olah berasal dari sumber yang terpercaya. Phishing sangat berbahaya karena dapat mengekspos data pribadi dan menyebabkan pencurian identitas.
2. **Tracking dan Profiling**: Di era digital saat ini, banyak perusahaan menggunakan teknologi untuk melacak perilaku pengguna secara online dan membuat profil berdasarkan aktivitas mereka. Data ini kemudian digunakan untuk tujuan komersial, seperti iklan yang disesuaikan, atau bahkan dijual ke pihak ketiga. Meskipun teknik ini mungkin tidak secara langsung membahayakan, namun merupakan ancaman signifikan terhadap privasi pengguna, terutama jika dilakukan tanpa persetujuan atau transparansi.
3. **Serangan Insider (Insider Threats)**: Ancaman dari dalam organisasi atau insider threats terjadi ketika seorang karyawan atau individu yang memiliki akses ke sistem organisasi menyalahgunakan akses tersebut untuk mendapatkan keuntungan pribadi atau merugikan organisasi. Insider threats sangat sulit dideteksi karena penyerang sering kali memiliki wewenang yang sah untuk mengakses sistem dan data sensitif.

Ancaman-ancaman ini memerlukan pendekatan yang holistik dalam pengelolaan keamanan dan privasi. **Kesadaran dan edukasi pengguna** sangat penting dalam meminimalkan ancaman privasi, seperti phishing. Di sisi lain, organisasi harus menerapkan kebijakan yang jelas mengenai penggunaan data pribadi, serta memanfaatkan teknologi yang dapat memonitor dan membatasi tracking berlebihan terhadap pengguna.

3.4.3 Kesulitan Implementasi Regulasi

Penerapan regulasi yang ketat terkait privasi dan perlindungan data, seperti *General Data Protection Regulation* (GDPR) di *Uni Eropa atau California Consumer Privacy Act* (CCPA) di Amerika Serikat, menambah kompleksitas dalam manajemen keamanan siber dan privasi. Regulasi-regulasi tersebut mengharuskan perusahaan untuk mematuhi standar tertentu dalam mengelola data pribadi, dengan sanksi yang berat bagi yang melanggar. Namun, mengimplementasikan regulasi ini tidaklah mudah. Beberapa kesulitan yang sering dihadapi adalah:

1. **Kesesuaian Internasional**: Banyak perusahaan global harus menghadapi tantangan dalam menyesuaikan operasional mereka dengan berbagai regulasi di berbagai yurisdiksi. Setiap negara atau wilayah sering kali memiliki aturan yang berbeda terkait privasi dan perlindungan data, yang dapat menimbulkan ketidakpastian hukum bagi organisasi yang beroperasi di lebih dari satu negara.
2. **Biaya dan Sumber Daya**: Mematuhi regulasi privasi dan keamanan data sering kali memerlukan investasi yang besar, baik dari segi teknologi, pelatihan, maupun tenaga kerja. Perusahaan harus mengalokasikan sumber daya untuk memastikan bahwa sistem mereka mematuhi regulasi yang berlaku, seperti melindungi data pribadi dengan enkripsi atau memastikan kepatuhan dengan permintaan penghapusan data dari subjek.
3. **Kompleksitas Teknologi**: Seiring dengan perkembangan teknologi, seperti **cloud computing**, **Internet of Things (IoT)**, dan **big data**, regulasi terkait privasi dan keamanan semakin sulit diimplementasikan. Teknologi baru ini sering kali

melibatkan aliran data yang besar dan tersebar di berbagai lokasi, sehingga organisasi kesulitan dalam melacak dan mengelola kepatuhan terhadap peraturan yang berlaku.

4. **Kesadaran Hukum yang Minim**: Banyak organisasi, terutama di negara-negara berkembang, masih minim dalam pemahaman tentang regulasi privasi dan kepatuhan yang berlaku. Ini membuat penerapan aturan menjadi lebih sulit, karena perusahaan tidak sepenuhnya memahami implikasi hukum dari penyalahgunaan atau kebocoran data.

Untuk mengatasi tantangan ini, organisasi harus proaktif dalam membangun tata kelola data yang kuat, memanfaatkan alat-alat otomatisasi untuk memantau kepatuhan, serta melibatkan ahli hukum dan profesional TI yang memahami regulasi yang relevan.

3.6 Proses Manajemen Privasi dan Kepatuhan Regulasi

Manajemen privasi dan kepatuhan regulasi adalah upaya sistematis yang dilakukan oleh organisasi untuk memastikan bahwa data pribadi dan informasi sensitif terlindungi, serta aktivitas operasionalnya sesuai dengan hukum dan regulasi yang berlaku. Proses ini melibatkan beberapa langkah penting yang saling berhubungan, mulai dari penilaian risiko hingga penanganan insiden. Berikut ini adalah uraian detail mengenai proses-proses kunci dalam manajemen privasi dan kepatuhan regulasi.

3.6.1 Penilaian Risiko Privasi (*Privacy Risk Assessment*)

Penilaian risiko privasi merupakan langkah awal dan paling penting dalam proses manajemen privasi. Tujuannya adalah untuk mengidentifikasi dan menganalisis potensi risiko terhadap data pribadi yang dikelola oleh organisasi. Dengan memahami risiko-risiko tersebut, organisasi dapat mengembangkan kebijakan dan langkah-langkah perlindungan yang lebih efektif. Tahapan dalam Penilaian Risiko Privasi:

1. **Identifikasi Data Pribadi yang Dikelola**: Langkah pertama adalah mengidentifikasi jenis-jenis data pribadi yang disimpan, diproses, atau ditransfer oleh organisasi. Data ini bisa berupa

informasi pelanggan, karyawan, atau mitra bisnis yang mencakup nama, alamat, nomor telepon, data keuangan, dan sebagainya.

2. **Identifikasi Potensi Ancaman dan Kerentanan**: Setelah data teridentifikasi, organisasi harus mengevaluasi potensi ancaman terhadap data tersebut. Ancaman bisa datang dari serangan siber, pelanggaran data internal, atau bahkan kesalahan manusia. Selain itu, organisasi juga perlu menganalisis kerentanan sistem yang memungkinkan ancaman tersebut terjadi, seperti perangkat lunak yang belum di-update atau sistem yang tidak dilindungi dengan baik.
3. **Evaluasi Dampak dan Probabilitas**: Organisasi kemudian mengevaluasi seberapa besar dampak yang mungkin timbul jika risiko privasi tersebut terjadi, serta seberapa besar kemungkinan risiko tersebut akan terjadi. Dampak bisa berkaitan dengan kerugian finansial, kerusakan reputasi, atau hukuman hukum.
4. **Penentuan Rencana Mitigasi**: Berdasarkan hasil analisis risiko, organisasi dapat menyusun rencana mitigasi, yaitu langkah-langkah untuk mengurangi atau mengelola risiko yang telah teridentifikasi. Misalnya, dengan meningkatkan keamanan sistem, membatasi akses ke data pribadi, atau memberikan pelatihan kepada karyawan tentang pentingnya keamanan data.

Penilaian risiko privasi perlu dilakukan secara berkala untuk menyesuaikan dengan perubahan teknologi, bisnis, dan regulasi yang berlaku.

3.6.2 Kebijakan Privasi dan Keamanan

Kebijakan privasi dan keamanan adalah pedoman formal yang ditetapkan oleh organisasi untuk mengatur bagaimana data pribadi dikumpulkan, disimpan, diproses, dan dilindungi. Kebijakan ini tidak hanya mencerminkan komitmen organisasi terhadap perlindungan data, tetapi juga merupakan cara untuk memastikan bahwa organisasi mematuhi peraturan yang berlaku, seperti General Data Protection Regulation (GDPR) atau *California*

Consumer Privacy Act (CCPA). Elemen Penting dalam Kebijakan Privasi dan Keamanan(Hermansyah et al., 2024):

1. **Pengumpulan dan Penggunaan Data**: Kebijakan ini harus menjelaskan secara rinci bagaimana data pribadi dikumpulkan dan untuk tujuan apa data tersebut digunakan. Pengguna atau subjek data harus diberi informasi yang jelas mengenai hak mereka untuk mengetahui bagaimana data mereka diproses dan, jika diinginkan, meminta penghapusan atau perubahan data tersebut.
2. **Perlindungan Data**: Organisasi harus mencantumkan langkah-langkah teknis dan administratif yang diterapkan untuk melindungi data pribadi dari akses yang tidak sah, kebocoran, atau penyalahgunaan. Ini bisa mencakup enkripsi, firewall, dan langkah-langkah pengamanan lainnya.
3. **Hak Subjek Data**: Kebijakan harus memastikan bahwa hak-hak subjek data diakui dan dipenuhi, termasuk hak untuk mengakses data, mengajukan keluhan, dan menuntut penghapusan data jika diinginkan.
4. **Transparansi dan Kepatuhan**: Kebijakan privasi juga harus memastikan transparansi dalam hal bagaimana organisasi mematuhi regulasi terkait privasi, termasuk pemberian notifikasi jika terjadi pelanggaran data.

Kebijakan privasi dan keamanan perlu dikomunikasikan dengan jelas kepada karyawan dan publik, dan diperbarui sesuai dengan perubahan regulasi atau kondisi organisasi.

3.6.3 Audit Kepatuhan Regulasi

Audit kepatuhan regulasi adalah proses evaluasi yang dilakukan secara berkala untuk memastikan bahwa kebijakan dan praktik manajemen data organisasi mematuhi peraturan yang berlaku. Audit ini bisa dilakukan secara internal oleh tim keamanan organisasi, atau eksternal oleh auditor independen. Langkah-langkah dalam Audit Kepatuhan Regulasi:

1. **Persiapan Audit**: Pada tahap ini, auditor akan mengumpulkan dokumen-dokumen terkait, seperti kebijakan privasi, catatan penilaian risiko, dan bukti tindakan perlindungan data yang telah diimplementasikan. Auditor juga akan meninjau regulasi yang berlaku untuk memastikan standar yang akan digunakan dalam evaluasi.
2. **Peninjauan Proses dan Sistem**: Auditor akan meninjau sistem dan proses yang ada untuk memastikan bahwa data pribadi dilindungi sesuai dengan kebijakan yang ditetapkan. Ini mencakup evaluasi infrastruktur IT, perangkat lunak, dan protokol keamanan yang diterapkan.
3. **Identifikasi Pelanggaran atau Ketidaksesuaian**: Jika ditemukan pelanggaran atau ketidaksesuaian dengan regulasi, auditor akan mencatatnya dan memberikan rekomendasi perbaikan. Contohnya, jika sebuah perusahaan gagal menyediakan mekanisme bagi pengguna untuk mengakses atau menghapus data pribadi mereka, ini bisa dianggap sebagai pelanggaran yang memerlukan tindakan segera.
4. **Laporan dan Tindak Lanjut**: Setelah audit selesai, auditor akan menyusun laporan yang merinci temuan, pelanggaran, dan rekomendasi perbaikan. Organisasi harus menindaklanjuti laporan tersebut dengan memperbaiki ketidaksesuaian yang ditemukan dan memastikan bahwa mereka tetap mematuhi regulasi yang berlaku.

Audit kepatuhan sangat penting karena membantu organisasi mengidentifikasi dan mengatasi kelemahan sebelum terjadi insiden serius, seperti kebocoran data atau denda dari pihak regulator.

3.6.4 Penanganan Insiden Pelanggaran Privasi

Meskipun organisasi telah menerapkan berbagai tindakan perlindungan, insiden pelanggaran privasi bisa tetap terjadi. Oleh karena itu, memiliki rencana penanganan insiden pelanggaran privasi yang baik sangat penting untuk meminimalkan dampak dari insiden tersebut dan memastikan bahwa organisasi dapat

merespons dengan cepat dan efektif. Langkah-langkah Penanganan Insiden Pelanggaran Privasi:

1. **Identifikasi dan Evaluasi Insiden**: Langkah pertama adalah mengidentifikasi apakah pelanggaran privasi telah terjadi, jenis data yang terlibat, serta skala dan dampaknya. Ini bisa mencakup pelanggaran teknis (seperti serangan siber) atau kebocoran data akibat kesalahan manusia.
2. **Pelaporan Insiden**: Regulasi seperti GDPR mengharuskan organisasi untuk melaporkan insiden pelanggaran data kepada otoritas pengawas dalam waktu tertentu (biasanya 72 jam setelah ditemukan). Selain itu, jika pelanggaran data memengaruhi individu, mereka juga harus diberitahukan.
3. **Tindakan Perbaikan**: Setelah insiden diidentifikasi, organisasi harus segera melakukan tindakan untuk memitigasi dampaknya, seperti memperbaiki celah keamanan, menonaktifkan akses yang tidak sah, atau memulihkan data yang hilang. Selain itu, jika pelanggaran terjadi karena kesalahan karyawan, pelatihan tambahan mungkin diperlukan.
4. **Evaluasi Pasca-Insiden**: Setelah insiden ditangani, penting untuk melakukan evaluasi menyeluruh untuk memahami penyebab utama insiden tersebut dan memastikan tindakan pencegahan yang lebih kuat diterapkan di masa mendatang.

Organisasi juga perlu menyusun rencana respon insiden (*incident response plan*) yang jelas dan mudah diikuti, agar seluruh tim dapat merespons insiden pelanggaran privasi dengan cepat dan tepat.

3.7 Teknologi untuk Mendukung Privasi dan Kepatuhan Regulasi

Dalam era digital, teknologi menjadi pilar utama dalam mendukung upaya perlindungan privasi dan kepatuhan terhadap regulasi. Organisasi membutuhkan solusi teknologi yang dapat melindungi data pribadi, memastikan bahwa akses ke informasi sensitif dibatasi, dan menyediakan mekanisme untuk memantau serta melaporkan kepatuhan terhadap regulasi. Dalam bagian ini, kita akan menguraikan tiga teknologi kunci yang digunakan untuk

mendukung privasi dan kepatuhan regulasi: enkripsi dan keamanan data, *Identity and Access Management* (IAM), serta pemantauan dan pelaporan kepatuhan.

3.7.1 Enkripsi dan Keamanan Data

Enkripsi adalah salah satu metode paling efektif untuk melindungi data pribadi dan sensitif. Enkripsi bekerja dengan mengubah data menjadi kode yang tidak dapat dibaca tanpa kunci khusus. Hal ini memastikan bahwa jika data dicuri atau disadap, informasi tersebut tidak akan bisa diakses oleh pihak yang tidak berwenang. Enkripsi telah menjadi bagian penting dari strategi keamanan informasi di berbagai organisasi, terutama yang menangani data sensitif seperti informasi keuangan, catatan medis, dan informasi pelanggan.

1. **Jenis-jenis Enkripsi:**
   a. **Enkripsi Simetris (*Symmetric Encryption*)**:
      Enkripsi simetris adalah metode enkripsi di mana data dienkripsi dan didekripsi menggunakan satu kunci yang sama. Ini adalah salah satu teknik enkripsi paling sederhana dan tercepat, yang telah digunakan selama bertahun-tahun untuk melindungi informasi sensitif. Dalam enkripsi simetris, baik pengirim maupun penerima informasi harus memiliki akses ke kunci yang sama untuk mengenkripsi dan mendekripsi pesan atau data. Proses ini memungkinkan data menjadi tidak terbaca oleh siapa pun yang tidak memiliki kunci tersebut. Sifat kesederhanaan ini membuat enkripsi simetris sangat efisien, terutama untuk pengolahan data dalam jumlah besar atau transfer data berkecepatan tinggi.
      1) **Cara Kerja Enkripsi Simetris**
         Proses enkripsi simetris mengikuti tiga langkah dasar:
         - **Pengguna mengidentifikasi kunci**: Sebelum data dapat dienkripsi, pengirim dan penerima harus berbagi kunci yang sama. Kunci ini adalah string karakter atau angka yang digunakan untuk

mengubah data asli menjadi format yang terenkripsi.

- **Proses enkripsi**: Data yang ingin dienkripsi, disebut sebagai teks terang (*plaintext*), dikombinasikan dengan kunci untuk menghasilkan teks terenkripsi (*ciphertext)*. Teks terenkripsi ini tampak acak dan tidak dapat dimengerti oleh orang yang tidak memiliki kunci.
- **Proses dekripsi**: Penerima menggunakan kunci yang sama untuk mendekripsi teks terenkripsi dan mengembalikannya menjadi teks terang yang dapat dibaca.

2) Contoh Algoritma Enkripsi Simetris

Ada beberapa algoritma enkripsi simetris yang umum digunakan, di antaranya:

- ***Data Encryption Standard* (DES)**: DES adalah salah satu algoritma enkripsi simetris pertama yang digunakan secara luas. DES menggunakan kunci sepanjang 56-bit, yang kini dianggap kurang aman karena rentan terhadap serangan brute force(T. Data & Standard, n.d.).
- ***Triple DES* (3DES)**: Triple DES adalah pengembangan dari DES, yang melakukan proses enkripsi sebanyak tiga kali untuk meningkatkan keamanannya. Meskipun lebih aman daripada DES, 3DES masih relatif lambat dan telah digantikan oleh algoritma yang lebih modern.
- ***Advanced Encryption Standard* (AES)**: AES adalah algoritma enkripsi simetris yang lebih aman dan efisien. AES mendukung kunci dengan panjang 128, 192, atau 256 bit, yang membuatnya sangat sulit untuk dipecahkan menggunakan serangan brute force. AES telah menjadi standar enkripsi yang banyak digunakan saat ini, terutama dalam komunikasi nirkabel dan transfer data yang

membutuhkan tingkat keamanan tinggi(Putra et al., 2021).

3) **Penggunaan Enkripsi Simetris dalam Kehidupan Sehari-hari**

Enkripsi simetribanyak digunakan dalam berbagai aplikasi dan teknologi, termasuk:

- **Jaringan Virtual Pribadi (VPN)**: VPN sering menggunakan enkripsi simetris untuk melindungi data pengguna yang dikirim melalui jaringan publik seperti internet.
- **Keamanan Wi-Fi**: Standar keamanan Wi-Fi, seperti WPA2, menggunakan enkripsi simetris untuk melindungi data yang ditransfer di antara perangkat dan router.
- **Proses transaksi perbankan online**: Banyak sistem perbankan menggunakan enkripsi simetris untuk memastikan bahwa informasi keuangan pribadi dan transaksi dilindungi saat berkomunikasi dengan server bank.

Enkripsi simetris adalah teknik enkripsi yang cepat, efisien, dan banyak digunakan dalam berbagai aplikasi. Meskipun menghadapi tantangan dalam distribusi kunci, algoritma seperti AES telah membuktikan kemampuannya untuk memberikan tingkat keamanan yang sangat tinggi. Namun, untuk jaringan yang besar atau publik, enkripsi simetris biasanya digabungkan dengan teknik enkripsi lainnya, seperti enkripsi asimetris, untuk mengatasi masalah distribusi kunci.

b. Enkripsi Asimetris (*Asymmetric Encryption*):

Enkripsi asimetris adalah metode enkripsi yang menggunakan dua kunci berbeda: **kunci publik** dan **kunci privat**. Kunci publik digunakan untuk mengenkripsi data, sementara kunci privat digunakan untuk mendekripsi data. Sistem ini berbeda dengan

enkripsi simetris yang hanya menggunakan satu kunci untuk enkripsi dan dekripsi. Enkripsi asimetris dianggap lebih aman dibandingkan dengan enkripsi simetris karena kunci publik dapat didistribusikan secara terbuka tanpa mengorbankan keamanan data, sementara kunci privat tetap dirahasiakan(Nabila Oper, Sabri Balafif, 2022).

1) Cara Kerja Enkripsi Asimetris

Proses enkripsi asimetris biasanya terdiri dari tiga langkah utama:

- **Generasi Kunci**: Setiap pengguna dalam sistem enkripsi asimetris menghasilkan sepasang kunci, yaitu kunci publik dan kunci privat. Kunci publik dapat dibagikan kepada siapa saja yang ingin mengirimkan data, sedangkan kunci privat disimpan dengan aman dan hanya diketahui oleh pemiliknya.
- **Proses Enkripsi**: Ketika seseorang ingin mengirim pesan atau data yang aman kepada penerima, mereka akan menggunakan kunci publik penerima untuk mengenkripsi data tersebut. Data yang sudah dienkripsi ini disebut sebagai *ciphertext*.
- **Proses Dekripsi**: Setelah pesan atau data yang terenkripsi diterima, penerima akan menggunakan kunci privat mereka untuk mendekripsi *ciphertext* dan mengubahnya kembali menjadi teks asli atau *plaintext* yang dapat dibaca.

Proses ini membuat enkripsi asimetris sangat aman karena meskipun kunci publik dapat diakses secara bebas, data hanya dapat didekripsi dengan kunci privat yang sesuai. Bahkan jika seseorang mendapatkan kunci publik, mereka tidak bisa mendekripsi data tanpa kunci privat.

2) Contoh Algoritma Enkripsi Asimetris

Ada beberapa algoritma enkripsi asimetris yang populer dan banyak digunakan di dunia modern, termasuk:

- **RSA (*Rivest-Shamir-Adleman*)**: RSA adalah salah satu algoritma enkripsi asimetris yang paling terkenal dan banyak digunakan. Algoritma ini berdasarkan pada kesulitan faktorisasi bilangan besar yang terdiri dari dua bilangan prima. RSA sering digunakan dalam komunikasi aman, seperti di dalam protokol HTTPS untuk melindungi transaksi online dan email terenkripsi (Internasional & Tangkere, 2023).
- ***Elliptic Curve Cryptography* (ECC)**: ECC menggunakan kurva elips untuk menghasilkan kunci enkripsi. ECC memiliki tingkat keamanan yang setara dengan RSA, tetapi dengan ukuran kunci yang lebih kecil, sehingga lebih efisien dalam penggunaan memori dan daya komputasi. ECC sering digunakan dalam perangkat dengan sumber daya terbatas, seperti perangkat mobile atau IoT (Internet of Things)(Yan, 2022).
- ***Diffie-Hellman***: Algoritma ini digunakan untuk pertukaran kunci secara aman di lingkungan publik, memungkinkan dua pihak untuk menghasilkan kunci simetris bersama melalui saluran komunikasi yang tidak aman. Meskipun Diffie-Hellman sendiri bukan algoritma enkripsi, ini sering digunakan bersama dengan enkripsi asimetris.

3) Penggunaan Enkripsi Asimetris dalam Kehidupan Sehari-hari

- **Sertifikat SSL/TLS**: Dalam komunikasi internet yang aman, enkripsi asimetris digunakan dalam **SSL/TLS** untuk melindungi data yang ditransmisikan antara pengguna dan server.

Sertifikat ini memastikan bahwa komunikasi, seperti transaksi online atau pengiriman data pribadi, terenkripsi dengan aman.

- **Email Aman**: Layanan email terenkripsi, seperti **PGP (*Pretty Good Privacy*)**, menggunakan enkripsi asimetris untuk melindungi isi pesan email dan memastikan bahwa hanya penerima yang dituju yang dapat membaca pesan tersebut.
- ***Cryptocurrency**:* Mata uang digital seperti **Bitcoin** dan **Ethereum** memanfaatkan enkripsi asimetris untuk memastikan keamanan transaksi, di mana setiap pengguna memiliki pasangan kunci publik dan kunci privat untuk menandatangani transaksi secara aman(Amsyar et al., 2020).

Tabel 3.2. Tabel Perbandingan Enkripsi Simetris dan Asimetris

Aspek	**Enkripsi Simetris**	**Enkripsi Asimetris**
Kecepatan	Lebih cepat	Lebih lambat karena perhitungan matematis yang kompleks
Distribusi Kunci	Memerlukan metode aman untuk berbagi kunci	Kunci publik dapat dibagikan secara bebas
Keamanan	Rentan jika kunci bocor	Lebih aman karena hanya kunci privat yang harus dijaga
Contoh Algoritma	AES, DES	RSA, ECC, Diffie-Hellman

Manfaat Enkripsi dalam Mendukung Kepatuhan Regulasi:

- Perlindungan Data Sensitif: Banyak regulasi privasi, seperti *General Data Protection Regulation* (GDPR) dan *Health Insurance Portability and Accountability Act* (HIPAA), mengharuskan organisasi untuk

melindungi data pribadi dengan enkripsi guna mencegah akses yang tidak sah.

- Mitigasi Risiko Kebocoran Data: Jika terjadi pelanggaran data, data yang telah dienkripsi secara kuat akan sulit untuk diakses oleh penjahat siber, sehingga dampak kebocoran bisa diminimalisir.
- Kepatuhan terhadap Regulasi: Enkripsi merupakan cara yang diakui secara global untuk memenuhi persyaratan regulasi terkait perlindungan data pribadi. Dengan menggunakan enkripsi, organisasi dapat membuktikan bahwa mereka telah mengambil langkah-langkah teknis yang memadai untuk melindungi data sensitif.

2. *Identity and Access Management* (IAM)

Identity and Access Management (IAM) adalah teknologi yang digunakan untuk mengelola dan mengontrol akses pengguna terhadap sistem, aplikasi, dan data. IAM memastikan bahwa hanya individu yang memiliki izin tertentu yang dapat mengakses informasi sensitif, dan memberikan mekanisme untuk memonitor serta mengatur siapa yang dapat melakukan apa dalam system. Komponen Utama IAM(Alsirhani et al., 2022):

a. Autentikasi: Autentikasi adalah proses verifikasi identitas pengguna sebelum mereka diizinkan untuk mengakses sistem atau data. Ini bisa berupa password, biometrik (sidik jari atau pengenalan wajah), atau autentikasi dua faktor (two-factor authentication, 2FA).
b. Otorisasi: Setelah pengguna berhasil diautentikasi, otorisasi menentukan apa yang diizinkan dilakukan oleh pengguna tersebut. Ini mencakup pembatasan akses berdasarkan peran (role-based access control, RBAC), di mana pengguna hanya dapat mengakses data yang relevan dengan tugas mereka.
c. Manajemen Identitas: IAM juga mencakup pencatatan dan pengelolaan informasi identitas pengguna, seperti kapan dan bagaimana mereka mengakses sistem. Hal ini

penting untuk pemantauan keamanan dan audit kepatuhan.

Manfaat IAM dalam Mendukung Kepatuhan Regulasi:

a. Pengendalian Akses yang Ketat: Dengan IAM, organisasi dapat memastikan bahwa hanya pengguna yang sah dengan otorisasi yang sesuai yang dapat mengakses data sensitif. Ini membantu mencegah pelanggaran internal dan eksternal yang dapat melanggar regulasi privasi.
b. Audit dan Pemantauan: IAM memungkinkan organisasi untuk melacak siapa yang mengakses data, kapan, dan untuk tujuan apa. Informasi ini penting untuk audit kepatuhan regulasi serta investigasi insiden keamanan.
c. Pengurangan Risiko Pelanggaran Privasi: Dengan pembatasan akses yang jelas dan pengelolaan identitas yang baik, risiko pelanggaran privasi dapat diminimalisir karena akses data hanya diberikan kepada individu yang benar-benar membutuhkannya.

3. Pemantauan dan Pelaporan Kepatuhan

Pemantauan dan pelaporan kepatuhan adalah aspek penting dari manajemen privasi dan keamanan data. Teknologi pemantauan memungkinkan organisasi untuk terus memeriksa apakah praktik mereka sejalan dengan regulasi yang berlaku dan memberikan laporan yang dapat diaudit oleh otoritas terkait. Komponen Pemantauan dan Pelaporan Kepatuhan:

a. Pemantauan *Real-Time*: Teknologi pemantauan *real-time* memungkinkan organisasi untuk mendeteksi anomali atau aktivitas mencurigakan yang dapat menandakan potensi pelanggaran privasi. Misalnya, jika terjadi upaya akses yang tidak sah atau volume data yang tidak biasa diunduh, sistem akan memberikan peringatan.
b. Pelaporan Otomatis: Alat pelaporan otomatis dapat menghasilkan laporan kepatuhan secara berkala

berdasarkan data yang dikumpulkan dari pemantauan. Laporan ini dapat mencakup informasi tentang akses pengguna, enkripsi data, serta insiden yang terjadi, dan dapat digunakan untuk audit atau pemeriksaan oleh regulator.

c. Analisis Keamanan: Pemantauan yang efektif mencakup analisis data untuk menemukan pola-pola tertentu yang mungkin menunjukkan adanya ancaman. Misalnya, peningkatan tiba-tiba dalam upaya autentikasi yang gagal mungkin menunjukkan adanya serangan brute force terhadap sistem.

Manfaat Pemantauan dan Pelaporan dalam Mendukung Kepatuhan Regulasi:

a. Kepatuhan Berkelanjutan: Regulasi seperti GDPR atau CCPA mengharuskan organisasi untuk memantau secara terus menerus aktivitas yang melibatkan data pribadi. Dengan teknologi pemantauan, organisasi dapat memastikan bahwa mereka selalu mematuhi regulasi dan mendeteksi pelanggaran secara proaktif.
b. Transparansi dan Akuntabilitas: Laporan kepatuhan memberikan transparansi dalam pengelolaan data, sehingga organisasi dapat dengan mudah menunjukkan kepada regulator bahwa mereka mematuhi aturan yang berlaku. Ini juga memungkinkan akuntabilitas dalam kasus pelanggaran, di mana penyebab dapat dilacak dengan cepat.
c. Respon Cepat terhadap Insiden: Dengan pemantauan real-time, organisasi dapat mendeteksi dan merespons insiden pelanggaran data dengan lebih cepat, mengurangi dampak dan risiko hukum.

DAFTAR PUSTAKA

Alsirhani, A., Ezz, M., & Mostafa, A. M. (2022). *Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing*. https://doi.org/10.32604/csse.2022.024854

Amsyar, I., Christopher, E., Dithi, A., Khan, A. N., & Maulana, S. (2020). *The Challenge of Cryptocurrency in the Era of the Digital Revolution : A Review of Systematic Literature*. *2*(2), 153–159.

Carmi, L., Zohar, M., & Riva, G. M. (2023). *The European General Data Protection Regulation (GDPR) in mHealth : Theoretical and practical aspects for practitioners ' use*. https://doi.org/10.1177/00258024221118411

Data, G., & Regulation, P. (2024). *General data protection regulation*. *4*(4).

Data, T., & Standard, E. (n.d.). *The Data Encryption Standard (DES) and Alternatives*. 73–74.

Ehimuan, B., Chimezie, O., Akagha, O. V., Reis, O., & Oguejiofor, B. (2024). *Global data privacy laws : A critical review of technology ' s impact on user rights*.

Fauzi, A., Putri, A. M., Fitriyani, F., & Astriyani, R. (2024). *Tinjauan Ancaman dan Risiko pada Sistem Keamanan Internet of Things , Berbasis Cloud Computing dalam Penggunaan E-Commerce dan Rencana Strategis*. *2*(2), 126–137.

Golden, D., & Extortion, T. (n.d.). *The Colonial Pipeline Ransomware Hackers Had a Secret Weapon : Self-Promoting Cybersecurity Firms*. 1–18.

Governance, C. S., Diplomacy, I. C., & Agency, E. (2019). *Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara*. *10*(2), 113–128.

Hanifa Salsabila, I. P. N. (2024). Analisis Dampak Regulasi Privasi Data Terhadap Manajemen Kemanan Data Di Sektor Bisnis Hanifa. *Https://Ejournal.Warunayama.Org/Kohesi Kohesi:*, *3*(10).

Hermansyah, D., Astini, B. I., & Mataram, U. M. (2024). *Penerapan Strategi Pemasaran Digital dalam Meningkatkan Visibilitas dan Pertumbuhan Bisnis di Era Digital*. *3*, 31–48.

Informatika, T., Komputer, F., & Universal, U. (2023). *Analisis Ancaman Keamanan Data Dalam Cloud Computing*. 1–5.

Internasional, H. P., & Tangkere, I. A. (2023). *Tanggung Jawab Negara Dalam Perlindungan E-Commerce Menurut Hukum Perdagang Internasional*. *5*, 3–10.

Kubben, P. (n.d.). *Fundamentals of Clinical Data Science*.

Manajemen, P. S., Ekonomi, F., Bisnis, D., & Negeri, U. I. (2024). *Pentingnya Kepatuhan Keamanan Informasi Dalam Mengurangi Risiko Data Breach Ripa Sabila Usni Sitompul Muhammad Irwan Padli Nasution*. *2*(1).

Margaretha Peggy Pomantow, 2Rokhmat, 3Anis Retnowati. (2023). Perlindungan Hukum Kepada Klinik Dan Dokter Terhadap Informasi Data Pasien Yang Tidak Lengkap. *Jurnal Cahaya Mandalika*, 644–657.

Nabila Oper, Sabri Balafif, T. F. A.-K. . (2022). *Modifikasi Algoritma Kriptografi Caesar Cipher Menjadi Algoritma Kriptografi Asimetris Dengan Metode Agile*. *4*(3), 179–184.

Niffari, H. (2020). *Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)*. *7*(1), 105–119.

Oakley, B. A. (2023). *What Really Is the Heath Insurance Portability*. *6*, 306–318. https://doi.org/10.1089/blr.2023.29329.aso

Putra, Y., Yuhandri, Y., & Sumijan, S. (2021). Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting. *Jurnal Sistim Informasi Dan Teknologi*, *3*, 56–63. https://doi.org/10.37034/jsisfotek.v3i2.44

Rawat, D. B. (2021). *Journal of Cybersecurity and Privacy : A New Open Access Journal*. 195–198.

Rima, K., Suari, A., & Sarjana, I. M. (2023). *Menjaga Privasi di Era Digital : Perlindungan Data Pribadi di Indonesia*. *1*, 132–146. https://doi.org/10.38043/jah.v6i1.4484

Romansky, R. (2022). *Available at Amazon*. *August*.

Saputra, D. F. (2023). *Literasi digital untuk perlindungan data pribadi 1*. *17*, 1–8.

Saputra, H. (2024). *Keamanan Cyber Di Era Web : Tantangan Dan Solusi*. *4*(4), 1–19.

Satria, M. K., & Yusuf, H. (2024). *Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Legal Analysis of Doxing Criminal Actions Reviewed Based on Law Number 27 of 2022 Concerning Personal Data Protection*. 2442–2456.

Sautunnida, L., Jurnal, K., & Hukum, I. (2018). *Perlindungan Data*. *20*(2), 369–384.

Selatan, J. R. (2019). *The Role of Religiosity , Halal Awareness , Halal Certification , and Food Ingredients on Sistem Purchase Integrasi Proteksi & of Manajemen Resiko Intention Halal Food Platform Fintech peer to peer (P2P) Lending dan Payment Gateway untuk * Meningkatkan Akselerasi Pertumbuhan Sistem Integrasi Proteksi & Manajemen Resiko Payment Gateway untuk Meningkatkan Akselerasi*. *0274*.

Siber, B., & Sandi, D. A. N. (2022). *Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui*. *7*(2), 295–316.

Sudarmadi, D. A., Indonesia, U., Josias, A., & Runturambi, S. (2019). *Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia*. *2*(2). https://doi.org/10.7454/jkskn.v2i2.10028

Sulistianingsih, D., Ihwan, M., & Setiawan, A. (2023). *Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi)*. *52*, 97–106.

Sutra, S. M., & Haryanto, A. (2023). *Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020*. *7*(April), 56–69. https://doi.org/10.34010/gpsjournal.v7i1

Wong, R. Y. (2023). *Privacy Legislation as Business Risks : How GDPR and CCPA are Represented in Technology Companies ' Investment Risk Disclosures*. *7*(April), 1–26. https://doi.org/10.1145/3579515

Yan, Y. (2022). *The Overview of Elliptic Curve Cryptography (ECC) The Overview of Elliptic Curve Cryptography (ECC)*.

https://doi.org/10.1088/1742-6596/2386/1/012019
Ziqra, Y., Siregar, M., & Leviza, J. (2021). *ISSN ONLINE : 2745-8369 Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online*. *2*, 330–336.

BAB 4
TANTANGAN TERKINI DALAM KEAMANAN INFORMASI

Oleh Addin Aditya

4.1 Pendahuluan

4.1.1 Konteks dan Pentingnya Keamanan Informasi

Di era digital saat ini, keamanan informasi telah menjadi pilar penting bagi semua jenis organisasi, mulai dari bisnis korporat hingga lembaga pemerintahan. Perkembangan teknologi tidak hanya membawa kemudahan dan efisiensi, tetapi juga risiko dan ancaman yang terus berkembang. Informasi, sebagai aset berharga, terus menerus diincar oleh pelaku kejahatan siber yang memiliki motif dan metode yang semakin canggih. Kehilangan, pencurian, atau kerusakan informasi dapat mengakibatkan kerugian finansial yang besar, kerusakan reputasi, serta gangguan operasional. Dengan demikian, memahami dan mengimplementasikan praktik keamanan informasi yang efektif menjadi esensial untuk melindungi aset dan memastikan kelangsungan operasi.

Keamanan informasi telah menjadi perhatian sejak manusia mulai menyimpan dan berbagi data penting. Sejak awal, upaya untuk menjaga kerahasiaan dan integritas informasi terus berkembang. Dalam dunia modern, perkembangan ini terjadi seiring dengan munculnya komputer, internet, dan sistem digital lainnya.

1. Era pre-Digital (sebelum 1970)
   Sebelum munculnya komputer, upaya keamanan informasi terbatas pada bentuk fisik, seperti menjaga dokumen penting dari pencurian, pemalsuan, atau kerusakan. Salah satu bentuk tertua adalah kriptografi, teknik penyandian pesan untuk melindungi informasi sensitif.
2. Era komputer (awal 1970)

Dengan perkembangan teknologi komputer, tantangan baru muncul dalam hal menjaga data digital. Pada periode ini, banyak organisasi mulai menggunakan komputer untuk memproses dan menyimpan informasi penting.

3. Era Internet (awal 1990)
   Munculnya internet secara signifikan mengubah lanskap keamanan informasi. Internet menghubungkan sistem di seluruh dunia, yang membuat data lebih rentan terhadap serangan jarak jauh. Serangan *Denial of Service* (DoS) pertama kali muncul pada pertengahan 1990-an (Haniyah et al., 2024), dan fenomena malware mulai merebak dengan lebih luas.
4. Era Mobile dan Cloud (2000-an sampai sekarang)
   Kemunculan perangkat mobile, *cloud computing*, dan *Internet of Things* (IoT) membawa tantangan baru. Data sekarang tersebar di banyak platform, dan keamanan tidak lagi hanya berfokus pada komputer pribadi atau server, tetapi juga perangkat mobile, aplikasi cloud, dan jaringan sensor yang saling terhubung. Di era ini, ancaman Ransomware, phishing, dan serangan *Distributed Denial of Service* (DDoS) menjadi lebih umum dan merugikan banyak pihak.

4.1.2 Tujuan dan Ruang Lingkup Bab

Bab ini dirancang untuk memberikan pemahaman mendalam tentang tantangan keamanan informasi yang dihadapi organisasi saat ini. Tujuannya adalah untuk mengeksplorasi berbagai ancaman keamanan yang terus berkembang, kerentanan sistem yang sering diabaikan, dan strategi mitigasi yang dapat diadopsi untuk melindungi informasi. Selain itu, bab ini juga akan membahas tentang regulasi terkini yang mempengaruhi keamanan informasi dan bagaimana organisasi dapat mematuhi ketentuan tersebut sambil meningkatkan postur keamanan mereka. Dengan menyajikan informasi ini, bab ini bertujuan untuk memberikan wawasan, alat, dan teknik yang dibutuhkan oleh profesional keamanan untuk menghadapi tantangan ini dan mempersiapkan untuk masa depan keamanan siber.

4.2 Ancaman Siber Kontemporer

4.2.1 Ransomware dan Serangan Pemerasan

Ransomware adalah salah satu ancaman siber paling signifikan dalam beberapa tahun terakhir (Alwashali et al., 2021). Serangan ransomware bekerja dengan mengenkripsi data korban, kemudian meminta tebusan untuk mendapatkan kembali akses ke data tersebut. Evolusi ransomware saat ini menunjukkan bahwa serangan ini semakin terstruktur, sering kali disertai dengan *Ransomware-as-a-Service* (RaaS), di mana kelompok kriminal menawarkan layanan kepada peretas yang tidak memiliki keterampilan teknis tinggi.

4.2.2 Phising dan Social Engineering

Phishing telah berkembang dari serangan email sederhana menjadi metode manipulasi yang sangat canggih (Aleroud & Zhou, 2017; Dhamija et al., 2006). Spear phishing adalah versi phishing yang lebih ditargetkan, di mana penyerang menggunakan informasi spesifik untuk menipu korban tertentu. Kampanye phishing dapat disebarkan melalui berbagai saluran, termasuk email, media sosial, atau aplikasi komunikasi.

Social engineering adalah teknik yang digunakan oleh penyerang untuk memanipulasi individu atau organisasi agar memberikan informasi sensitif atau melakukan tindakan tertentu yang menguntungkan penyerang (Salahdine & Kaabouch, 2019). Teknik ini sering kali memanfaatkan kepercayaan manusia dan interaksi sosial untuk mengecoh korban, sehingga mereka tidak menyadari bahwa mereka sedang dieksploitasi. Berikut adalah beberapa konsep mengenai social engineering :

1. Manipulasi psikologis
   Penyerang menggunakan teknik manipulasi psikologis untuk mempengaruhi keputusan dan perilaku korban. Mereka sering kali memanfaatkan emosi, seperti rasa takut, urgensi, atau keinginan untuk membantu, untuk mendorong korban agar memberikan informasi yang diinginkan.
2. Kepercayaan manusia
   Social engineering berakar pada sifat manusia yang cenderung mempercayai orang lain. Penyerang sering kali

berpura-pura menjadi pihak yang sah, seperti rekan kerja, penyedia layanan, atau institusi keuangan, untuk membangun kepercayaan dan membuat korban merasa nyaman dalam memberikan informasi.

3. Interaksi sosial
   Teknik ini sering melibatkan interaksi langsung, baik secara tatap muka, melalui telepon, atau melalui media digital. Penyerang dapat menggunakan berbagai saluran komunikasi untuk menjangkau korban dan menciptakan situasi yang mendukung tujuan
4. Ketersembunyian
   Salah satu aspek penting dari social engineering adalah bahwa korban sering kali tidak menyadari bahwa mereka sedang dieksploitasi. Penyerang berusaha untuk menyembunyikan niat jahat mereka dan menciptakan narasi yang tampak sah untuk menutupi tindakan mereka.
5. Phising
   Beberapa contoh serangan social engineering termasuk phishing (mengirim email palsu untuk mendapatkan informasi), baiting (menawarkan sesuatu yang menarik untuk mendapatkan akses), dan pretexting (menciptakan skenario palsu untuk mendapatkan informasi).

Secara keseluruhan, social engineering merupakan ancaman serius dalam dunia keamanan siber karena ia mengeksploitasi kelemahan manusia, yang sering kali lebih rentan dibandingkan dengan sistem teknologi yang ada.

4.3 Keamanan Data dan Privasi

4.3.1 Perlindungan Data Pribadi di Era Big Data

Era Big Data telah membawa perubahan besar dalam cara organisasi mengumpulkan, menyimpan, dan memanfaatkan data. Data tidak lagi hanya dalam bentuk terstruktur seperti angka, tetapi juga termasuk informasi tidak terstruktur seperti data dari media sosial, email, rekaman suara, dan video. Penggunaan big data dalam skala besar ini telah menciptakan tantangan baru dalam melindungi privasi individu (Aditya, 2024). Dengan semakin banyaknya data

yang dikumpulkan dari berbagai sumber, melindungi informasi pribadi menjadi lebih rumit. Banyak organisasi mengumpulkan data dalam jumlah besar tanpa pemahaman yang cukup tentang bagaimana data tersebut harus dilindungi atau digunakan secara etis.

Pada saat ini banyak sekali kasus pelanggaran atas Perlindungan Data Pribadi yang terjadi di Indonesia, termasuk kasus besar yaitu kebocoran data kependudukan di BPJS yang jumlah data yang bocor mencapai diatas 270 juta data. Lemahnya pengaturan mengenai aspek hukum perlindungan data pribadi dan rendahnya budaya untuk pelaporan dari korban membuat pelanggaran atas perlindungan data pribadi Di Indonesia sangat tinggi (Sutrisna, 2021). Pada Mei 2020, platform e-commerce besar Indonesia, Tokopedia, mengalami kebocoran data besar-besaran yang mengungkapkan informasi pribadi dari sekitar 91 juta pengguna. Data yang bocor termasuk nama, email, tanggal lahir, dan hashed passwords. Peretas menawarkan data ini untuk dijual di dark web, yang memicu kekhawatiran terkait penyalahgunaan informasi. Kebocoran data ini menyoroti pentingnya keamanan siber di sektor e-commerce, terutama karena platform seperti Tokopedia menangani jutaan transaksi dan informasi sensitif setiap hari.

4.3.2 Peraturan Perlindungan Data

Peraturan perlindungan data di Indonesia saat ini diatur oleh Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada September 2022. UU PDP bertujuan untuk memberikan perlindungan hukum yang lebih kuat terhadap data pribadi masyarakat Indonesia, dengan mengadopsi banyak elemen dari *General Data Protection Regulation* (GDPR). Adapun GDPR adalah regulasi perlindungan data pribadi yang diterapkan di Uni Eropa (UE) sejak 25 Mei 2018 (Voigt & von dem Bussche, 2017). Sebelum UU PDP disahkan, regulasi tentang perlindungan data pribadi tersebar di berbagai peraturan sektor, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan lainnya.

Peraturan perlindungan data di Indonesia, terutama setelah pengesahan UU PDP, telah memberikan fondasi yang kuat untuk melindungi data pribadi masyarakat. Dengan adanya UU PDP, Indonesia memiliki kerangka hukum yang komprehensif yang mengatur pengumpulan, pengolahan, dan penyimpanan data pribadi, serta memberikan hak-hak yang lebih jelas kepada pemilik data. Namun, keberhasilan implementasi UU PDP akan sangat tergantung pada kesadaran masyarakat, kepatuhan organisasi, dan pengawasan yang efektif oleh lembaga terkait.

4.4 Perkembangan Teknologi Keamanan Informasi

4.4.1 Kecerdasan Buatan (AI) dalam Keamanan Siber

Kecerdasan buatan (AI) dan pembelajaran mesin (machine learning) telah menjadi pilar dalam mendeteksi dan merespons ancaman siber (Li, 2018). AI mampu menganalisis pola lalu lintas jaringan dan perilaku pengguna untuk mendeteksi anomali yang mungkin menunjukkan adanya serangan siber. Dengan memanfaatkan algoritma pembelajaran mesin, sistem keamanan dapat mengidentifikasi ancaman baru yang belum pernah ditemukan sebelumnya, serta bereaksi lebih cepat daripada yang dapat dilakukan manusia. Berikut adalah beberapa manfaat AI dalam keamanan siber :

1. Deteksi Anomali : Deteksi anomali berarti menggunakan berbagai teknik dan metode untuk mendeteksi pola yang berbeda yang tidak sesuai dengan fitur yang ditentukan dari keseluruhan data (Alabadi & Celik, 2020). AI membantu mengenali aktivitas tidak normal di dalam sistem, baik itu melalui lalu lintas jaringan, akses data, atau perilaku pengguna yang mencurigakan.
2. Respon otomatis dalam insiden : Beberapa sistem keamanan yang didukung AI dapat secara otomatis mengambil tindakan untuk menahan atau menghentikan serangan ketika ancaman terdeteksi, tanpa perlu intervensi manusia.
3. Keamanan prediktif : Dengan analisis data historis dan tren ancaman, AI mampu memberikan prediksi ancaman masa

depan dan memungkinkan organisasi untuk mempersiapkan langkah mitigasi.

4.4.2 *Blockchain* dan Keamanan Informasi

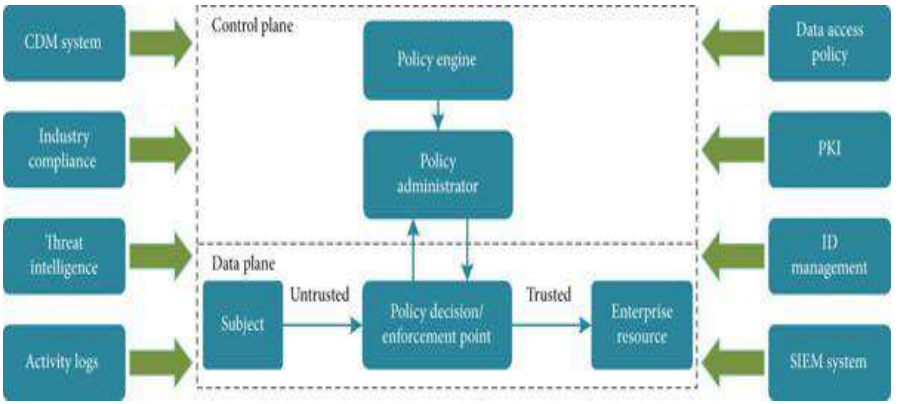
Blockchain adalah teknologi buku besar terdistribusi (*distributed ledger technology*) yang memungkinkan data untuk dicatat secara transparan, aman, dan tidak dapat diubah (Liu & Xu, 2018). Teknologi ini pertama kali diperkenalkan melalui mata uang kripto, Bitcoin, pada tahun 2008, tetapi sekarang telah berkembang ke berbagai aplikasi lain, termasuk di bidang keamanan informasi. Blockchain terdiri dari serangkaian blok, di mana setiap blok menyimpan informasi transaksi. Setiap blok dihubungkan ke blok sebelumnya, membentuk rantai yang tidak dapat diubah tanpa persetujuan jaringan. Berikut adalah beberapa prinsip dari teknologi blockchain :

1. Terdesentralisasi. Tidak ada otoritas pusat yang mengontrol jaringan. Setiap node dalam jaringan blockchain memiliki salinan lengkap dari buku besar, dan semua transaksi baru harus diverifikasi oleh konsensus dari node-node ini.
2. Ketidakberubahan. Setelah transaksi dimasukkan ke dalam blockchain dan divalidasi, transaksi tersebut tidak dapat diubah. Setiap perubahan akan segera terdeteksi oleh jaringan, karena perubahan tersebut harus disetujui oleh mayoritas node.
3. Keamanan kriptografi. Blockchain menggunakan algoritma kriptografi yang kuat untuk mengamankan data. Setiap blok memiliki hash kriptografis yang unik, dan setiap perubahan kecil dalam data akan mengubah hash tersebut secara signifikan, sehingga perubahan atau manipulasi data dapat segera dideteksi.

4.4.3 *Zero Trust Architecture*

Zero Trust Architecture (ZTA) adalah pendekatan keamanan siber yang didasarkan pada prinsip bahwa tidak ada entitas, baik internal maupun eksternal, yang dapat sepenuhnya dipercaya tanpa verifikasi yang ketat (Rose et al., 2020). Berbeda dengan model keamanan tradisional yang mengandalkan perimeter keamanan,

seperti firewall yang melindungi jaringan internal dari ancaman eksternal, ZTA mengasumsikan bahwa ancaman bisa datang dari mana saja, baik dari dalam maupun luar organisasi. Oleh karena itu, setiap akses harus divalidasi, baik untuk pengguna, perangkat, maupun aplikasi.



Gambar 4.1. Elemen ZTA (He et al., 2022)

Di antara komponen-komponen tersebut, sistem manajemen identitas (ID management) dan infrastruktur kunci publik perusahaan (PKI) terutama digunakan untuk autentikasi personel dan perangkat, yang menjadi dasar keamanan (He et al., 2022). Kebijakan akses data terutama menyediakan kebijakan akses sumber daya, dan sistem manajemen informasi keamanan serta peristiwa (sistem SIEM) menyediakan manajemen informasi keamanan dan peristiwa untuk seluruh arsitektur. Pada saat yang sama, untuk mengintegrasikan kemampuan seperti kebijakan kepatuhan industri dan deteksi ancaman, perhatian lebih perlu diberikan pada sistem diagnostik dan mitigasi berkelanjutan (CDM).
Secara umum, ZTA (*Zero Trust Architecture*) didasarkan pada identitas, memberikan identitas digital kepada orang dan perangkat, serta menetapkan izin minimum untuk subjek akses; bertujuan untuk keamanan bisnis, mewujudkan penyembunyian bisnis, enkripsi transmisi, dan kontrol yang cermat; dengan penilaian kepercayaan berkelanjutan sebagai jaminan, termasuk penilaian kepercayaan pengguna, penentuan risiko lingkungan, dan

penemuan perilaku yang tidak normal; menggunakan kontrol izin dinamis sebagai sarana, termasuk kontrol akses berbasis atribut, akses hierarkis berbasis tingkat kepercayaan, dan izin dinamis yang peka terhadap risiko.

Arsitektur zero trust berfokus pada kemampuan keamanan dalam dimensi identitas, kepercayaan, kontrol akses, izin, dan lainnya. Kemampuan keamanan ini juga merupakan bagian yang tak terpisahkan dari sistem bisnis berbasis informasi, sehingga zero trust secara inheren adalah bentuk "keamanan endogen." Dalam arti tertentu, ini merupakan peningkatan spiral antara bisnis dan keamanan. Dari sistem bisnis awal hingga pencapaian tujuan bisnis yang lengkap, perangkat keamanan mewujudkan sistem mandiri dari jaminan keamanan dan mengintegrasikan hubungan yang erat antara keamanan dan bisnis, lalu kembali lagi ke keamanan dan aplikasi.

4.4.4 *Cloud Security*

Cloud security atau keamanan cloud adalah serangkaian kebijakan, kontrol, teknologi, dan praktik yang dirancang untuk melindungi data, aplikasi, dan infrastruktur yang terkait dengan komputasi awan (*cloud computing*) (Annisa Wahdiniawati et al., 2023). Dengan semakin banyaknya organisasi yang memanfaatkan layanan cloud untuk menyimpan data dan menjalankan aplikasi, keamanan cloud menjadi prioritas utama untuk melindungi informasi sensitif dari ancaman siber, kehilangan data, serta pelanggaran keamanan lainnya (Singh & Chatterjee, 2017). Keamanan cloud adalah bidang yang kompleks dan terus berkembang seiring dengan peningkatan adopsi layanan cloud oleh organisasi di seluruh dunia. Tantangan seperti pengelolaan identitas, keamanan data, dan kepatuhan regulasi harus diatasi dengan menerapkan teknologi keamanan yang tepat, praktik terbaik, dan model tanggung jawab bersama. Dengan pendekatan yang tepat, layanan cloud dapat memberikan keuntungan dalam hal fleksibilitas dan skalabilitas tanpa mengorbankan keamanan.

4.5 Strategi Mitigasi dan Pertahanan

Dalam konteks keamanan informasi di era digitalisasi, strategi mitigasi dan pertahanan yang efektif harus mencakup pendekatan proaktif dan reaktif untuk menjaga keamanan data dan sistem. Pendekatan proaktif fokus pada pencegahan insiden keamanan sebelum terjadi. Ini melibatkan :

1. Melakukan audit keamanan dan penilaian risiko secara rutin untuk mengidentifikasi kerentanan dalam sistem dan aplikasi. Ini membantu organisasi memperbarui tindakan keamanannya berdasarkan ancaman terbaru dan kerentanan yang terdeteksi.
2. Mengadopsi teknologi keamanan terkini seperti firewall next-generation, sistem deteksi dan pencegahan intrusi (IDS/IPS), dan solusi enkripsi. AI dan machine learning dapat digunakan untuk mendeteksi pola yang tidak biasa yang mungkin menunjukkan upaya penyusupan.
3. Memberikan pelatihan kesadaran keamanan secara berkala kepada semua karyawan untuk mengenali taktik phishing, social engineering, dan ancaman lainnya. Karyawan yang terinformasi adalah garis pertahanan pertama yang kuat.
4. Mengembangkan kebijakan keamanan informasi yang ketat dan prosedur operasional yang mencakup keamanan data, akses terkontrol, dan protokol respon insiden.
5. Memastikan bahwa semua sistem operasi dan aplikasi tetap diperbarui dengan patch keamanan terbaru untuk mengurangi risiko eksploitasi melalui kerentanan yang diketahui.

Meskipun langkah-langkah proaktif penting, organisasi juga harus siap dengan strategi reaktif untuk menangani insiden setelah terjadi. Ini termasuk :

1. Mengembangkan rencana respon insiden yang terperinci yang mencakup identifikasi, investigasi, pemberantasan, pemulihan, dan pelaporan. Rencana harus menyertakan peran dan tanggung jawab yang jelas serta prosedur komunikasi selama insiden keamanan.

2. Memiliki kemampuan forensik digital untuk segera menelusuri sumber dan metode serangan setelah terdeteksi. Ini membantu dalam memahami bagaimana serangan itu berhasil dan bagaimana mencegah insiden serupa di masa depan.
3. Melakukan simulasi serangan dan latihan respon insiden secara berkala untuk memastikan bahwa tim siap dan proses bekerja seperti yang diharapkan. Latihan ini harus melibatkan semua tingkat organisasi.
4. Backup dan Pemulihan Data: Menjaga backup data yang aman dan terpisah secara regular. Rencana pemulihan bencana yang efektif dan teruji adalah kunci untuk meminimalkan downtime dan kerugian data dalam insiden keamanan.
5. Analisis Pasca Insiden: Setelah insiden teratasi, melakukan review komprehensif untuk menentukan penyebabnya, mengevaluasi respons yang diberikan, dan mengidentifikasi pelajaran yang bisa dipetik untuk memperkuat tindakan keamanan di masa depan.

Menggabungkan pendekatan proaktif dan reaktif dalam strategi keamanan informasi memberikan pertahanan berlapis yang lebih baik terhadap ancaman siber, memastikan bahwa organisasi tidak hanya siap mencegah serangan tetapi juga efektif dalam merespon insiden yang tidak dapat dihindari.

DAFTAR PUSTAKA

Aditya, A. (2024). UPAYA PREVENTIF CEGAH KEJAHATAN SIBER DAN PENYALAHGUNAAN TRANSAKSI ELEKTRONIK MELALUI SOSIALISASI UU ITE. *Jurnal AbdiMas Nusa Mandiri*, *6*(1), 22–27. https://doi.org/10.33480/abdimas.v6i1.5370

Alabadi, M., & Celik, Y. (2020). Anomaly Detection for Cyber-Security Based on Convolution Neural Network : A survey. *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 1–14. https://doi.org/10.1109/HORA49412.2020.9152899

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

Alwashali, A. A. M. A., Rahman, N. A. A., & Ismail, N. (2021). A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack. *2021 14th International Conference on Developments in ESystems Engineering (DeSE)*, 92–96. https://doi.org/10.1109/DeSE54285.2021.9719456

Annisa Wahdiniawati, S., Yanto Rukmana, A., Fajrillah, Setiady Pasaribu, J., Fauzan, R., Soetikno, Y. J. W., Aditya, A., & Harto, B. (2023). *ENTERPRISE INFORMATION SYSTEM* (1st ed.). PT. Global Eksekutif Teknologi. https://www.researchgate.net/publication/372658600

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 581–590. https://doi.org/10.1145/1124772.1124861

Haniyah, W., Hidayat, M. C., Putra, Z. F. I., Pertama, V. A., & Setiawan, A. (2024). Simulasi Serangan Denial of Service (DoS) menggunakan Hping3 melalui Kali Linux. *Journal of Internet and Software Engineering*, *1*(2), 8. https://doi.org/10.47134/pjise.v1i2.2654

He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communications and Mobile Computing*, *2022*, 1–13. https://doi.org/10.1155/2022/6476274

Li, J. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462–1474. https://doi.org/10.1631/FITEE.1800573

Liu, L., & Xu, B. (2018). Research on information security technology based on blockchain. *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, 380–384. https://doi.org/10.1109/ICCCBDA.2018.8386546

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. https://doi.org/10.6028/NIST.SP.800-207

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, *79*, 88–115. https://doi.org/10.1016/j.jnca.2016.11.027

Sutrisna, C. (2021). ASPEK HUKUM PERLINDUNGAN DATA PRIBADI DAN KONDISI DARURAT KEBOCORAN ATAS DATA PRIBADI DI INDONESIA. *Wacana Paramarta*, *20*(5), 1–10.

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR)*. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

BIODATA PENULIS

Deddy Rudhistiar, S.Kom., M.Cs.
Dosen Program Studi S1 Teknik Informatika
Fakultas Teknologi Industri Institut Teknologi Nasional Malang

Penulis lahir di Pasuruan tanggal 28 Desember 1989. Penulis adalah dosen tetap pada Program Studi S1 Teknik Informatika Fakultas Teknologi Industri Institut Teknologi Nasional Malang. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Ilmu Komputer. Penulis menekuni bidang Jaringan Komputer, Kemanan Jaringan, Kriptografi dan Teknologi yang berhubungan dengan Cloud Computing.

BIODATA PENULIS

Muhammad Irwan Syahib, S.T., M.Kom.

Penulis saat ini beraktifitas sebagai tenaga pengajar di Program Studi Sistem dan Teknologi Informasi Fakultas Teknik Universitas Muhammadiyah Kendari. Menyelesaikan pendidikan S1 di Jurusan Teknik Informatika Universitas Halu Oleo dan melanjutkan S2 di Jurusan Teknik Informatika Universitas Ahmad Dahlan Yogyakarta. Penulis juga menekuni bidang Jaringan komputer dan digital forensik dan sedang berfokus pada penelitian bidang forensik kejahatan mobile, system informasi dan jaringan komputer.

BIODATA PENULIS

Yendi Putra, S. Kom., M. Kom, MTA
Dosen Program Studi Manajemen Informatika
Fakultas Eknomi Universitas Mahaputra Muhammad Yamin

Penulis lahir di Salimpaung pada 3 Januari 1988 dan merupakan anak kedua dari tiga bersaudara. Saat ini, ia mengabdikan diri sebagai dosen tetap di Program Studi Manajemen Informatika di Fakultas Ekonomi, Universitas Mahaputra Muhammad Yamin. Perjalanan pendidikan Penulis dimulai pada tahun 2007, ketika meraih gelar D1 di LKP Palapa Komputer Batusangkar. kemudian melanjutkan studi S1 di STMIK Indonesia Padang, menyelesaikannya pada tahun 2010. Tak berhenti di situ, Penulis mengejar gelar Magister di Universitas Putra Indonesia (UPI YPTK-Padang) dan berhasil meraih gelar tersebut pada tahun 2018. Keamanan teknologi adalah passion utama Penulis. Selama menempuh studi S2, menulis tesis yang menarik tentang penggunaan Algoritma Advanced Encryption Standard (AES) untuk meningkatkan keamanan token sebuah website dari serangan Cross-Site Scripting (XSS). Dengan pemahaman mendalam tentang berbagai aspek keamanan, Penulis terus berusaha memperluas pengetahuannya di bidang ini.mDi luar dunia akademik, Penulis juga aktif berkompetisi dalam berbagai lomba komputer. Pada tahun 2022, meraih juara ketiga di Lomba Kompetensi Keterampilan Instruktur Nasional (KKIN) Wilayah Barat yang diadakan di Banda

Aceh. Kegiatan ini menunjukkan dedikasi dan keahlian Penulis dalam bidang teknologi. Sebagai seorang ayah dari dua anak—Ayumna yang berusia 4 tahun dan Ibrahim yang berusia 8 bulan—keluarga adalah sumber inspirasi dan dukungan terbesarnya dalam mengejar karir dan minat di dunia teknologi. Penulis adalah sosok yang penuh semangat, berdedikasi, dan selalu berusaha menjadi yang terbaik dalam bidang keamanan teknologi.

BIODATA PENULIS

Addin Aditya, S.Kom., M.Kom.
Dosen Program Studi Sistem Informasi
Sekolah Tinggi Informatika dan Komputer Indonesia Malang

Penulis lahir di Malang tanggal 2 Juni 1991. Penulis adalah dosen tetap pada Program Studi Sistem Informasi, Sekolah Tinggi Informatika & Komputer Indonesia (STIKI) Malang. Penulis Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika di STIKI Malang dan melanjutkan S2 pada Jurusan Sistem Informasi di Institut Teknologi Sepuluh Nopember. Penulis menekuni bidang Sistem Informasi Manajemen dan Rekayasa Perangkat Lunak. Adapun penulis dapat dihubungi melalui email di addin@stiki.ac.id