KEAMANAN SISTEM INFORMASI

Bahan Ajar untuk Program Studi D3-Manajemen Informatika

DOSEN PENGAMPU

Ir. H.A. Mooduto, M.Kom.

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI PADANG

TAHUN 2026

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT, Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, bahan ajar **"Keamanan Sistem Informasi"** ini dapat diselesaikan dengan baik. Bahan ajar ini disusun sebagai panduan utama dalam proses perkuliahan mata kuliah Keamanan Sistem Informasi (ISY3210) untuk mahasiswa Program Studi D3-Manajemen Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Padang.

Penyusunan bahan ajar ini didasarkan pada Rencana Pembelajaran Semester (RPS) yang telah dirancang secara sistematis untuk mencapai Capaian Pembelajaran Lulusan (CPL) yang telah ditetapkan. Materi dalam buku ini tidak hanya berfokus pada teori semata, tetapi juga mengintegrasikan studi kasus, analisis kebijakan, dan contoh-contoh nyata di industri, sehingga diharapkan mampu membangun kompetensi analitis mahasiswa sesuai dengan kerangka kualifikasi KKNI Level 5. Topik-topik krusial seperti prinsip CIA Triad, kriptografi, manajemen risiko, hingga aspek hukum seperti UU ITE dan UU Perlindungan Data Pribadi dibahas secara terstruktur untuk membekali mahasiswa menghadapi tantangan keamanan informasi di dunia kerja.

Penulis menyadari bahwa bahan ajar ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun dari rekan sejawat, mahasiswa, dan pembaca sangat diharapkan demi penyempurnaan di masa yang akan datang. Semoga bahan ajar ini dapat memberikan kontribusi nyata bagi peningkatan kualitas pembelajaran di lingkungan Program Studi D3-Manajemen Informatika Politeknik Negeri Padang.

Padang, Februari 2026

Dosen Pengampu,

Ir. H.A. Mooduto, M.Kom.

NIP. 196605101994031003

PETUNJUK PENGGUNAAN BAHAN AJAR

Bahan ajar ini dirancang untuk memudahkan mahasiswa dalam mempelajari mata kuliah Keamanan Sistem Informasi selama satu semester (16 pertemuan). Berikut adalah panduan penggunaan buku ini:

A. Target Pembelajaran

Setiap bab dalam buku ini diawali dengan **Kemampuan Akhir (Sub-CPMK)** yang harus dicapai oleh mahasiswa. Fokuskan pembelajaran pada target tersebut.

B. Struktur Bab

Setiap bab disusun dengan alur sebagai berikut:

1. **Judul Bab dan Sub-CPMK:** Menyatakan topik utama dan kemampuan spesifik yang akan dicapai.
2. **Penyajian Materi:** Uraian konsep, teori, dan teknologi yang relevan dengan topik.
3. **Studi Kasus/Contoh:** Aplikasi nyata dari konsep yang dipelajari untuk memperdalam pemahaman.
4. **Rangkuman:** Ringkasan poin-poin penting dari bab tersebut.
5. **Latihan Soal dan Tugas Mandiri:** Soal untuk menguji pemahaman individu dan tugas yang harus dikumpulkan sesuai jadwal perkuliahan.

C. Ikon-Ikon yang Digunakan

Untuk memudahkan navigasi, bahan ajar ini menggunakan ikon-ikon berikut:

- 🎯 **Kemampuan Akhir:** Menyatakan target yang harus dicapai setelah mempelajari bab.
- 📖 **Materi Inti:** Bagian utama yang berisi konsep dan penjelasan.
- 💡 **Studi Kasus:** Contoh aplikasi atau kejadian nyata yang relevan.
- ✍️ **Latihan:** Pertanyaan untuk menguji pemahaman.
- 📝 **Tugas Mandiri:** Kegiatan yang harus dikerjakan secara individu dan dinilai.
- 🗝️ **Rangkuman:** Kesimpulan dari seluruh materi bab.

D. Keterkaitan dengan RPS

Bahan ajar ini merupakan implementasi dari RPS mata kuliah Keamanan Sistem Informasi. Mahasiswa sangat disarankan untuk membaca RPS di awal semester agar memahami gambaran besar mata kuliah, sistem penilaian, dan aturan-aturan perkuliahan.

E. Strategi Belajar yang Disarankan

1. **Pra-Perkuliahan:** Bacalah sekilas materi bab yang akan dibahas.
2. **Saat Perkuliahan:** Ikuti diskusi dan catat poin-poin penting.
3. **Pasca-Perkuliahan:** Kerjakan latihan soal dan tugas mandiri untuk memantapkan pemahaman.
4. **Diskusi Kelompok:** Bentuklah kelompok belajar untuk mendiskusikan studi kasus yang kompleks.

DAFTAR ISI

Halaman

BAGIAN 1
FONDASI KEAMANAN INFORMASI

BAB 1
PRINSIP DASAR KEAMANAN INFORMASI (CIA TRIAD)

🎯 Kemampuan Akhir (Sub-CPMK 1.1)

Setelah mempelajari bab ini, mahasiswa mampu:

1. Menjelaskan definisi dan tujuan keamanan informasi.
2. Menganalisis prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dalam berbagai konteks organisasi.
3. Mengidentifikasi pelanggaran CIA Triad dalam studi kasus nyata dan memberikan rekomendasi perbaikan dasar.

🕮 1.1 Pendahuluan: Mengapa Keamanan Informasi Penting?

Bayangkan sebuah skenario: Anda bangun di pagi hari, meraih ponsel, dan mendapati semua data Anda—foto, pesan, kontak, hingga aplikasi perbankan—tiba-tiba lenyap. Atau, Anda menemukan bahwa akun media sosial Anda memposting hal-hal aneh yang tidak pernah Anda tulis. Bagaimana perasaan Anda? Mungkin marah, frustrasi, atau bahkan panik.

Sekarang, bayangkan skenario yang sama terjadi pada sebuah organisasi besar. Data pelanggan yang bocor, sistem pembayaran yang tidak bisa diakses, atau laporan keuangan yang diubah oleh pihak tidak bertanggung jawab. Dampaknya bukan

hanya sekadar ketidaknyamanan, tetapi bisa berupa kerugian finansial jutaan rupiah, tuntutan hukum, kehilangan kepercayaan pelanggan, hingga kebangkrutan.

Keamanan informasi bukan lagi sekadar urusan departemen TI. Ini adalah fondasi utama bagi kelangsungan bisnis dan reputasi organisasi di era digital. Setiap hari, kita mendengar berita tentang kebocoran data, serangan ransomware, atau peretasan sistem. Pertanyaannya bukan lagi "*Apakah organisasi saya akan diserang?*", tetapi "*Kapan organisasi saya akan diserang, dan seberapa siap kita menghadapinya?*"

Mata kuliah ini akan membekali Anda dengan pemahaman konseptual dan analitis untuk menjawab pertanyaan tersebut. Dan perjalanan kita dimulai dari fondasi paling dasar: **CIA Triad**.

🕮 1.2 Definisi dan Tujuan Keamanan Informasi

Sebelum memahami konsep CIA Triad, kita perlu sepakat terlebih dahulu tentang apa yang dimaksud dengan keamanan informasi.

Keamanan informasi adalah upaya perlindungan aset informasi dari berbagai ancaman untuk memastikan kelangsungan bisnis, meminimalkan risiko, dan memaksimalkan pengembalian investasi. Aset informasi sendiri bisa berupa apa saja yang memiliki nilai bagi organisasi: data pelanggan, laporan keuangan, rahasia dagang, kekayaan intelektual, hingga reputasi merek.

Menurut **Whitman & Mattord (2021)**, keamanan informasi memiliki tiga tujuan utama yang menjadi pilar segala upaya perlindungan:

1. **Melindungi kerahasiaan data.**
2. **Menjaga integritas informasi.**
3. **Memastikan ketersediaan sistem dan data saat dibutuhkan.**

Ketiga tujuan inilah yang kemudian dikenal dengan nama **CIA Triad** (*Confidentiality, Integrity, Availability*).

🕮 1.3 CIA Triad: Tiga Pilar Utama Keamanan Informasi

CIA Triad adalah model yang paling widely accepted dalam dunia keamanan informasi. Setiap kebijakan, kontrol, dan teknologi keamanan pada dasarnya dirancang untuk memenuhi satu atau lebih dari ketiga prinsip ini.

1.3.1 Kerahasiaan (Confidentiality)

Kerahasiaan berarti memastikan bahwa informasi hanya dapat diakses oleh pihak-pihak yang berwenang. Informasi harus terlindungi dari pengungkapan kepada entitas, individu, atau proses yang tidak memiliki otorisasi.

Analogi Sederhana:
Bayangkan Anda memiliki buku harian pribadi. Anda menguncinya di dalam laci dan hanya Anda yang memiliki kuncinya. Jika orang lain berhasil membuka laci dan membaca buku harian Anda, maka kerahasiaan telah dilanggar.

Dalam Konteks Organisasi:

- Data pelanggan (nama, alamat, nomor KTP, riwayat transaksi) harus dijaga kerahasiaannya.
- Laporan keuangan sebelum dipublikasikan hanya boleh diakses oleh direksi dan bagian keuangan.
- Rahasia dagang, seperti resep minuman ringan, harus dijaga ketat dari pesaing.

Mekanisme untuk Menjaga Kerahasiaan:

- **Enkripsi:** Mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi.
- **Kontrol Akses:** Membatasi siapa yang dapat mengakses data (misalnya, menggunakan username dan password, atau biometrik).
- **Klasifikasi Data:** Memberi label pada data berdasarkan tingkat sensitivitasnya (misalnya: Publik, Internal, Rahasia, Sangat Rahasia).

1.3.2 Integritas (Integrity)

Integritas berarti menjaga keakuratan, keutuhan, dan keaslian informasi. Data tidak boleh diubah atau dirusak oleh pihak yang tidak berwenang. Lebih dari itu, integritas

juga memastikan bahwa jika perubahan dilakukan oleh pihak yang berwenang, perubahan tersebut dapat dilacak dan direkam.

Analogi Sederhana:
Anda mengirimkan pesan singkat kepada teman: "Temui saya di kantin A jam 12 siang." Jika di tengah jalan, seseorang menyadap dan mengubah pesan Anda menjadi "Temui saya di kantin B jam 1 siang," maka integritas pesan Anda telah dilanggar. Teman Anda akan salah informasi.

Dalam Konteks Organisasi:

- Angka-angka dalam laporan keuangan tidak boleh diubah, baik oleh kesalahan sistem maupun oleh oknum yang ingin melakukan fraud.
- Data rekam medis pasien harus akurat dan tidak boleh diubah oleh pihak yang tidak berwenang.
- Kode sumber aplikasi harus dijaga agar tidak disisipi *backdoor* oleh peretas.

Mekanisme untuk Menjaga Integritas:

- **Fungsi Hash:** Algoritma yang menghasilkan "sidik jari" digital unik untuk sebuah data. Jika data diubah sedikit saja, nilai hash-nya akan berubah total.
- **Tanda Tangan Digital:** Memastikan keaslian dan keutuhan dokumen elektronik.
- **Logging dan Audit Trail:** Merekam siapa yang mengakses dan mengubah data, kapan, dan dari mana.
- **Checksum:** Digunakan untuk memverifikasi integritas file setelah diunduh atau ditransfer.

1.3.3 Ketersediaan (Availability)

Ketersediaan berarti memastikan bahwa informasi dan sistem dapat diakses dan digunakan oleh pihak yang berwenang setiap kali dibutuhkan. Sistem harus handal dan tahan terhadap gangguan.

Analogi Sederhana:
Anda ingin menarik uang tunai di ATM karena ada keperluan mendesak. Sesampainya di ATM, ternyata semua mesin mati karena listrik padam dan genset tidak berfungsi. Di saat itu, ketersediaan layanan ATM telah gagal.

Dalam Konteks Organisasi:

- Situs web e-commerce harus tersedia 24/7, terutama saat hari besar seperti Harbolnas.
- Sistem reservasi tiket pesawat harus bisa diakses kapan saja oleh calon penumpang.
- Aplikasi perbankan mobile harus selalu *online* agar nasabah bisa bertransaksi.

Mekanisme untuk Menjaga Ketersediaan:

- **Redundansi:** Memiliki cadangan perangkat keras, seperti server cadangan atau sumber listrik cadangan (UPS, genset).
- **Backup dan Disaster Recovery:** Memiliki salinan data di lokasi yang aman dan rencana untuk memulihkan sistem jika terjadi bencana.
- **Load Balancing:** Mendistribusikan lalu lintas ke beberapa server agar tidak ada server yang kelebihan beban.
- **Pemeliharaan Rutin:** Memastikan sistem selalu dalam kondisi optimal dan bebas dari kerentanan yang bisa menyebabkan *crash*.

Hubungan Antar Pilar

Ketiga pilar CIA saling terkait dan tidak bisa dipisahkan. Seringkali, upaya untuk memperkuat satu pilar dapat melemahkan pilar lainnya, sehingga diperlukan keseimbangan. Misalnya:

- Enkripsi yang sangat kuat (memperkuat **Confidentiality**) dapat memperlambat akses data, sehingga berpotensi menurunkan **Availability**.
- Redundansi yang berlebihan (memperkuat **Availability**) bisa sangat mahal dan kompleks, sehingga berpotensi menimbulkan kesalahan konfigurasi yang mengancam **Integrity**.

Tantangan seorang profesional keamanan informasi adalah menemukan keseimbangan yang tepat sesuai dengan kebutuhan dan profil risiko organisasi.

1.4 Studi Kasus: Analisis Kebocoran Data dari Perspektif CIA Triad

Untuk memahami aplikasi CIA Triad dalam dunia nyata, mari kita analisis dua kasus kebocoran data besar yang pernah terjadi di Indonesia.

Kasus 1: Kebocoran Data Tokopedia (2020)

Kronologi Singkat:
Pada bulan Mei 2020, seorang peretas (*hacker*) mengklaim telah mencuri data 91 juta pengguna Tokopedia. Data yang bocor diduga meliputi nama lengkap, alamat email, nomor telepon, kata sandi terenkripsi (hash), dan tanggal lahir. Data tersebut kemudian dijual di forum gelap (*dark web*).

Analisis Pelanggaran CIA Triad:

Pilar CIA	Analisis Pelanggaran
Kerahasiaan (Confidentiality)	**Dilanggar berat.** Data pribadi jutaan pengguna yang seharusnya bersifat rahasia dan hanya diketahui oleh pengguna dan Tokopedia, berhasil diakses dan disebarluaskan oleh pihak tidak berwenang. Informasi ini kemudian dijual, sehingga kerahasiaannya hilang selamanya.
Integritas (Integrity)	**Berpotensi dilanggar.** Meskipun data yang dijual adalah data asli, peretas bisa saja memodifikasi data tersebut sebelum menjualnya. Lebih jauh lagi, dengan data yang bocor, pihak tidak bertanggung jawab bisa melakukan *account takeover* dan mengubah data pengguna di platform lain jika pengguna menggunakan kata sandi yang sama.
Ketersediaan (Availability)	**Tidak dilanggar secara langsung.** Situs Tokopedia tetap dapat diakses selama dan setelah insiden. Namun, sebagai dampak lanjutan, Tokopedia mungkin harus menonaktifkan sementara beberapa fitur untuk melakukan investigasi dan perbaikan keamanan.

Dampak Pelanggaran:

- **Finansial:** Potensi kerugian akibat tuntutan hukum, denda regulasi (terkait UU PDP), dan biaya pemulihan keamanan.
- **Reputasi:** Kepercayaan pengguna menurun drastis. Banyak pengguna yang memilih untuk menghapus akun atau beralih ke kompetitor.
- **Operasional:** Tokopedia harus mereset kata sandi semua pengguna, mengkomunikasikan insiden secara masif, dan memperkuat sistem keamanannya.

Kasus 2: Kebocoran Data Facebook (Cambridge Analytica, 2018)

Kronologi Singkat:

Data jutaan pengguna Facebook dikumpulkan tanpa persetujuan mereka oleh sebuah aplikasi kuis psikologi. Data tersebut kemudian digunakan oleh perusahaan konsultan politik, Cambridge Analytica, untuk membuat profil psikologis pemilih dan menargetkan iklan politik selama kampanye pemilu AS 2016.

Analisis Pelanggaran CIA Triad:

Pilar CIA	Analisis Pelanggaran
Kerahasiaan (Confidentiality)	**Dilanggar berat.** Data pengguna dikumpulkan dan digunakan untuk tujuan yang sama sekali berbeda dari tujuan awal saat data diberikan. Ini adalah pelanggaran kepercayaan dan kerahasiaan data.
Integritas (Integrity)	**Dilanggar.** Profil psikologis yang dibuat oleh Cambridge Analytica adalah "informasi baru" yang diturunkan dari data mentah. Informasi turunan ini digunakan untuk membentuk opini publik, yang pada dasarnya memanipulasi integritas proses demokrasi.
Ketersediaan (Availability)	**Tidak dilanggar.** Facebook tetap dapat diakses.

Poin Penting dari Kasus Ini:

Kasus Cambridge Analytica menunjukkan bahwa pelanggaran CIA Triad tidak selalu bersifat teknis (peretasan). Pelanggaran juga bisa terjadi karena lemahnya kontrol atas bagaimana data pihak ketiga mengakses dan menggunakan data pengguna.

🗝 1.5 Rangkuman

1. **Keamanan informasi** adalah upaya melindungi aset informasi dari berbagai ancaman.
2. **CIA Triad** adalah fondasi utama keamanan informasi, terdiri dari:
    - **Confidentiality (Kerahasiaan):** Informasi hanya dapat diakses oleh pihak yang berwenang.
    - **Integrity (Integritas):** Informasi akurat, utuh, dan tidak diubah oleh pihak tidak berwenang.
    - **Availability (Ketersediaan):** Informasi dan sistem dapat diakses saat dibutuhkan.
3. Ketiga pilar CIA saling terkait dan harus dijaga keseimbangannya.
4. Pelanggaran terhadap salah satu pilar dapat berdampak serius pada finansial, reputasi, dan operasional organisasi.

✍ 1.6 Latihan Soal

1. Jelaskan dengan kata-kata Anda sendiri perbedaan antara kerahasiaan dan integritas. Berikan masing-masing satu contoh pelanggaran di dunia nyata.
2. Sebuah rumah sakit mengalami serangan ransomware yang mengenkripsi semua data pasien. Rumah sakit memilih untuk membayar tebusan agar data kembali normal. Pilar CIA mana saja yang terdampak dalam insiden ini? Jelaskan.
3. Mengapa menjaga keseimbangan antara ketiga pilar CIA itu penting? Berikan contoh situasi di mana terlalu fokus pada satu pilar justru bisa merugikan organisasi.

📝 1.7 Tugas Mandiri (Bobot 2%)

Instruksi:

Carilah satu berita terbaru (maksimal 1 tahun terakhir) tentang insiden keamanan informasi yang terjadi di Indonesia atau dunia.

Langkah Tugas:

1. **Identifikasi Pelanggaran CIA:** Analisis berita tersebut dan identifikasi aspek CIA Triad mana saja yang dilanggar. Jelaskan alasannya.
2. **Analisis Dampak:** Jelaskan dampak pelanggaran tersebut terhadap organisasi yang menjadi korban (dampak finansial, reputasi, operasional).
3. **Rekomendasi Dasar:** Berikan minimal dua rekomendasi sederhana yang seharusnya bisa dilakukan oleh organisasi tersebut untuk mencegah insiden serupa di masa depan.

Format Penugasan:

- Ditulis dalam format PDF.
- Panjang maksimal 2 halaman.
- Sertakan tautan/link berita asli.

BAB 2
ANCAMAN, KERENTANAN, DAN SERANGAN KEAMANAN INFORMASI

🎯 Kemampuan Akhir (Sub-CPMK 1.2)

Setelah mempelajari bab ini, mahasiswa mampu:

1. Mengidentifikasi berbagai jenis aset informasi dalam organisasi.
2. Membedakan konsep ancaman (*threat*), kerentanan (*vulnerability*), dan serangan (*attack*).
3. Menjelaskan berbagai jenis ancaman dan serangan siber beserta modus operandinya.
4. Membuat peta ancaman sederhana untuk organisasi fiktif.

🕮 2.1 Pendahuluan: Memahami Musuh dan Medan Perang

Jika CIA Triad adalah "benteng" yang ingin kita lindungi, maka bab ini akan membahas tentang "musuh" yang ingin menyerang benteng tersebut, "kelemahan" pada benteng yang bisa dimanfaatkan musuh, dan "strategi serangan" yang mereka gunakan.

Dalam dunia keamanan informasi, kita tidak bisa bersikap reaktif. Kita harus **proaktif**. Artinya, kita harus memahami apa saja yang bisa salah, siapa yang mungkin mencoba membuatnya salah, dan bagaimana cara mereka melakukannya. Pemahaman inilah yang menjadi dasar untuk membangun pertahanan yang efektif.

🕮 2.2 Klasifikasi Aset Informasi

Sebelum melindungi sesuatu, kita harus tahu persis apa yang kita lindungi. Dalam terminologi keamanan informasi, "sesuatu" itu disebut **aset**. Aset adalah segala sesuatu yang memiliki nilai bagi organisasi.

Aset informasi dapat diklasifikasikan ke dalam beberapa kategori:

Kategori Aset	Deskripsi	Contoh
Aset Data	Informasi itu sendiri, yang tersimpan dalam basis data, file, dokumen, dll.	Data pelanggan, laporan keuangan, rahasia dagang, kekayaan intelektual, strategi pemasaran.
Aset Perangkat Lunak	Aplikasi dan program yang digunakan untuk memproses data.	Sistem operasi, aplikasi ERP, aplikasi mobile, perangkat lunak akuntansi, kode sumber.
Aset Perangkat Keras	Perangkat fisik yang mendukung operasional TI.	Server, komputer karyawan, laptop, perangkat jaringan (router, switch, firewall), media penyimpanan (hard disk, SSD).
Aset Manusia	Pengetahuan, keterampilan, dan keahlian karyawan.	Admin jaringan yang ahli, programmer senior, manajer TI, seluruh karyawan yang memiliki akses ke sistem.
Aset Layanan	Layanan yang disediakan oleh sistem TI.	Layanan email, layanan website, layanan cloud, koneksi internet, layanan VoIP.
Aset Reputasi	Nama baik dan kepercayaan publik terhadap organisasi.	Merek perusahaan, kepercayaan pelanggan, citra di mata publik.

Pentingnya Klasifikasi Aset:

Tidak semua aset memiliki nilai yang sama. Data pelanggan jelas lebih berharga daripada daftar menu kantin. Oleh karena itu, klasifikasi aset membantu organisasi untuk mengalokasikan sumber daya keamanan secara proporsional. Aset yang paling kritis harus mendapatkan perlindungan yang paling kuat.

🕮 2.3 Ancaman (Threats)

Ancaman adalah segala sesuatu yang berpotensi menyebabkan kerugian atau kerusakan pada aset informasi. Ancaman adalah "aktor" atau "kejadian" yang dapat mengeksploitasi kerentanan.

Ancaman dapat diklasifikasikan berdasarkan asalnya:

2.3.1 Ancaman Alam

Bencana alam yang berada di luar kendali manusia.

- **Contoh:** Gempa bumi, banjir, kebakaran, petir, angin topan.
- **Dampak:** Kerusakan fisik pada pusat data dan infrastruktur TI, menyebabkan hilangnya ketersediaan data.

2.3.2 Ancaman Manusia

Ancaman yang berasal dari tindakan manusia, baik disengaja maupun tidak disengaja.

- **Ancaman Tidak Disengaja:**
  - Karyawan yang tidak sengaja menghapus file penting.
  - Karyawan yang mengklik tautan phishing.
  - Admin yang salah konfigurasi server sehingga menjadi rentan.
- **Ancaman Disengaja:**
  - **Peretas (Hackers/Crackers):** Individu atau kelompok yang mencoba menerobos sistem untuk berbagai motif (keuntungan finansial, tantangan, aktivisme).
  - **Insider Threat (Ancaman dari Dalam):** Karyawan yang tidak puas dan sengaja merusak sistem atau mencuri data.
  - **Pesaing Bisnis:** Perusahaan pesaing yang melakukan spionase industri.
  - **Teroris Siber:** Kelompok yang melakukan serangan untuk tujuan politik atau ideologis.

2.3.3 Ancaman Lingkungan

Ancaman yang berasal dari kondisi lingkungan di sekitar organisasi.

- **Contoh:** Gangguan listrik jangka panjang, fluktuasi tegangan listrik, kebocoran pipa air di dekat ruang server, polusi debu yang merusak perangkat keras.

🕮 2.4 Kerentanan (Vulnerabilities)

Kerentanan adalah kelemahan atau celah dalam sistem keamanan yang dapat dimanfaatkan oleh ancaman untuk menyebabkan kerusakan. Kerentanan adalah "titik lemah" pada benteng kita.
Kerentanan juga dapat diklasifikasikan:

2.4.1 Kerentanan Teknis

- **Kerentanan Perangkat Lunak:** *Bug* dalam kode program, *software* yang sudah usang (tidak di-*patch*), kesalahan konfigurasi.
- **Kerentanan Perangkat Keras:** Desain perangkat keras yang lemah, paparan terhadap medan elektromagnetik, kurangnya cadangan.
- **Kerentanan Jaringan:** Port jaringan yang terbuka tanpa perlu, protokol yang tidak aman, kurangnya segmentasi jaringan.

2.4.2 Kerentanan Administratif

- **Tidak Ada Kebijakan:** Organisasi tidak memiliki kebijakan keamanan informasi yang jelas.
- **Kurangnya Pelatihan:** Karyawan tidak pernah mendapat pelatihan kesadaran keamanan (*security awareness training*).
- **Prosedur Lemah:** Prosedur *onboarding* dan *offboarding* karyawan yang tidak aman (misal: akun karyawan yang resign masih aktif).

2.4.3 Kerentanan Fisik

- **Kontrol Akses Fisik Lemah:** Ruang server tidak terkunci, tidak ada kartu akses untuk masuk gedung.
- **Tidak Ada Pengawasan:** Tidak ada kamera CCTV di area sensitif.
- **Lokasi Rentan:** Gedung kantor berada di daerah rawan banjir.

2.4.4 Hubungan Ancaman dan Kerentanan

Poin penting yang harus dipahami adalah: **Ancaman hanya menjadi berbahaya jika ada kerentanan yang dapat dieksploitasi.**

Sebuah organisasi mungkin berada di daerah rawan gempa (ancaman alam), tetapi jika pusat datanya dibangun dengan struktur tahan gempa dan memiliki cadangan di lokasi lain, maka risikonya kecil. Sebaliknya, seorang peretas (ancaman manusia)

tidak akan bisa masuk ke sistem jika tidak ada celah keamanan yang bisa dimanfaatkan (kerentanan).

🕮 2.5 Serangan (Attacks)

Serangan adalah tindakan nyata yang dilakukan oleh ancaman untuk mengeksploitasi kerentanan. Serangan adalah "tembakan" yang dilancarkan musuh ke titik lemah benteng.

Berikut adalah beberapa jenis serangan yang paling umum:

2.5.1 Malware (Malicious Software)

Perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mendapatkan akses tidak sah ke sistem.

- **Virus:** Menyebar dengan menempel pada file atau program lain dan membutuhkan interaksi manusia (misal: membuka file yang terinfeksi).
- **Worm:** Menyebar sendiri melalui jaringan tanpa memerlukan interaksi manusia.
- **Trojan Horse:** Berpura-pura menjadi perangkat lunak yang berguna, tetapi diam-diam menjalankan fungsi jahat di latar belakang.
- **Ransomware:** Mengenkripsi data korban dan meminta tebusan (biasanya dalam bentuk mata uang kripto) untuk mengembalikan akses.
- **Spyware:** Diam-diam memata-matai aktivitas pengguna dan mencuri informasi (seperti kebiasaan browsing, kata sandi).
- **Adware:** Menampilkan iklan yang tidak diinginkan, seringkali secara agresif.

2.5.2 Social Engineering

Serangan yang memanipulasi psikologi manusia, bukan teknologi, untuk mendapatkan akses atau informasi.

- **Phishing:** Mengirim email palsu yang tampak seperti berasal dari entitas terpercaya (bank, perusahaan ternama) untuk mengelabui korban agar mengklik tautan berbahaya atau memberikan informasi sensitif.
- **Spear Phishing:** Versi phishing yang lebih terarah, menyasar individu tertentu dengan pesan yang dipersonalisasi.

- **Pretexting:** Membuat skenario palsu (kedok) untuk mencuri informasi pribadi korban. Misal: seseorang berpura-pura menjadi teknisi TI dan meminta kata sandi untuk "memperbaiki" sistem.
- **Baiting:** Menawarkan sesuatu yang menarik (misal: USB flash drive gratis, unduhan film gratis) yang telah terinfeksi malware.
- **Tailgating/Piggybacking:** Seseorang yang tidak berwenang mengikuti karyawan yang berwenang masuk ke area terbatas.

2.5.3 Network Attacks

Serangan yang menargetkan infrastruktur jaringan.

- **DDoS (Distributed Denial of Service):** Membanjiri server atau jaringan dengan lalu lintas palsu dari banyak sumber sehingga sistem kewalahan dan tidak dapat melayani pengguna yang sah. Ini adalah serangan terhadap **ketersediaan**.
- **Man-in-the-Middle (MitM):** Penyerang diam-diam menyadap dan berpotensi mengubah komunikasi antara dua pihak yang saling percaya. Misal: saat korban terhubung ke WiFi publik yang tidak aman, penyerang bisa membaca semua data yang dikirimkan.
- **Packet Sniffing:** Menangkap dan menganalisis paket data yang melintasi jaringan untuk mencuri informasi.
- **DNS Spoofing:** Mengarahkan pengguna yang mengetik alamat website tertentu ke website palsu yang dikendalikan penyerang.

2.5.4 Password Attacks

Serangan yang bertujuan untuk mencuri atau memecahkan kata sandi.

- **Brute Force Attack:** Mencoba semua kemungkinan kombinasi karakter hingga menemukan kata sandi yang benar.
- **Dictionary Attack:** Menggunakan daftar kata-kata umum, frasa, dan kata sandi yang sering digunakan untuk mencoba masuk.
- **Credential Stuffing:** Menggunakan kombinasi username/password yang bocor dari satu situs untuk mencoba masuk ke situs lain.

💡 2.6 Studi Kasus: Analisis Serangan Siber Terkini

Kasus: Serangan Ransomware pada Rumah Sakit (Contoh)

Kronologi:
Pada tahun 2023, sebuah rumah sakit besar di Indonesia mengalami serangan ransomware. Seorang karyawan tanpa sengaja mengklik tautan phishing di email yang tampak seperti undangan seminar kesehatan. Malware kemudian menyebar melalui jaringan internal, mengenkripsi ribuan file, termasuk rekam medis pasien, data penjadwalan operasi, dan sistem administrasi.

Dampak:

- Rumah sakit tidak dapat mengakses data pasien, sehingga pelayanan terhambat.
- Pasien dengan kondisi gawat darurat harus dirujuk ke rumah sakit lain.
- Operasi elektif ditunda.
- Rumah sakit harus membayar tebusan dalam bentuk Bitcoin untuk mendapatkan kunci dekripsi.
- Reputasi rumah sakit tercoreng, kepercayaan pasien menurun.

Analisis:

- **Ancaman:** Peretas (ancaman manusia disengaja).
- **Kerentanan yang Dieksploitasi:**
    - Kurangnya kesadaran karyawan terhadap phishing (kerentanan administratif).
    - Kemungkinan tidak ada segmentasi jaringan yang baik, sehingga malware menyebar dengan cepat (kerentanan teknis).
    - Kemungkinan *backup* tidak tersedia atau tidak diuji (kerentanan teknis/administratif).
- **Serangan:** Phishing + Malware (Ransomware).

🗝 2.7 Rangkuman

1. **Aset** adalah segala sesuatu yang bernilai bagi organisasi dan perlu dilindungi.
2. **Ancaman** adalah potensi penyebab kerugian. Bisa berasal dari alam, manusia, atau lingkungan.
3. **Kerentanan** adalah kelemahan yang bisa dieksploitasi oleh ancaman.
4. **Serangan** adalah aksi nyata yang mengeksploitasi kerentanan.
5. Memahami hubungan antara aset, ancaman, kerentanan, dan serangan adalah langkah pertama dalam membangun strategi pertahanan yang efektif.
6. Serangan dapat menyasar manusia (social engineering), perangkat lunak (malware), atau jaringan (DDoS).

✍ 2.8 Latihan Soal

1. Jelaskan perbedaan antara ancaman, kerentanan, dan serangan. Berikan analogi sederhana untuk menjelaskan ketiganya.
2. Seorang karyawan menyimpan kata sandi akun kantornya di *sticky note* yang ditempel di monitor komputer. Dalam konteks ini, identifikasi: apa asetnya, apa ancamannya, dan apa kerentanannya?
3. Sebutkan tiga jenis serangan social engineering dan jelaskan bagaimana cara kerjanya.

📝 2.9 Tugas Mandiri (Bobot 2%)

Instruksi:

Buatlah **Peta Ancaman (Threat Map)** untuk sebuah organisasi fiktif. Pilih salah satu jenis organisasi berikut: **Usaha Kecil Menengah (UKM) bidang e-commerce** atau **Rumah Sakit Tipe C**.

Langkah Tugas:

1. **Identifikasi Aset:** Sebutkan minimal 5 aset kritis yang dimiliki organisasi tersebut.
2. **Identifikasi Ancaman:** Untuk setiap aset, identifikasi minimal 3 ancaman potensial yang mungkin terjadi.
3. **Vektor Serangan:** Jelaskan bagaimana ancaman tersebut dapat mengeksploitasi kerentanan (modus serangan).
4. **Dampak:** Jelaskan dampak jika serangan tersebut berhasil.
5. **Mitigasi Awal:** Berikan satu saran mitigasi sederhana untuk setiap ancaman.

Format Penugasan:

- Boleh dalam bentuk tabel atau mind map.
- Dikumpulkan dalam format PDF.

BAB 3
STANDAR DAN FRAMEWORK KEAMANAN INFORMASI

🎯 Kemampuan Akhir (Sub-CPMK 1.3)

Setelah mempelajari bab ini, mahasiswa mampu:

1. Menjelaskan tujuan dan manfaat penggunaan standar/framework keamanan informasi.
2. Menjelaskan struktur dan komponen utama ISO/IEC 27001.
3. Menjelaskan fungsi inti NIST Cybersecurity Framework.
4. Membandingkan pendekatan ISO 27001 dan NIST CSF.
5. Merekomendasikan standar yang sesuai untuk organisasi tertentu.

🕮 3.1 Pendahuluan: Mengapa Perlu Standar?

Bayangkan Anda ingin membangun sebuah rumah. Apakah Anda akan membangunnya tanpa cetak biru, hanya berdasarkan perkiraan dan "kira-kira" saja? Tentu tidak. Anda membutuhkan arsitek yang membuat gambar desain, menghitung struktur, dan memastikan rumah tersebut aman dan nyaman.

Demikian pula dengan keamanan informasi. Membangun sistem keamanan tanpa panduan yang jelas akan menghasilkan pertahanan yang "tambal sulam", tidak konsisten, dan sulit diukur efektivitasnya. Di sinilah peran **standar** dan **framework**.

Standar dan **framework** keamanan informasi menyediakan:

- **Bahasa yang sama:** Memudahkan komunikasi antara departemen TI, manajemen, dan auditor.

- **Praktik terbaik (*best practices*):** Berisi kumpulan pengetahuan dari para ahli di seluruh dunia.
- **Dasar pengukuran:** Memungkinkan organisasi menilai tingkat kematangan keamanannya.
- **Kepatuhan:** Membantu organisasi memenuhi persyaratan hukum dan regulasi.

Dua standar/framework yang paling banyak diadopsi secara global adalah **ISO/IEC 27001** dan **NIST Cybersecurity Framework**.

🕮 3.2 ISO/IEC 27001

ISO/IEC 27001 adalah standar internasional untuk **Sistem Manajemen Keamanan Informasi (SMKI)** atau *Information Security Management System (ISMS)*. Standar ini diterbitkan oleh *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC).

3.2.1 Konsep Dasar ISO 27001

ISO 27001 bersifat **preskriptif** dalam hal manajemen, tetapi **fleksibel** dalam hal teknis. Artinya, standar ini menetapkan *apa* yang harus dilakukan (persyaratan), tetapi tidak menentukan *bagaimana* cara melakukannya. Hal ini memungkinkan organisasi dari berbagai ukuran dan jenis untuk menerapkannya sesuai dengan kebutuhan masing-masing.

Inti dari ISO 27001 adalah pendekatan **PDCA (Plan-Do-Check-Act)**:

- **Plan (Rencanakan):** Menetapkan kebijakan, tujuan, proses, dan prosedur yang relevan dengan manajemen risiko dan peningkatan keamanan informasi.
- **Do (Lakukan):** Menerapkan dan mengoperasikan kebijakan, kontrol, dan proses yang telah direncanakan.
- **Check (Periksa):** Memantau dan meninjau ulang kinerja proses terhadap kebijakan, tujuan, dan pengalaman praktis, serta melaporkan hasilnya kepada manajemen.
- **Act (Tindak Lanjuti):** Melakukan tindakan perbaikan dan pencegahan berdasarkan hasil audit dan tinjauan manajemen untuk mencapai peningkatan berkelanjutan.

3.2.2 Lampiran A (Annex A): 14 Domain Kontrol

Bagian paling sering dirujuk dari ISO 27001 adalah **Lampiran A (Annex A)** yang berisi daftar 93 kontrol keamanan yang dikelompokkan ke dalam 14 domain. Kontrol-kontrol ini adalah langkah-langkah yang dapat diambil organisasi untuk memitigasi risiko. Ke-14 domain tersebut adalah:

No	Domain (Klausul A.5 - A.18)	Deskripsi Singkat
1	A.5 **Kebijakan Keamanan Informasi**	Menyediakan arahan dan dukungan manajemen untuk keamanan informasi.
2	A.6 **Organisasi Keamanan Informasi**	Menetapkan kerangka kerja pengelolaan keamanan di dalam organisasi.
3	A.7 **Keamanan Sumber Daya Manusia**	Memastikan karyawan dan kontraktor memahami tanggung jawab mereka.
4	A.8 **Manajemen Aset**	Mengidentifikasi aset organisasi dan menetapkan tanggung jawab perlindungan.
5	A.9 **Kontrol Akses**	Membatasi akses ke informasi dan fasilitas pemrosesan informasi.
6	A.10 **Kriptografi**	Memastikan penggunaan kriptografi yang tepat untuk melindungi informasi.
7	A.11 **Keamanan Fisik dan Lingkungan**	Mencegah akses fisik tidak sah, kerusakan, dan gangguan.
8	A.12 **Keamanan Operasional**	Memastikan operasi fasilitas pemrosesan informasi yang benar dan aman.
9	A.13 **Keamanan Komunikasi**	Melindungi informasi dalam jaringan dan fasilitas pendukungnya.
10	A.14 **Akuisisi, Pengembangan, & Pemeliharaan Sistem**	Memastikan keamanan menjadi bagian integral dari sistem informasi.
11	A.15 **Hubungan dengan Pemasok**	Melindungi aset organisasi yang diakses oleh pemasok.
12	A.16 **Manajemen Insiden Keamanan Informasi**	Memastikan respons yang konsisten dan efektif terhadap insiden.
13	A.17 **Aspek Keamanan Informasi dalam Manajemen Kelangsungan Bisnis**	Memastikan ketersediaan informasi saat terjadi gangguan.
14	A.18 **Kepatuhan**	Menghindari pelanggaran hukum, peraturan, dan

No	Domain (Klausul A.5 - A.18)	Deskripsi Singkat
		kewajiban kontraktual.

Organisasi yang ingin mendapatkan **sertifikasi ISO 27001** harus diaudit oleh lembaga sertifikasi independen untuk membuktikan bahwa mereka telah menerapkan SMKI sesuai dengan standar.

🕮 3.3 NIST Cybersecurity Framework

NIST Cybersecurity Framework (CSF) dikembangkan oleh *National Institute of Standards and Technology* (NIST) di Amerika Serikat. Berbeda dengan ISO 27001 yang bersifat standar dengan sertifikasi, NIST CSF lebih bersifat **framework sukarela** yang memberikan panduan berbasis risiko.

3.3.1 Struktur Inti NIST CSF

NIST CSF terdiri dari tiga bagian utama: **Framework Core**, **Implementation Tiers**, dan **Framework Profiles**. Bagian yang paling sering digunakan adalah **Framework Core**.

Framework Core terdiri dari 5 fungsi paralel dan berkelanjutan yang memberikan pandangan tingkat tinggi tentang siklus hidup manajemen risiko keamanan siber.

Fungsi	Deskripsi	Kategori (Contoh)
Identify (Identifikasi)	Mengembangkan pemahaman organisasi untuk mengelola risiko keamanan siber terhadap sistem, aset, data, dan kemampuan.	Manajemen Aset, Lingkungan Bisnis, Tata Kelola, Penilaian Risiko, Manajemen Risiko Rantai Pasok.
Protect (Lindungi)	Mengembangkan dan menerapkan pengamanan yang sesuai untuk memastikan penyampaian layanan infrastruktur kritis.	Kontrol Akses, Kesadaran dan Pelatihan, Keamanan Data, Proses dan Prosedur Proteksi Informasi, Pemeliharaan, Teknologi Protektif.
Detect (Deteksi)	Mengembangkan dan menerapkan aktivitas yang sesuai untuk mengidentifikasi terjadinya insiden keamanan siber.	Anomali dan Kejadian, Pemantauan Keamanan Berkelanjutan, Proses Deteksi.

Fungsi	Deskripsi	Kategori (Contoh)
Respond (Respons)	Mengembangkan dan menerapkan aktivitas yang sesuai untuk mengambil tindakan terkait insiden keamanan siber yang terdeteksi.	Perencanaan Respons, Komunikasi, Analisis, Mitigasi, Perbaikan.
Recover (Pemulihan)	Mengembangkan dan menerapkan aktivitas yang sesuai untuk mempertahankan rencana ketahanan dan memulihkan kemampuan atau layanan apa pun yang terganggu akibat insiden keamanan siber.	Perencanaan Pemulihan, Perbaikan, Komunikasi.

Kelima fungsi ini tidak bersifat linier, melainkan berjalan secara paralel dan terus-menerus. Organisasi dapat memulai dari fungsi mana pun dan meningkatkan kemampuannya dari waktu ke waktu.

3.3.2 Implementation Tiers dan Profiles

- **Implementation Tiers (Tingkat Implementasi):** Menggambarkan seberapa canggih praktik manajemen risiko keamanan siber organisasi, dari Tier 1 (Parsial) hingga Tier 4 (Adaptif).
- **Profiles (Profil):** Menyelaraskan fungsi, kategori, dan subkategori Framework Core dengan persyaratan bisnis, toleransi risiko, dan sumber daya organisasi. Ada *Current Profile* (kondisi saat ini) dan *Target Profile* (kondisi yang diinginkan).

💡 3.4 Studi Kasus: Perbandingan ISO 27001 dan NIST CSF

Untuk memahami perbedaan pendekatan, mari kita bandingkan kedua framework ini.

Aspek Perbandingan	ISO/IEC 27001	NIST Cybersecurity Framework
Sifat	Standar internasional yang dapat disertifikasi.	Framework sukarela (berbasis AS, tetapi diadopsi global).
Pendekatan	Manajemen (Sistem Manajemen Keamanan Informasi - SMKI).	Risiko (Manajemen Risiko Keamanan Siber).
Fokus Utama	Membangun, menerapkan, memelihara, dan meningkatkan SMKI secara berkelanjutan.	Membantu organisasi memahami, mengelola, dan mengurangi risiko keamanan siber.
Struktur	Klausul (4-10) untuk persyaratan sistem manajemen + Lampiran A (14 domain kontrol).	5 Fungsi Inti (Identify, Protect, Detect, Respond, Recover) + Tiers + Profiles.
Sertifikasi	Ada. Organisasi dapat diaudit dan mendapatkan sertifikat ISO 27001.	Tidak ada. Organisasi menggunakan framework untuk menilai dan meningkatkan kemampuan mereka sendiri.
Fleksibilitas	Fleksibel dalam implementasi teknis, tetapi ketat dalam persyaratan manajemen.	Sangat fleksibel, dapat disesuaikan dengan kebutuhan dan ukuran organisasi mana pun.

Kapan Menggunakan ISO 27001?

- Ketika organisasi membutuhkan sertifikasi untuk membuktikan kepatuhan kepada pelanggan atau mitra bisnis.
- Ketika organisasi ingin membangun sistem manajemen keamanan yang terstruktur dan formal.
- Cocok untuk organisasi yang sudah mapan dan memiliki sumber daya untuk menjalankan proses formal.

Kapan Menggunakan NIST CSF?

- Ketika organisasi ingin memulai perjalanan keamanan siber dengan pendekatan yang praktis dan berbasis risiko.
- Ketika organisasi ingin berkomunikasi tentang risiko keamanan siber kepada manajemen puncak atau dewan direksi dengan bahasa yang lebih mudah dipahami.
- Cocok untuk organisasi dari semua ukuran, termasuk UKM.

🗝 3.5 Rangkuman

1. **Standar dan framework** menyediakan panduan, praktik terbaik, dan bahasa yang sama untuk mengelola keamanan informasi.
2. **ISO/IEC 27001** adalah standar internasional untuk Sistem Manajemen Keamanan Informasi (SMKI) dengan pendekatan PDCA dan 14 domain kontrol di Lampiran A. Organisasi dapat disertifikasi.
3. **NIST Cybersecurity Framework** adalah framework sukarela berbasis risiko dengan 5 fungsi inti: *Identify, Protect, Detect, Respond, Recover*. Tidak ada sertifikasi.
4. ISO 27001 lebih berfokus pada sistem manajemen, sedangkan NIST CSF lebih berfokus pada manajemen risiko. Keduanya dapat digunakan secara saling melengkapi.
5. Pemilihan standar tergantung pada kebutuhan, tujuan, dan sumber daya organisasi.

✍ 3.6 Latihan Soal

1. Jelaskan apa yang dimaksud dengan pendekatan PDCA dalam ISO 27001.
2. Sebutkan dan jelaskan secara singkat 3 dari 5 fungsi inti dalam NIST Cybersecurity Framework.
3. Sebuah perusahaan rintisan (startup) bidang teknologi finansial (fintech) ingin membangun fondasi keamanan informasinya. Menurut Anda, apakah lebih baik memulai dengan ISO 27001 atau NIST CSF? Jelaskan alasan Anda.

📝 3.7 Tugas Mandiri (Bobot 2.5%)

Instruksi:
Buatlah laporan analisis perbandingan singkat antara ISO 27001 dan NIST CSF.

Langkah Tugas:

1. **Jelaskan Struktur:** Jelaskan secara singkat struktur utama ISO 27001 (termasuk 14 domain di Lampiran A) dan 5 fungsi inti NIST CSF.
2. **Analisis Perbandingan:** Buatlah tabel perbandingan yang mencakup minimal 5 aspek (misal: sifat, pendekatan, fokus, struktur, sertifikasi).
3. **Rekomendasi:** Berikan rekomendasi, menurut analisis Anda, jenis organisasi seperti apa yang paling cocok menggunakan ISO 27001 dan jenis organisasi apa yang paling cocok menggunakan NIST CSF. Berikan justifikasi singkat.

Format Penugasan:

- Panjang maksimal 3 halaman.
- Dikumpulkan dalam format PDF.

📚 DAFTAR PUSTAKA

- ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.
- NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*. National Institute of Standards and Technology.
- Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.
- Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.

BAGIAN 2
KRIPTOGRAFI DAN IMPLEMENTASINYA

BAB 4
DASAR-DASAR KRIPTOGRAFI

🎯 Kemampuan Akhir (Sub-CPMK 2.1)

Setelah mempelajari bab ini, mahasiswa mampu:

1. Menjelaskan konsep dasar dan tujuan kriptografi.
2. Membedakan kriptografi simetris dan asimetris beserta kelebihan dan kekurangannya.
3. Memberikan contoh algoritma simetris (AES, DES) dan asimetris (RSA).
4. Menganalisis skenario penggunaan kriptografi dalam aplikasi nyata seperti e-commerce, email, dan perbankan.

🕮 4.1 Pendahuluan: Seni Menulis Rahasia

Sejak ribuan tahun lalu, manusia telah berusaha menyembunyikan pesan dari pihak yang tidak berhak membacanya. Julius Caesar, Kaisar Romawi, menggunakan metode sederhana dengan menggeser setiap huruf dalam pesannya sebanyak tiga posisi. Huruf A menjadi D, B menjadi E, dan seterusnya. Metode ini kemudian dikenal sebagai **Caesar Cipher**. Inilah awal mula dari apa yang kini kita kenal sebagai **kriptografi**.

Kriptografi berasal dari bahasa Yunani: *kryptos* (tersembunyi) dan *graphein* (menulis). Secara sederhana, kriptografi adalah seni dan ilmu untuk menjaga kerahasiaan pesan dengan mengubahnya menjadi format yang tidak dapat dipahami.

Di era digital modern, kriptografi bukan lagi sekadar seni, tetapi telah menjadi fondasi teknis yang memungkinkan berbagai aktivitas kita sehari-hari:

- **Belanja online:** Saat Anda memasukkan nomor kartu kredit di website, kriptografi melindungi data tersebut agar tidak dicuri.
- **Email:** Layanan email mengenkripsi komunikasi agar hanya Anda dan penerima yang dapat membaca isinya.
- **Aplikasi chatting:** Pesan WhatsApp Anda dilindungi dengan *end-to-end encryption*.
- **ATM:** Saat Anda memasukkan PIN, kriptografi melindungi data tersebut saat dikirim ke server bank.

Tanpa kriptografi, internet seperti yang kita kenal sekarang tidak akan mungkin ada. Setiap transaksi, setiap komunikasi, akan menjadi "bacaan umum" yang dapat disadap oleh siapa pun.

🕮 4.2 Tujuan Kriptografi

Kriptografi memiliki empat tujuan utama yang selaras dengan CIA Triad yang telah kita pelajari di Bab 1:

1. **Kerahasiaan (Confidentiality):** Memastikan bahwa pesan hanya dapat dibaca oleh pihak yang berwenang. Ini adalah fungsi paling klasik dari kriptografi.
2. **Integritas (Integrity):** Memastikan bahwa pesan tidak diubah selama proses pengiriman. Jika ada perubahan, penerima harus bisa mendeteksinya.
3. **Autentikasi (Authentication):** Memastikan identitas pengirim pesan. Penerima harus yakin bahwa pesan benar-benar berasal dari orang yang diklaim.
4. **Non-Repudiasi (Non-Repudiation):** Mencegah pengirim untuk menyangkal bahwa ia telah mengirim pesan. Ini penting dalam transaksi elektronik yang memiliki konsekuensi hukum.

🕮 4.3 Terminologi Dasar Kriptografi

Sebelum masuk ke jenis-jenis kriptografi, kita perlu memahami beberapa istilah dasar:

Istilah	Deskripsi	Analogi
Plaintext	Pesan asli yang dapat dibaca.	Surat biasa yang ditulis di kertas.
Ciphertext	Pesan yang telah diubah (dienkripsi) sehingga tidak dapat dibaca.	Surat yang ditulis dengan kode rahasia.
Enkripsi	Proses mengubah *plaintext* menjadi *ciphertext*.	Menulis surat dalam kode rahasia.
Dekripsi	Proses mengubah *ciphertext* kembali menjadi *plaintext*.	Menerjemahkan kode rahasia kembali ke surat biasa.
Kunci (Key)	Nilai rahasia yang digunakan untuk melakukan enkripsi dan dekripsi.	"Buku kode" atau "panduan" yang digunakan untuk membuat dan membaca kode rahasia.
Algoritma/Cipher	Prosedur matematis yang digunakan untuk enkripsi dan dekripsi.	Aturan atau rumus yang digunakan untuk membuat kode rahasia.

Prinsip penting dalam kriptografi modern adalah **Keamanan harus terletak pada kerahasiaan kunci, bukan pada kerahasiaan algoritma**. Aturan ini dikenal sebagai **Prinsip Kerckhoffs**. Algoritma kriptografi boleh diketahui publik, selama kuncinya dijaga kerahasiaannya, pesan tetap aman.

🕮 4.4 Kriptografi Simetris

Kriptografi simetris, juga dikenal sebagai **kriptografi kunci rahasia**, adalah metode di mana kunci yang sama digunakan untuk proses enkripsi dan dekripsi.

4.4.1 Konsep Dasar

Bayangkan Anda memiliki sebuah kotak surat dengan gembok. Anda membuat satu anak kunci. Anda menggunakan anak kunci itu untuk mengunci kotak (enkripsi) dan juga untuk membukanya kembali (dekripsi). Itulah analogi sederhana dari kriptografi simetris. Satu kunci untuk dua fungsi.

Prosesnya:

1. Pengirim menggunakan kunci rahasia (K) untuk mengenkripsi *plaintext* (P) menjadi *ciphertext* (C). Rumusnya: **C = Enkripsi(K, P)**
2. *Ciphertext* dikirim melalui jaringan (yang mungkin tidak aman).
3. Penerima menggunakan **kunci yang sama (K)** untuk mendekripsi *ciphertext* (C) kembali menjadi *plaintext* (P). Rumusnya: **P = Dekripsi(K, C)**

4.4.2 Kelebihan dan Kekurangan

Kelebihan	Kekurangan
Cepat dan efisien: Algoritma simetris dirancang untuk memproses data dalam jumlah besar dengan cepat. Cocok untuk enkripsi data di penyimpanan atau komunikasi real-time.	**Masalah distribusi kunci:** Kunci rahasia harus dikirimkan dari pengirim ke penerima melalui saluran yang aman. Jika saluran sudah aman, mengapa perlu enkripsi? Ini adalah "paradoks" dalam kriptografi simetris.
Kuat: Dengan kunci yang cukup panjang (misal 256-bit), algoritma simetris sangat sulit dipecahkan.	**Skalabilitas:** Dalam jaringan dengan banyak pengguna, jumlah kunci yang harus dikelola sangat besar. Untuk 100 orang yang ingin saling berkomunikasi secara aman, dibutuhkan ribuan kunci. Setiap pasangan komunikasi membutuhkan kunci unik.

4.4.3 Contoh Algoritma Simetris

- **DES (Data Encryption Standard):** Dikembangkan oleh IBM pada 1970-an. Menggunakan kunci 56-bit. Saat ini dianggap sudah tidak aman karena dapat dipecahkan dengan serangan *brute force* menggunakan komputer modern.
- **3DES (Triple DES):** Menerapkan algoritma DES sebanyak tiga kali untuk meningkatkan keamanan. Lebih aman dari DES, tetapi lebih lambat.
- **AES (Advanced Encryption Standard):** Standar enkripsi yang saat ini paling banyak digunakan di seluruh dunia. Digunakan oleh pemerintah AS, industri perbankan, dan berbagai aplikasi komersial. AES tersedia dalam tiga varian

panjang kunci: 128-bit, 192-bit, dan 256-bit. Semakin panjang kunci, semakin aman.

🕮 4.5 Kriptografi Asimetris

Kriptografi asimetris, juga dikenal sebagai **kriptografi kunci publik**, adalah metode yang menggunakan sepasang kunci yang berbeda secara matematis: **kunci publik** dan **kunci privat**.

4.5.1 Konsep Dasar

Kembali ke analogi kotak surat. Kali ini, kotak surat Anda memiliki desain khusus. Ada dua kunci:

- **Kunci Publik:** Kunci ini dapat Anda bagikan kepada siapa pun di dunia. Kunci ini berfungsi untuk **mengunci** kotak surat, tetapi tidak dapat membukanya. Siapa pun yang memiliki kunci publik dapat memasukkan surat ke dalam kotak dan menguncinya.
- **Kunci Privat:** Kunci ini Anda simpan sendiri dan tidak boleh diberikan kepada siapa pun. **Hanya kunci privat ini yang dapat membuka kotak surat.**

Prosesnya:

1. Penerima membuat sepasang kunci: kunci publik dan kunci privat. Kunci publik dikirimkan kepada pengirim (bisa melalui saluran tidak aman).
2. Pengirim menggunakan **kunci publik penerima** untuk mengenkripsi *plaintext* (P) menjadi *ciphertext* (C). Rumusnya: **C = Enkripsi(KunciPublik_Penerima, P)**
3. *Ciphertext* dikirim melalui jaringan.
4. Penerima menggunakan **kunci privatnya sendiri** untuk mendekripsi *ciphertext*(C) kembali menjadi *plaintext*(P). Rumusnya: **P=Dekripsi(KunciPrivat_Penerima, C)**

Pesan yang dienkripsi dengan kunci publik **hanya dapat** didekripsi dengan kunci privat yang berpasangan. Bahkan kunci publik itu sendiri tidak dapat digunakan untuk mendekripsi pesan.

4.5.2 Kelebihan dan Kekurangan

Kelebihan	Kekurangan
Menyelesaikan masalah distribusi kunci: Kunci publik dapat dikirimkan melalui saluran tidak aman. Tidak perlu ada saluran rahasia untuk bertukar kunci.	**Jauh lebih lambat:** Algoritma asimetris membutuhkan perhitungan matematis yang kompleks, sehingga puluhan hingga ratusan kali lebih lambat dibanding algoritma simetris. Tidak cocok untuk enkripsi data dalam jumlah besar.
Skalabilitas: Jumlah kunci yang dikelola jauh lebih sedikit. Setiap orang cukup memiliki satu pasang kunci (publik dan privat).	**Ukuran ciphertext lebih besar:** Hasil enkripsi asimetris biasanya lebih besar dari ukuran data aslinya.

4.5.3 Contoh Algoritma Asimetris

- **RSA (Rivest-Shamir-Adleman):** Algoritma kunci publik paling terkenal, dinamai sesuai nama penciptanya (Ron Rivest, Adi Shamir, Leonard Adleman) pada 1977. Keamanan RSA didasarkan pada sulitnya memfaktorkan bilangan besar hasil perkalian dua bilangan prima.
- **ECC (Elliptic Curve Cryptography):** Algoritma yang lebih baru dan menawarkan tingkat keamanan setara RSA dengan panjang kunci yang jauh lebih pendek. Banyak digunakan pada perangkat dengan sumber daya terbatas seperti ponsel dan perangkat IoT.

🕮 4.6 Perbandingan dan Penggunaan Praktis

Dalam praktiknya, kriptografi simetris dan asimetris tidak digunakan secara eksklusif, melainkan **dikombinasikan** untuk mendapatkan manfaat terbaik dari keduanya. Pendekatan ini disebut **Kriptografi Hibrida**.

Contoh: Protokol HTTPS (yang membuat gembok di browser Anda)

1. **Tahap 1 (Asimetris):** Browser Anda (klien) meminta kunci publik dari server website. Server mengirimkan kunci publiknya (dalam bentuk sertifikat digital).
2. **Tahap 2 (Pertukaran Kunci):** Browser membuat **kunci sesi (session key)** acak. Kunci sesi ini adalah kunci simetris yang akan digunakan untuk sesi komunikasi

kali ini saja. Browser mengenkripsi kunci sesi tersebut dengan **kunci publik server** dan mengirimkannya ke server.

3. **Tahap 3 (Dekripsi Kunci):** Server menggunakan **kunci privatnya** untuk mendekripsi pesan dan mendapatkan kunci sesi. Sekarang, kedua pihak memiliki kunci simetris yang sama.
4. **Tahap 4 (Komunikasi Simetris):** Untuk sisa sesi komunikasi, browser dan server menggunakan **kunci sesi** dan algoritma simetris (biasanya AES) untuk mengenkripsi semua data yang dikirim. Ini jauh lebih cepat.

Ringkasan:

- **Kriptografi Asimetris** digunakan untuk bertukar kunci secara aman (menyelesaikan masalah distribusi kunci).
- **Kriptografi Simetris** digunakan untuk mengenkripsi data aktual (karena cepat dan efisien).

💡 4.7 Studi Kasus: Analisis Penggunaan Kriptografi

Mari kita analisis bagaimana kriptografi diterapkan dalam tiga skenario umum.

Skenario 1: E-commerce (Transaksi Online)
Saat Anda berbelanja di Tokopedia, Shopee, atau Amazon, dan Anda masuk ke halaman *checkout*, perhatikan URL browser. Pasti diawali dengan **https://** (bukan http://). Huruf 's' itu singkatan dari *secure*.

- **Teknologi:** HTTPS (Hypertext Transfer Protocol Secure) yang menggunakan protokol SSL/TLS.
- **Kriptografi yang Digunakan:** Kombinasi asimetris (untuk *handshake* dan pertukaran kunci) dan simetris (untuk enkripsi data transaksi).
- **Tujuan:** Melindungi data sensitif seperti nomor kartu kredit, alamat, dan informasi pribadi lainnya agar tidak disadap saat dikirim dari browser ke server.

Skenario 2: Email (Layanan seperti Gmail)

Email pada dasarnya adalah sistem yang tidak aman. Pesan email melewati banyak server sebelum sampai ke tujuan. Untuk mengamankannya, digunakan protokol tambahan.

- **Teknologi:** S/MIME (Secure/Multipurpose Internet Mail Extensions) atau PGP (Pretty Good Privacy).
- **Kriptografi yang Digunakan:** Kombinasi asimetris dan simetris. Pengirim mengambil kunci publik penerima, mengenkripsi email (atau kunci simetris untuk email), dan mengirimkannya. Hanya penerima dengan kunci privat yang dapat membaca.
- **Tujuan:** Memastikan kerahasiaan email dan mengautentikasi bahwa email benar-benar berasal dari pengirim yang sah.

Skenario 3: Perbankan (Transaksi ATM dan Mobile Banking)

Saat Anda bertransaksi di ATM atau menggunakan aplikasi mobile banking, keamanan adalah prioritas utama.

- **Teknologi:** Berbagai protokol kepemilikan bank, seringkali menggunakan enkripsi end-to-end.
- **Kriptografi yang Digunakan:**
    - **PIN:** PIN Anda tidak pernah dikirim dalam bentuk aslinya. PIN dienkripsi (sering dengan algoritma simetris seperti 3DES atau AES) sebelum dikirim ke server.
    - **Data Transaksi:** Semua data transaksi (nomor rekening tujuan, jumlah uang) dienkripsi.
- **Tujuan:** Mencegah pencurian data transaksi dan melindungi PIN nasabah dari penyadapan.

🗝 4.8 Rangkuman

1. **Kriptografi** adalah seni dan ilmu menjaga kerahasiaan pesan dengan mengubahnya menjadi format yang tidak dapat dipahami.
2. Tujuan kriptografi: Kerahasiaan, Integritas, Autentikasi, dan Non-Repudiasi.
3. **Kriptografi Simetris** menggunakan satu kunci untuk enkripsi dan dekripsi. Cepat, tetapi memiliki masalah distribusi kunci. Contoh: AES.
4. **Kriptografi Asimetris** menggunakan sepasang kunci: publik (untuk enkripsi) dan privat (untuk dekripsi). Memecahkan masalah distribusi kunci, tetapi lambat. Contoh: RSA.
5. Dalam praktiknya, **kriptografi hibrida** menggabungkan keduanya: asimetris untuk pertukaran kunci, simetris untuk enkripsi data.

✍ 4.9 Latihan Soal

1. Jelaskan perbedaan mendasar antara kriptografi simetris dan asimetris dari segi jumlah kunci, kecepatan, dan masalah distribusi kunci.
2. Mengapa protokol HTTPS menggunakan kombinasi kriptografi simetris dan asimetris, bukan hanya salah satunya saja?
3. Jika Anda diminta memilih algoritma untuk mengenkripsi hard disk eksternal berkapasitas 1 TB, apakah Anda akan memilih AES atau RSA? Jelaskan alasan Anda.

📝 4.10 Tugas Mandiri (Bobot 2%)

Instruksi:

Buatlah laporan analisis singkat tentang penggunaan kriptografi dalam tiga skenario aplikasi nyata: e-commerce, email, dan perbankan (seperti contoh di sub-bab 4.7).

Langkah Tugas:

1. Untuk setiap skenario, identifikasi **teknologi/protokol** yang digunakan (misal: HTTPS, PGP, dll.).
2. Jelaskan **jenis kriptografi** (simetris, asimetris, atau kombinasi) yang digunakan dan **bagaimana** penerapannya.
3. Analisis **kelebihan** dan **potensi kelemahan** dari implementasi kriptografi di setiap skenario.
4. Berikan **rekomendasi perbaikan** jika Anda menemukan potensi kelemahan.

Format Penugasan:

- Ditulis dalam bentuk tabel atau narasi per skenario.
- Dikumpulkan dalam format PDF.

BAB 5
FUNGSI HASH DAN TANDA TANGAN DIGITAL

🎯 Kemampuan Akhir (Sub-CPMK 2.2)

Setelah mempelajari bab ini, mahasiswa mampu:

1. Menjelaskan konsep fungsi hash kriptografi dan sifat-sifatnya.
2. Menganalisis penggunaan fungsi hash untuk verifikasi integritas data.
3. Menjelaskan konsep tanda tangan digital (*digital signature*) dan cara kerjanya.
4. Mengevaluasi implementasi tanda tangan digital dalam dokumen elektronik.

🕮 5.1 Pendahuluan: Sidik Jari Digital

Pada bab sebelumnya, kita belajar tentang enkripsi yang bertujuan untuk **menyembunyikan** pesan. Namun, bagaimana jika kita tidak perlu menyembunyikan pesannya, tetapi kita hanya perlu memastikan bahwa pesan tersebut **tidak diubah** sejak dibuat? Atau kita perlu membuktikan bahwa pesan tersebut benar-benar berasal dari pengirim yang sah?

Di sinilah peran **fungsi hash** dan **tanda tangan digital**. Keduanya tidak dirancang untuk menyembunyikan pesan, tetapi untuk menjaga **integritas** dan **autentikasi**. Anggap saja ini seperti "sidik jari" digital atau "meterai" elektronik yang melekat pada data.

🕮 5.2 Fungsi Hash Kriptografi

Fungsi hash kriptografi adalah algoritma matematis yang mengubah input dengan ukuran berapa pun (file, teks, video) menjadi output dengan ukuran tetap yang disebut **nilai hash**, **message digest**, atau **sidik jari digital**.

5.2.1 Karakteristik Fungsi Hash

Agar berguna untuk keamanan, sebuah fungsi hash harus memiliki sifat-sifat berikut:

1. **Deterministik:** Input yang sama akan selalu menghasilkan nilai hash yang sama.
2. **Cepat:** Proses hash harus cepat untuk input berapa pun.
3. **One-Way Function (Fungsi Satu Arah):** Dari nilai hash, sangat sulit (praktis tidak mungkin) untuk merekayasa ulang (*reverse engineering*) menjadi input aslinya. Anda tidak bisa mengubah "sidik jari" kembali menjadi "orangnya".
4. **Tahan Tabrakan (Collision Resistant):** Sangat sulit untuk menemukan dua input yang berbeda (A dan B) yang menghasilkan nilai hash yang sama.
5. **Avalanche Effect (Efek Longsor):** Perubahan kecil pada input, bahkan hanya satu bit, harus menghasilkan perubahan yang signifikan dan tidak terduga pada nilai hash (sekitar setengah bit berubah).

5.2.2 Analogi Sederhana

Bayangkan Anda memiliki mesin penghitung jumlah halaman. Setiap buku yang Anda masukkan ke mesin, akan keluar angka berupa jumlah halaman buku tersebut.

- Jika Anda memasukkan buku "A" setebal 250 halaman, keluar angka "250".
- Jika Anda memasukkan buku "B" setebal 250 halaman yang berbeda, keluar angka yang sama, "250". (Ini tabrakan! padahal isi buku berbeda).
- Jika Anda mengubah satu kata di halaman 100 buku "A", jumlah halamannya tetap 250. (Tidak ada efek longsor).

Mesin penghitung halaman ini adalah **hash yang buruk** untuk keamanan. Fungsi hash kriptografi yang baik harus bisa membedakan buku "A" dan buku "B" yang sama tebalnya, dan harus peka terhadap perubahan sekecil apa pun.

5.2.3 Contoh Algoritma Hash

- **MD5 (Message Digest 5):** Menghasilkan hash 128-bit. Dulu sangat populer, tetapi sekarang sudah dianggap **tidak aman** karena telah ditemukan kerentanannya (tabrakan dapat dibuat dengan sengaja).
- **SHA (Secure Hash Algorithm):** Dikembangkan oleh NSA.
    - **SHA-1:** Menghasilkan hash 160-bit. Saat ini juga sudah dianggap **tidak aman**.
    - **SHA-2:** Keluarga algoritma yang lebih aman, termasuk SHA-224, SHA-256, SHA-384, SHA-512 (angka menunjukkan panjang hash dalam bit). SHA-256 sangat umum digunakan saat ini.
    - **SHA-3:** Standar terbaru, dirancang sebagai cadangan jika SHA-2 suatu saat ditemukan kelemahan.

5.2.4 Aplikasi Fungsi Hash

1. **Verifikasi Integritas File:** Saat Anda mengunduh file besar (misal: ISO Linux, installer software), situs web biasanya mencantumkan nilai hash (SHA-256) dari file tersebut. Setelah unduh, Anda dapat menghitung hash file yang Anda terima dan membandingkannya dengan hash yang dicantumkan. Jika sama, file Anda utuh dan tidak rusak atau disusupi malware.
2. **Penyimpanan Kata Sandi:** Situs web yang baik **tidak pernah** menyimpan kata sandi Anda dalam bentuk aslinya (*plaintext*). Mereka menyimpan nilai hash dari kata sandi Anda. Saat Anda login, sistem menghitung hash dari kata sandi yang Anda ketik, lalu membandingkannya dengan hash yang tersimpan di database. Jika serangan terjadi dan database bocor, penyerang hanya mendapatkan nilai hash, bukan kata sandi asli.
3. **Deteksi Duplikasi Data:** Sistem penyimpanan dapat menggunakan hash untuk mendeteksi apakah file yang sama sudah pernah disimpan.

🕮 5.3 Tanda Tangan Digital (Digital Signature)

Tanda tangan digital adalah mekanisme kriptografi yang setara dengan tanda tangan basah di dunia fisik, tetapi untuk dokumen elektronik. Tanda tangan digital memberikan:

- **Autentikasi:** Membuktikan bahwa dokumen benar-benar ditandatangani oleh pengirim yang sah.
- **Integritas:** Membuktikan bahwa dokumen tidak diubah setelah ditandatangani.
- **Non-Repudiasi:** Pengirim tidak dapat menyangkal bahwa ia telah menandatangani dokumen tersebut.

5.3.1 Cara Kerja Tanda Tangan Digital

Tanda tangan digital menggabungkan **fungsi hash** dan **kriptografi asimetris**. Perhatikan bahwa prosesnya berbeda dengan enkripsi.

Proses Penandatanganan (oleh Pengirim):

1. Pengirim memiliki dokumen (P).
2. Pengirim menghitung **nilai hash** dari dokumen tersebut, misal menggunakan SHA-256. Hasilnya adalah **H = Hash(P)**.
3. Pengirim mengenkripsi **nilai hash H** dengan **kunci privatnya sendiri**. Hasil enkripsi inilah yang disebut **tanda tangan digital (S)**. Rumus: **S = Enkripsi(KunciPrivat_Pengirim, H)**
4. Pengirim mengirimkan **dokumen asli (P)** bersama dengan **tanda tangan digital (S)** kepada penerima. Dokumen P dikirim dalam bentuk *plaintext* (tidak dienkripsi). Yang penting adalah tanda tangannya.

Proses Verifikasi (oleh Penerima):

1. Penerima menerima dokumen (P) dan tanda tangan digital (S).
2. Penerima menghitung sendiri **nilai hash** dari dokumen yang diterima, menggunakan algoritma hash yang sama. Hasilnya **H1 = Hash(P)**.
3. Penerima mendekripsi **tanda tangan digital (S)** yang diterima menggunakan **kunci publik pengirim**. Hasil dekripsi ini adalah nilai hash yang ditandatangani oleh pengirim, sebut saja **H2**. Rumus: **H2 = Dekripsi(KunciPublik_Pengirim, S)**

4. Penerima membandingkan **H1** (hash dari dokumen yang diterima) dan **H2** (hash dari dokumen asli yang ditandatangani pengirim).
    - **Jika H1 = H2:** Tanda tangan **valid**. Artinya, dokumen tidak berubah (integritas terjaga) dan benar-benar ditandatangani oleh pemilik kunci privat yang sesuai dengan kunci publik yang digunakan (autentikasi terpenuhi).
    - **Jika H1 ≠ H2:** Tanda tangan **tidak valid**. Artinya, dokumen telah diubah setelah ditandatangani, atau tanda tangan tersebut palsu.

5.3.2 Perbedaan dengan Enkripsi

Penting untuk tidak mencampuradukkan tanda tangan digital dengan enkripsi.

- **Enkripsi** menggunakan **kunci publik penerima** untuk menjaga **kerahasiaan**.
- **Tanda Tangan Digital** menggunakan **kunci privat pengirim** untuk menjaga **integritas dan autentikasi**, tanpa menyembunyikan isi dokumen.

💡 5.4 Studi Kasus: Implementasi Tanda Tangan Digital

Kasus 1: Distribusi Perangkat Lunak (Software Distribution)

Perusahaan seperti Microsoft atau pengembang aplikasi open source sering menandatangani kode (*code signing*) aplikasi mereka.

- **Skenario:** Anda ingin mengunduh aplikasi "Video Editor Pro" dari situs web resminya.
- **Proses:**
    1. Pengembang menghitung hash dari file installer "video_editor_pro.exe".
    2. Pengembang menandatangani hash tersebut dengan kunci privatnya.
    3. File installer dan tanda tangan digital diunggah ke server.
    4. Anda mengunduh file installer. Sistem operasi Anda (Windows, macOS) secara otomatis memverifikasi tanda tangan digital menggunakan kunci publik pengembang yang sudah tertanam di sistem.
- **Hasil:** Jika verifikasi berhasil, Anda akan melihat pesan "Publisher yang diverifikasi: Nama Pengembang". Jika gagal, Anda akan mendapat peringatan

bahwa file tidak aman. Ini melindungi Anda dari menginstal aplikasi palsu yang mengandung malware.

Kasus 2: Kontrak Digital dan Dokumen Elektronik

Di Indonesia, tanda tangan digital telah diakui secara hukum melalui UU ITE. Layanan seperti PrivyID, Digisign, atau Adobe Sign digunakan untuk menandatangani kontrak secara digital.

- **Skenario:** Sebuah perusahaan ingin menandatangani kontrak kerja sama dengan vendor. Kedua pihak berada di kota berbeda.
- **Proses:**
    1. Dokumen kontrak (PDF) diunggah ke platform tanda tangan digital.
    2. Pihak pertama menandatangani secara digital (menggunakan kunci privatnya). Platform menambahkan lapisan keamanan dengan menghitung hash dokumen dan mengenkripsinya.
    3. Pihak kedua menerima notifikasi, membaca dokumen, dan juga menandatangani secara digital.
    4. Dokumen yang telah ditandatangani memiliki "seg el" yang membuktikan keasliannya. Jika ada yang mengubah satu kata pun dalam PDF setelah ditandatangani, segel akan rusak dan tanda tangan menjadi tidak valid.
- **Hasil:** Kontrak sah secara hukum, menghemat waktu dan biaya, dan memiliki tingkat keamanan yang lebih tinggi daripada dokumen fisik yang mudah dipalsukan.

🗝 5.5 Rangkuman

1. **Fungsi hash kriptografi** adalah fungsi satu arah yang menghasilkan "sidik jari" digital unik untuk setiap input. Sifatnya: deterministik, cepat, satu arah, tahan tabrakan, dan efek longsor.
2. Fungsi hash digunakan untuk verifikasi integritas file dan penyimpanan kata sandi yang aman. Contoh algoritma: SHA-256.
3. **Tanda tangan digital** adalah mekanisme untuk membuktikan autentikasi, integritas, dan non-repudiasi dokumen elektronik.

4. Tanda tangan digital bekerja dengan menggabungkan **fungsi hash** (untuk meringkas dokumen) dan **kriptografi asimetris** (untuk menandatangani hash dengan kunci privat).
5. Verifikasi dilakukan dengan mendekripsi tanda tangan menggunakan **kunci publik** dan membandingkannya dengan hash dokumen yang diterima.
6. Tanda tangan digital banyak digunakan dalam distribusi perangkat lunak dan kontrak elektronik.

✍ 5.6 Latihan Soal

1. Sebutkan tiga sifat fungsi hash kriptografi dan jelaskan mengapa setiap sifat itu penting.
2. Jelaskan perbedaan tujuan antara fungsi hash dan enkripsi.
3. Dalam proses tanda tangan digital, mengapa yang dienkripsi adalah nilai hash, bukan seluruh dokumen?
4. Apa yang terjadi jika seorang penyerang berhasil mengganti kunci publik seseorang dengan kunci publik palsu? Ancaman apa yang mungkin muncul?

📝 5.7 Tugas Mandiri (Bobot 2%)

Instruksi:
Lakukan analisis terhadap penggunaan fungsi hash dan tanda tangan digital.

Langkah Tugas:

1. **Verifikasi Integritas File:**
   - Pilih satu file berukuran kecil (misal: file PDF tugas atau gambar).
   - Gunakan tools online atau aplikasi (seperti CertUtil di Windows atau `shasum` di Linux/Mac) untuk menghitung nilai hash SHA-256 dari file tersebut. Catat hasilnya.

- Ubah sedikit file tersebut (misal: tambahkan satu spasi atau hapus satu karakter). Hitung lagi nilai hash SHA-256-nya.
- Bandingkan kedua nilai hash tersebut. Apa yang terjadi? Mengapa? Sertakan screenshot hasil hash.

2. **Analisis Tanda Tangan Digital:**
   - Cari informasi tentang salah satu penyedia layuran tanda tangan digital yang beroperasi di Indonesia (misal: PrivyID, Digisign, atau lainnya).
   - Jelaskan bagaimana layanan tersebut menggunakan konsep kriptografi yang Anda pelajari (hash, kunci privat-publik) untuk memberikan jaminan keamanan.
   - Identifikasi satu kelebihan dan satu potensi risiko dari penggunaan layanan tersebut.

Format Penugasan:

- Laporan dalam format PDF, dilengkapi screenshot.
- Sertakan tautan ke sumber informasi layanan tanda tangan digital yang Anda analisis.

BAB 6
INFRASTRUKTUR KUNCI PUBLIK (PKI)

🎯 Kemampuan Akhir (Sub-CPMK 2.3)

Setelah mempelajari bab ini, mahasiswa mampu:

1. Menjelaskan komponen-komponen utama dalam Infrastruktur Kunci Publik (PKI).
2. Menganalisis hierarki kepercayaan (*chain of trust*) dalam PKI.
3. Mengevaluasi implementasi SSL/TLS pada website melalui analisis sertifikat digital.
4. Mengidentifikasi potensi kerentanan dalam implementasi PKI.

🕮 6.1 Pendahuluan: Masalah Kunci Publik

Di Bab 4, kita belajar tentang kriptografi asimetris yang memecahkan masalah distribusi kunci. Pengirim dapat mengenkripsi pesan menggunakan kunci publik penerima yang dikirim melalui saluran tidak aman.

Namun, muncul pertanyaan baru: **Bagaimana penerima yakin bahwa kunci publik yang diterimanya benar-benar milik orang yang dituju, dan bukan kunci palsu yang dibuat oleh penyerang?**

Bayangkan skenario ini:

1. Anda ingin mengirim pesan rahasia ke teman Anda, Budi.
2. Budi mengirimkan kunci publiknya kepada Anda. Namun, di tengah jalan, seorang penyerang bernama Charlie menyadap pesan tersebut. Charlie mengganti kunci publik Budi dengan **kunci publik Charlie sendiri**.

3. Anda menerima "kunci publik" yang Anda kira milik Budi, padahal itu milik Charlie.
4. Anda mengenkripsi pesan dengan kunci publik Charlie dan mengirimkannya.
5. Charlie menyadap pesan tersebut, mendekripsinya dengan kunci privatnya, membaca pesan Anda, lalu mengenkripsinya ulang dengan kunci publik Budi yang asli, dan mengirimkannya ke Budi.
6. Budi menerima pesan dan mendekripsinya dengan kunci privatnya. Budi tidak tahu bahwa pesannya telah dibaca Charlie. Anda juga tidak tahu bahwa kunci publik Anda telah dipalsukan.

Serangan ini dikenal sebagai **Man-in-the-Middle (MitM)** . Untuk mengatasinya, kita membutuhkan pihak ketiga yang terpercaya yang dapat "menjamin" bahwa sebuah kunci publik benar-benar milik entitas yang diklaim. Di sinilah peran **PKI**.

PKI (Public Key Infrastructure) adalah sistem yang terdiri dari perangkat keras, perangkat lunak, kebijakan, prosedur, dan orang-orang yang diperlukan untuk membuat, mengelola, mendistribusikan, menggunakan, menyimpan, dan mencabut sertifikat digital.

🕮 6.2 Komponen Utama PKI

PKI memiliki beberapa komponen kunci yang bekerja bersama:

6.2.1 Sertifikat Digital (Digital Certificate)

Sertifikat digital adalah dokumen elektronik yang mengikat sebuah kunci publik dengan identitas entitas pemiliknya (misal: nama orang, nama organisasi, nama domain website). Sertifikat ini diterbitkan dan ditandatangani oleh *Certificate Authority*.

Isi sertifikat digital (berdasarkan standar X.509) antara lain:

- **Versi:** Versi standar X.509.
- **Nomor Seri:** Nomor unik yang diberikan oleh penerbit.

- **Informasi Pemilik (Subject):** Identitas pemilik, seperti Common Name (CN) untuk domain (misal: www.contoh.com), Organisasi (O), dll.
- **Informasi Penerbit (Issuer):** Identitas CA yang menerbitkan sertifikat.
- **Masa Berlaku:** Tanggal mulai dan tanggal berakhir sertifikat.
- **Kunci Publik Pemilik:** Kunci publik yang "diikat" dengan identitas pemilik.
- **Tanda Tangan Digital Penerbit:** Tanda tangan dari CA yang menjamin keaslian seluruh isi sertifikat.

Analogi: Sertifikat digital seperti **KTP elektronik** atau **paspor**. KTP membuktikan bahwa foto dan identitas di dalamnya benar-benar milik Anda, karena diterbitkan dan ditandatangani oleh Dinas Kependudukan dan Pencatatan Sipil (yang merupakan pihak berwenang). Demikian pula, sertifikat digital membuktikan bahwa kunci publik di dalamnya benar-benar milik entitas tersebut, karena diterbitkan dan ditandatangani oleh CA.

6.2.2 Certificate Authority (CA)

Certificate Authority (CA) adalah entitas tepercaya yang menerbitkan dan mengelola sertifikat digital. CA adalah "Dinas Kependudukan"-nya dunia digital. Contoh CA terkenal: DigiCert, Let's Encrypt, GlobalSign, Verisign.

Tugas utama CA:

- Memverifikasi identitas pemohon sertifikat (sejauh apa verifikasi dilakukan tergantung pada jenis sertifikat).
- Menerbitkan sertifikat dengan menandatanganinya secara digital menggunakan kunci privat CA.
- Menyediakan mekanisme pencabutan sertifikat melalui **CRL (Certificate Revocation List)** atau **OCSP (Online Certificate Status Protocol)**.
- Memelihara dan mempublikasikan kunci publik CA sendiri agar dapat digunakan oleh siapa pun untuk memverifikasi sertifikat yang diterbitkannya.

6.2.3 Registration Authority (RA)

Registration Authority (RA) adalah komponen opsional yang bertugas sebagai perpanjangan tangan CA. RA bertanggung jawab untuk menerima permintaan sertifikat, memverifikasi identitas pemohon, tetapi **tidak** menerbitkan sertifikat.

Setelah verifikasi selesai, RA meneruskan permintaan ke CA untuk diterbitkan sertifikatnya. Ini membantu CA untuk fokus pada tugas intinya.

6.2.4 Subscriber dan Relying Party

- **Subscriber:** Entitas yang meminta dan menerima sertifikat dari CA (misal: pemilik website).
- **Relying Party:** Entitas yang mengandalkan sertifikat untuk berkomunikasi dengan subscriber (misal: pengunjung website). *Relying party* harus mempercayai CA yang menerbitkan sertifikat tersebut.

🕮 6.3 Hirarki Kepercayaan (Chain of Trust)

Sertifikat digital tidak berdiri sendiri. Mereka membentuk rantai kepercayaan yang disebut **Chain of Trust**.

Rantai ini biasanya terdiri dari tiga tingkatan:

1. **Root CA (Root Certificate):** Ini adalah CA tingkat atas, yang paling tepercaya. Sertifikat Root CA adalah **self-signed** (ditandatangani sendiri). Kunci publik Root CA sudah tertanam di dalam browser, sistem operasi, atau *trust store* perangkat Anda. Jika Root CA tidak aman, seluruh sistem PKI runtuh.
2. **Intermediate CA (Intermediate Certificate):** Root CA tidak menerbitkan sertifikat untuk publik secara langsung. Ini terlalu berisiko. Root CA menerbitkan sertifikat untuk *Intermediate CA*, yang bertindak sebagai perantara. Jika kunci privat Intermediate CA bocor, Root CA dapat mencabut sertifikat Intermediate CA tersebut tanpa harus membuat ulang seluruh sistem.
3. **End-Entity Certificate (Leaf Certificate):** Ini adalah sertifikat yang diterbitkan oleh Intermediate CA untuk entitas akhir, seperti website (www.contoh.com).

Proses Verifikasi oleh Browser:
Saat Anda mengunjungi website dengan HTTPS, browser Anda menerima sertifikat leaf website tersebut. Browser kemudian:

1. Melihat siapa penerbit (*issuer*) sertifikat leaf. Misal: "R3" (Intermediate CA Let's Encrypt).

2. Browser mencari sertifikat Intermediate CA "R3". Sertifikat ini biasanya juga dikirim oleh server bersama sertifikat leaf.
3. Sertifikat Intermediate "R3" diterbitkan oleh Root CA, misal "ISRG Root X1".
4. Browser mencari sertifikat Root "ISRG Root X1" di *trust store*-nya. Karena Root CA sudah tertanam dan dipercaya, browser menggunakan kunci publik Root untuk memverifikasi tanda tangan pada sertifikat Intermediate.
5. Setelah Intermediate terverifikasi, browser menggunakan kunci publik Intermediate untuk memverifikasi tanda tangan pada sertifikat leaf website.
6. Jika seluruh rantai terverifikasi dan valid, koneksi aman dapat dibuat. Jika salah satu mata rantai putus (misal: sertifikat kadaluarsa, penerbit tidak dikenal), browser akan menampilkan peringatan.

🕮 6.4 Jenis-Jenis Sertifikat SSL/TLS

Dalam konteks website, sertifikat digital yang digunakan sering disebut **sertifikat SSL/TLS**. Ada beberapa jenis berdasarkan tingkat validasi:

Jenis Sertifikat	Tingkat Validasi	Indikator di Browser	Penggunaan
DV (Domain Validation)	**Rendah.** CA hanya memverifikasi bahwa pemohon memiliki kontrol atas domain (misal: dengan mengirim email ke admin@domain.com). Proses otomatis, cepat, dan gratis (seperti Let's Encrypt).	Gembok saja.	Blog, website informasi, UKM yang membutuhkan enkripsi dasar.
OV (Organization Validation)	**Sedang.** CA memverifikasi kepemilikan domain **dan** keberadaan organisasi (nama, alamat, nomor telepon terdaftar). Proses lebih lama.	Gembok, dan informasi organisasi dapat dilihat di detail sertifikat.	Situs e-commerce, perusahaan yang ingin menunjukkan kredibilitas.
EV (Extended Validation)	**Tinggi.** Proses verifikasi paling ketat. CA melakukan pengecekan legal, fisik, dan operasional organisasi. Proses bisa memakan waktu berminggu-minggu.	Di browser lama, URL berwarna hijau dan nama organisasi muncul. Di browser baru,	Bank, institusi keuangan, perusahaan besar yang sangat sensitif terhadap phishing.

Jenis Sertifikat	Tingkat Validasi	Indikator di Browser	Penggunaan
		tetap gembok, tetapi dengan reputasi lebih tinggi.	

💡 6.5 Studi Kasus: Analisis Sertifikat SSL pada Website

Mari kita praktikkan analisis sederhana terhadap sertifikat SSL sebuah website.

Langkah-langkah (di Google Chrome):

1. Buka website yang menggunakan HTTPS, misal: **https://www.bni.co.id** (situs bank) dan **https://www.tokopedia.com** (situs e-commerce).
2. Klik ikon **gembok** di sebelah kiri alamat URL.
3. Klik **"Koneksi aman"** lalu **"Ikon gembok"** atau **"Sertifikat (Valid)"** (tergantung versi browser).
4. Akan muncul jendela informasi sertifikat. Amati beberapa hal berikut:

Informasi yang Dianalisis	Contoh pada Bank (BNI)	Contoh pada E-commerce (Tokopedia)
Dikeluarkan Untuk (Subject)	CN = www.bni.co.id	CN = tokopedia.com (atau *.tokopedia.com)
Dikeluarkan Oleh (Issuer)	DigiCert Inc (kemungkinan EV)	Let's Encrypt (kemungkinan DV)
Masa Berlaku	Tanggal berlaku dan tanggal kadaluarsa.	Tanggal berlaku dan tanggal kadaluarsa.
Jenis Sertifikat	Biasanya OV atau EV. Terlihat dari detail organisasi yang lengkap di Subject.	Biasanya DV. Informasi organisasi mungkin tidak ada.
Rantai Sertifikat	Tab "Rantai Sertifikat" akan menunjukkan hierarki: Leaf -> Intermediate -> Root.	Tab "Rantai Sertifikat" akan menunjukkan hierarki yang sama.

Apa yang Dapat Disimpulkan?

- **Bank (BNI):** Menggunakan sertifikat dengan validasi lebih tinggi (OV/EV) karena sangat penting untuk mencegah phishing. Pengunjung perlu kepastian bahwa situs yang mereka akses benar-benar milik Bank BNI.
- **E-commerce (Tokopedia):** Menggunakan sertifikat DV (banyak yang beralih ke Let's Encrypt yang gratis). Untuk situs sebesar Tokopedia, ini menunjukkan bahwa enkripsi (HTTPS) sudah dianggap cukup, dan reputasi merek sudah sangat kuat sehingga pengguna tidak terlalu bergantung pada informasi organisasi di sertifikat.

🕮 6.6 Potensi Kerentanan dan Kelemahan PKI

Meskipun PKI adalah fondasi keamanan internet, sistem ini tidak sempurna. Beberapa potensi kerentanan:

1. **CA yang Dikompromikan:** Jika kunci privat sebuah CA (terutama Root CA) bocor, penyerang dapat menerbitkan sertifikat palsu untuk domain mana pun. Ini adalah skenario mimpi buruk. Contoh: Kasus DigiNotar (2011) di mana CA Belanda ini diretas dan menerbitkan sertifikat palsu untuk Google, Yahoo, dll. Akibatnya, DigiNotar bangkrut.
2. **Sertifikat yang Dicuri:** Penyerang dapat mencuri kunci privat dan sertifikat dari server korban, lalu menggunakannya untuk membuat server palsu yang tampak sah.
3. **Sertifikat Kadaluarsa dan Pencabutan:** Mekanisme pencabutan sertifikat (CRL/OCSP) tidak selalu berjalan sempurna. Beberapa browser mungkin mengabaikan pemeriksaan pencabutan demi kecepatan, sehingga sertifikat yang sudah dicabut masih bisa digunakan untuk sementara.
4. **Serangan terhadap Pengguna:** *Phishing* masih menjadi ancaman besar. Penyerang tidak perlu merusak PKI; mereka cukup membuat website palsu dengan nama domain mirip (contoh: go0gle.com) dan membeli sertifikat DV murah untuk domain tersebut. Pengguna yang tidak jeli akan melihat gembok dan mengira situs itu aman.

🗝 6.7 Rangkuman

1. **PKI** adalah infrastruktur yang diperlukan untuk mengelola kepercayaan dalam komunikasi digital, terutama melalui **sertifikat digital**.
2. **Sertifikat digital** berfungsi seperti KTP elektronik yang mengikat **kunci publik** dengan **identitas** pemiliknya.
3. Komponen utama PKI: **Sertifikat Digital**, **Certificate Authority (CA)** , **Registration Authority (RA)** .
4. **Chain of Trust** adalah hierarki sertifikat yang memungkinkan verifikasi berantai dari *end-entity certificate* hingga ke *Root CA* yang sudah tertanam dan dipercaya oleh sistem.
5. Sertifikat SSL/TLS untuk website memiliki tingkat validasi berbeda: **DV** (hanya validasi domain), **OV** (validasi organisasi), dan **EV** (validasi diperpanjang).
6. PKI bukannya tanpa kelemahan. Ancaman seperti CA yang diretas atau sertifikat palsu tetap ada, meskipun risikonya relatif kecil.

✍ 6.8 Latihan Soal

1. Jelaskan fungsi utama dari Certificate Authority (CA) dalam PKI.
2. Apa yang dimaksud dengan *Chain of Trust*? Mengapa Root CA tidak langsung menerbitkan sertifikat untuk pengguna akhir?
3. Sebutkan perbedaan antara sertifikat DV, OV, dan EV. Jenis sertifikat apa yang paling cocok untuk situs perbankan online? Mengapa?
4. Apa yang terjadi jika sebuah Certificate Authority (CA) besar diretas dan kunci privatnya dicuri?

📝 6.9 Tugas Mandiri (Bobot 2%)

Instruksi:

Lakukan analisis terhadap implementasi SSL/TLS pada beberapa website.

Langkah Tugas:

1. Pilih **tiga website** dari kategori berbeda, misal:
    - Situs perbankan (contoh: bca.co.id, mandiri.co.id)
    - Situs e-commerce besar (contoh: shopee.co.id, lazada.co.id)
    - Situs pemerintah (contoh: kemendagri.go.id, pajak.go.id)
2. Untuk setiap website, lakukan analisis sertifikat SSL (lihat panduan di sub-bab 6.5) dan catat informasi berikut:
    - **Issuer (Penerbit):** CA apa yang menerbitkan?
    - **Subject (Pemilik):** Domain apa yang dilindungi? Apakah ada informasi organisasi?
    - **Masa Berlaku:** Kapan berlaku dan kadaluarsa?
    - **Chain of Trust:** Sebutkan rantai sertifikatnya (Leaf -> Intermediate -> Root).
    - **Jenis Sertifikat:** Menurut Anda, apakah ini DV, OV, atau EV? Berikan alasan.
3. Berikan **evaluasi singkat** untuk setiap website. Apakah implementasinya sudah baik? Apakah ada potensi masalah (misal: sertifikat mendekati kadaluarsa, rantai tidak lengkap)?
4. **Kesimpulan:** Bandingkan ketiga website tersebut. Adakah perbedaan signifikan dalam kualitas atau jenis sertifikat yang mereka gunakan? Mengapa menurut Anda demikian?

Format Penugasan:

- Laporan dalam format PDF.
- Sertakan screenshot detail sertifikat untuk setiap website sebagai bukti.

📚 DAFTAR PUSTAKA

- Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.
- Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.
- Easttom, C. (2021). *Computer Security Fundamentals* (5th ed.). Pearson.
- OWASP Foundation. (2021). *OWASP Top Ten - 2021*. The Open Web Application Security Project. (Untuk konteks keamanan aplikasi).
- Dokumentasi dan publikasi dari Let's Encrypt, DigiCert, dan otoritas sertifikat lainnya.

BAGIAN 3
MANAJEMEN RISIKO DAN KEBIJAKAN KEAMANAN

BAB 7
ANALISIS RISIKO KEAMANAN INFORMASI

🎯 Kemampuan Akhir (Sub-CPMK 3.1)

Setelah mempelajari bab ini, mahasiswa mampu:

1. Menjelaskan konsep dasar manajemen risiko keamanan informasi.
2. Melakukan identifikasi aset informasi dalam organisasi.
3. Melakukan penilaian risiko kualitatif dengan menggunakan skala *likelihood* dan *impact*.
4. Membuat dan memaknai matriks risiko.
5. Menentukan prioritas penanganan risiko dan opsi perlakuan risiko.

🕮 7.1 Pendahuluan: Hidup dalam Ketidakpastian

Setiap hari, kita mengambil risiko. Saat menyebrang jalan, kita mengambil risiko tertabrak kendaraan. Saat berinvestasi, kita mengambil risiko kerugian. Saat memutuskan untuk tidak membawa payung, kita mengambil risiko kehujanan. Namun, kita tidak pernah benar-benar menghilangkan risiko tersebut. Kita hanya mengelolanya: melihat ke kiri-kanan sebelum menyebrang, melakukan riset sebelum investasi, atau melihat prakiraan cuaca.

Demikian pula dengan organisasi. Tidak mungkin menghilangkan 100% risiko keamanan informasi. Anggaran terbatas, sumber daya terbatas, dan ancaman terus berkembang. Pertanyaannya bukan **"Apakah kita bisa menghilangkan semua risiko?"**, tetapi **"Risiko mana yang harus kita prioritaskan untuk ditangani dengan sumber daya yang ada?"**

Inilah inti dari **manajemen risiko keamanan informasi**: proses sistematis untuk memahami, mengevaluasi, dan mengelola risiko terhadap aset informasi organisasi.

🕮 7.2 Konsep Dasar Manajemen Risiko

Sebelum melangkah lebih jauh, kita perlu memahami beberapa istilah kunci dalam manajemen risiko:

Istilah	Definisi	Analogi
Aset (Asset)	Sesuatu yang bernilai bagi organisasi dan perlu dilindungi.	Rumah Anda beserta isinya.
Ancaman (Threat)	Potensi penyebab kerugian atau kerusakan pada aset.	Pencuri, kebakaran, banjir.
Kerentanan (Vulnerability)	Kelemahan pada aset atau sistem yang dapat dieksploitasi oleh ancaman.	Pintu rumah yang tidak dikunci, kunci yang mudah rusak.
Risiko (Risk)	Kemungkinan (probabilitas) terjadinya ancaman yang mengeksploitasi kerentanan, dikalikan dengan dampak yang ditimbulkan. **Risiko = (Likelihood × Impact)** .	Seberapa besar kemungkinan pencuri masuk melalui pintu yang tidak dikunci, dan seberapa besar kerugian jika itu terjadi.
Perlakuan Risiko (Risk Treatment)	Langkah-langkah yang diambil untuk mengurangi, mentransfer, menghindari, atau menerima risiko.	Memasang kunci tambahan, membeli asuransi, memindahkan barang berharga ke bank, atau menerima risiko karena barang tidak berharga.

7.2.1 Rumus Dasar Risiko

Rumus fundamental dalam manajemen risiko adalah:

Risiko = Kemungkinan (Likelihood) × Dampak (Impact)

- **Kemungkinan (Likelihood):** Seberapa besar kemungkinan ancaman akan mengeksploitasi kerentanan. Bisa dinyatakan dalam skala kualitatif (Rendah, Sedang, Tinggi) atau kuantitatif (probabilitas 0-100%).
- **Dampak (Impact):** Seberapa besar kerugian yang akan diderita organisasi jika risiko tersebut terjadi. Kerugian bisa bersifat finansial, reputasi, operasional, hukum, dll.

🕮 7.3 Proses Manajemen Risiko

Manajemen risiko bukanlah kegiatan sekali jadi, melainkan siklus berkelanjutan. Secara umum, prosesnya terdiri dari empat tahap utama:

1. **Identifikasi Risiko:** Mengidentifikasi aset, ancaman, dan kerentanan.
2. **Analisis dan Evaluasi Risiko:** Menilai tingkat risiko (Likelihood × Impact) dan memprioritaskan risiko mana yang harus ditangani terlebih dahulu.
3. **Perlakuan Risiko:** Memilih dan menerapkan langkah-langkah untuk mengelola risiko.
4. **Monitoring dan Review:** Memantau risiko dan efektivitas kontrol secara berkala, karena lingkungan ancaman selalu berubah.

Mari kita bahas setiap tahap secara lebih rinci.

🕮 7.4 Identifikasi Risiko: Mengenal Apa yang Kita Lindungi

Tahap pertama adalah mengidentifikasi "apa" yang perlu dilindungi (aset), "dari siapa" (ancaman), dan "di mana kelemahannya" (kerentanan).

7.4.1 Identifikasi Aset

Langkah awal adalah membuat **inventarisasi aset**. Tidak mungkin melindungi sesuatu jika kita tidak tahu bahwa sesuatu itu ada. Daftar aset harus mencakup:

- **Aset Data:** Database pelanggan, laporan keuangan, rencana strategis, kekayaan intelektual.
- **Aset Perangkat Lunak:** Aplikasi utama (ERP, CRM), sistem operasi, perangkat lunak perkantoran.
- **Aset Perangkat Keras:** Server, komputer karyawan, perangkat jaringan, media penyimpanan.
- **Aset Manusia:** Karyawan kunci dengan pengetahuan spesifik.
- **Aset Layanan:** Layanan email, website, koneksi internet.

Setelah diinventarisasi, aset perlu **diklasifikasikan** berdasarkan nilai dan tingkat kepentingannya bagi organisasi. Misalnya, skala:

- **Kritis:** Jika terganggu, organisasi tidak dapat beroperasi sama sekali.
- **Penting:** Jika terganggu, operasi terganggu tetapi masih bisa berjalan terbatas.
- **Normal:** Jika terganggu, dampaknya kecil dan dapat ditoleransi.

7.4.2 Identifikasi Ancaman dan Kerentanan

Untuk setiap aset, identifikasi:

- **Ancaman potensial:** Apa saja yang bisa menyebabkan kerusakan pada aset ini? (Lihat kembali Bab 2).
- **Kerentanan yang ada:** Kelemahan apa yang dimiliki aset ini sehingga mudah dieksploitasi?

Contoh untuk Aset "Database Pelanggan":

- **Ancaman:** Peretas (insider/outsider), malware, kesalahan karyawan, bencana alam.

- **Kerentanan:** Kata sandi lemah, software database tidak di-*patch*, tidak ada backup, akses fisik ke server tidak terkontrol.

🕮 7.5 Analisis dan Evaluasi Risiko (Penilaian Risiko Kualitatif)

Setelah risiko teridentifikasi, langkah selanjutnya adalah menilai seberapa besar risiko tersebut. Dalam mata kuliah ini, kita akan fokus pada **penilaian risiko kualitatif**, yang paling umum digunakan karena relatif sederhana dan mudah dipahami manajemen.

7.5.1 Menentukan Skala Likelihood dan Impact

Buat skala sederhana, misalnya 1-3 atau 1-5. Mari kita gunakan skala 1-3 untuk memudahkan.

Skala Kemungkinan (Likelihood):

Skala	Tingkat	Deskripsi
1	Rendah	Kemungkinan kecil terjadi (misal: <30% dalam setahun). Membutuhkan kondisi khusus.
2	Sedang	Mungkin terjadi (misal: 30-70% dalam setahun). Pernah terjadi di industri sejenis.
3	Tinggi	Sangat mungkin terjadi (misal: >70% dalam setahun). Sudah pernah terjadi di organisasi sendiri.

Skala Dampak (Impact):

Skala	Tingkat	Deskripsi (Contoh untuk UKM)
1	Rendah	Dampak kecil. Gangguan operasional <1 hari. Kerugian finansial kecil. Tidak berdampak pada reputasi.
2	Sedang	Dampak signifikan. Gangguan operasional 1-3 hari. Kerugian finansial menengah. Keluhan pelanggan mulai muncul.
3	Tinggi	Dampak sangat serius. Gangguan operasional >3 hari. Kerugian finansial besar. Kepercayaan pelanggan hilang, potensi tuntutan hukum.

7.5.2 Membuat Matriks Risiko

Setelah setiap risiko diberi nilai Likelihood (L) dan Impact (I), hitung tingkat risiko dengan rumus **Risiko = L × I**. Hasilnya akan berada di rentang 1 hingga 9.

Nilai risiko ini kemudian dipetakan ke dalam **Matriks Risiko** untuk memvisualisasikan prioritas.

Matriks Risiko 3×3:

	Dampak Rendah (1)	**Dampak Sedang (2)**	**Dampak Tinggi (3)**
Kemungkinan Tinggi (3)	**Sedang (3)**	**Tinggi (6)**	**Tinggi (9)**
Kemungkinan Sedang (2)	**Rendah (2)**	**Sedang (4)**	**Tinggi (6)**
Kemungkinan Rendah (1)	**Rendah (1)**	**Rendah (2)**	**Sedang (3)**

Kategori Prioritas:

- **Risiko Rendah (Nilai 1-2):** Dapat diterima. Mungkin tidak perlu tindakan langsung, cukup dipantau.
- **Risiko Sedang (Nilai 3-4):** Perlu perhatian. Harus ada rencana untuk mengelola risiko ini dalam jangka menengah.
- **Risiko Tinggi (Nilai 6-9):** Prioritas utama. Harus segera ditangani dengan alokasi sumber daya yang memadai.

7.5.3 Contoh Penilaian Risiko

Bayangkan sebuah UKM e-commerce fiktif bernama "TokoOnline".

Aset	**Ancaman**	**Kerentanan**	**L**	**I**	**Risiko (L×I)**	**Prioritas**
Database Pelanggan	Peretas mencuri data	Kata sandi lemah, software usang	3	3	**9**	**Tinggi**
Website TokoOnline	Serangan DDoS	Tidak ada proteksi DDoS	2	3	**6**	**Tinggi**
Komputer Karyawan	Infeksi malware	Karyawan bisa unduh file sembarangan	3	2	**6**	**Tinggi**

Aset	Ancaman	Kerentanan	L	I	Risiko (L×I)	Prioritas
Layanan Internet	Gangguan ISP	Hanya 1 ISP, tidak ada backup	2	2	**4**	**Sedang**
Ruang Server (fisik)	Banjir	Kantor di daerah rawan banjir	1	3	**3**	**Sedang**
Akun Media Sosial	Akun diretas	Kata sandi lemah, tidak ada 2FA	2	1	**2**	**Rendah**

Dari tabel ini, manajemen TokoOnline dapat langsung melihat bahwa risiko tertinggi adalah kebocoran data pelanggan dan gangguan website. Sumber daya dan perhatian harus difokuskan ke sana terlebih dahulu.

🕮 7.6 Perlakuan Risiko (Risk Treatment)

Setelah risiko diidentifikasi dan diprioritaskan, langkah selanjutnya adalah memutuskan apa yang akan dilakukan terhadap risiko tersebut. Ada empat opsi utama:

1. **Mitigasi (Reduce/Mitigate):** Mengurangi kemungkinan atau dampak risiko. Ini adalah opsi yang paling umum. Contoh: memasang firewall (mengurangi kemungkinan), melakukan backup rutin (mengurangi dampak).
2. **Transfer (Transfer/Share):** Memindahkan sebagian atau seluruh risiko ke pihak lain. Contoh: membeli asuransi siber, menggunakan layanan cloud pihak ketiga (di mana penyedia cloud bertanggung jawab atas sebagian keamanan).
3. **Hindari (Avoid):** Menghentikan aktivitas yang menimbulkan risiko. Contoh: memutuskan untuk tidak menyimpan data pelanggan yang sensitif sama sekali, atau menutup layanan yang tidak aman.
4. **Terima (Accept):** Menerima risiko dan tidak melakukan tindakan apa pun. Ini dilakukan jika biaya penanganan risiko lebih besar daripada dampaknya, atau risiko memang sangat kecil. Risiko yang diterima harus dipantau secara berkala.

Contoh Perlakuan Risiko untuk TokoOnline:

- **Risiko Database Pelanggan (Tinggi): Mitigasi**. Menerapkan kebijakan kata sandi kuat, meng-update software, mengenkripsi database.
- **Risiko DDoS (Tinggi): Transfer/Mitigasi**. Menggunakan layanan proteksi DDoS dari penyedia cloud atau CDN.
- **Risiko Komputer Karyawan (Tinggi): Mitigasi**. Memasang antivirus, memberikan pelatihan keamanan, membatasi hak instalasi software.
- **Risiko Banjir (Sedang): Mitigasi**. Memindahkan server ke lantai yang lebih tinggi, memasang sensor air.
- **Risiko Akun Medsos (Rendah): Terima**. Dampak kecil, cukup dipantau.

💡 7.7 Workshop: Analisis Risiko untuk Organisasi Fiktif

Untuk mempraktikkan pemahaman, mari kita lakukan simulasi analisis risiko untuk dua jenis organisasi fiktif: **UKM E-commerce** dan **Rumah Sakit Tipe C**.

Skenario 1: UKM E-commerce "TokoBatuku"

- **Bisnis:** Menjual kerajinan tangan secara online.
- **Aset Kritis:** Database pelanggan (nama, alamat, no HP, riwayat transaksi), website toko, akun media sosial (Instagram, Facebook), stok barang di gudang.
- **Karakteristik:** Tim TI kecil (1-2 orang), anggaran terbatas, sangat bergantung pada reputasi online.

Skenario 2: Rumah Sakit Tipe C "SehatSejahtera"

- **Bisnis:** Pelayanan kesehatan rawat inap dan rawat jalan.
- **Aset Kritis:** Rekam medis pasien (sangat sensitif), sistem informasi rumah sakit (SIRS), peralatan medis terhubung jaringan (IoT), data keuangan dan klaim BPJS.
- **Karakteristik:** Ada tim TI, kepatuhan terhadap regulasi kesehatan dan UU PDP sangat ketat, dampak gangguan bisa nyawa pasien.

Tugas Workshop (untuk dikerjakan dalam kelompok):

1. Pilih salah satu skenario.
2. Identifikasi minimal 5 aset kritis.

3. Untuk setiap aset, identifikasi minimal 2 ancaman dan kerentanan.
4. Lakukan penilaian risiko kualitatif (tentukan L, I, dan hitung nilai risiko) dengan skala 1-3.
5. Buat matriks risiko dan tentukan prioritas (Rendah, Sedang, Tinggi).
6. Untuk 3 risiko dengan prioritas tertinggi, usulkan opsi perlakuan risiko (mitigasi, transfer, hindari, terima) dan jelaskan secara singkat.

🗝 7.8 Rangkuman

1. **Manajemen risiko** adalah proses sistematis untuk memahami, mengevaluasi, dan mengelola risiko terhadap aset informasi.
2. Proses manajemen risiko terdiri dari: **Identifikasi** aset, ancaman, kerentanan → **Analisis** risiko (Likelihood × Impact) → **Perlakuan** risiko → **Monitoring**.
3. **Risiko = Kemungkinan (Likelihood) × Dampak (Impact).**
4. **Matriks risiko** membantu memvisualisasikan dan memprioritaskan risiko.
5. Ada empat opsi **perlakuan risiko**: Mitigasi, Transfer, Hindari, Terima.
6. Manajemen risiko adalah siklus berkelanjutan, bukan proyek sekali jadi.

✍ 7.9 Latihan Soal

1. Jelaskan perbedaan antara ancaman, kerentanan, dan risiko. Berikan contoh untuk masing-masing dalam konteks sebuah universitas.
2. Sebuah perusahaan memiliki risiko kebakaran di ruangan server. Dampaknya dinilai Tinggi (3), tetapi kemungkinannya Rendah (1). Berapa nilai risikonya? Masuk kategori apa? Opsi perlakuan risiko apa yang paling mungkin dipilih?
3. Mengapa tidak semua risiko dapat atau harus dihilangkan?

📝 7.10 Tugas Mandiri (Bobot 2.5%)

Instruksi:

Lakukan analisis risiko keamanan informasi untuk sebuah organisasi fiktif. Pilih salah satu jenis organisasi: **UKM bidang jasa konsultan IT** atau **Sekolah Menengah Kejuruan (SMK)** .

Langkah Tugas:

1. **Identifikasi Aset:** Buat daftar minimal 8 aset informasi yang dimiliki organisasi tersebut, lengkap dengan deskripsi singkat.
2. **Identifikasi Risiko:** Untuk setiap aset, identifikasi minimal satu ancaman dan satu kerentanan yang relevan.
3. **Penilaian Risiko:**
    - Tentukan skala Likelihood (L) dan Impact (I) dengan skala 1-3 (Rendah, Sedang, Tinggi). Berikan justifikasi singkat mengapa Anda memilih skala tersebut.
    - Hitung nilai risiko (L × I) untuk setiap risiko.
4. **Matriks Risiko:** Buatlah matriks risiko 3×3 dan petakan semua risiko yang telah Anda identifikasi ke dalam matriks tersebut.
5. **Prioritas dan Rekomendasi:**
    - Identifikasi 3 risiko dengan prioritas tertinggi (nilai 6 atau 9).
    - Untuk setiap risiko prioritas tinggi tersebut, berikan rekomendasi perlakuan risiko yang spesifik (misal: "Memasang firewall aplikasi web (WAF) untuk mitigasi serangan SQL injection").

Format Penugasan:

- Laporan dalam format PDF, maksimal 4 halaman.
- Gunakan tabel untuk memudahkan penyajian data identifikasi dan penilaian risiko.

BAB 8
KONTROL KEAMANAN

🎯 Kemampuan Akhir (Sub-CPMK 3.2)

Setelah mempelajari bab ini, mahasiswa mampu:

1. Menjelaskan klasifikasi kontrol keamanan berdasarkan fungsi dan jenis.
2. Membedakan kontrol administratif, teknis, dan fisik.
3. Merancang kontrol keamanan yang relevan berdasarkan hasil analisis risiko.
4. Mengevaluasi efektivitas kontrol keamanan yang diusulkan.

🕮 8.1 Pendahuluan: Dari Analisis ke Tindakan

Bab 7 telah membahas cara mengidentifikasi dan memprioritaskan risiko. Sekarang tibalah saatnya untuk bertindak. **Kontrol keamanan** (atau *safeguards/counter-measures*) adalah langkah-langkah konkret yang diambil untuk menangani risiko yang telah diidentifikasi.

Kontrol keamanan dapat diibaratkan sebagai sistem pertahanan sebuah benteng:

- Ada **tembok tinggi** (kontrol fisik) untuk mencegah musuh masuk.
- Ada **prajurit yang berjaga** (kontrol administratif) yang menjalankan prosedur dan patroli.
- Ada **sistem alarm dan jebakan** (kontrol teknis) untuk mendeteksi dan menghadang musuh yang mencoba menerobos.

Tidak ada satu kontrol pun yang sempurna. Oleh karena itu, organisasi perlu menerapkan **pertahanan berlapis** (*defense in depth*), yaitu menggunakan kombinasi

berbagai jenis kontrol sehingga jika satu kontrol gagal, masih ada kontrol lain yang melindungi.

🕮 8.2 Klasifikasi Kontrol Berdasarkan Fungsi

Berdasarkan fungsinya dalam siklus pengelolaan insiden, kontrol keamanan dapat diklasifikasikan menjadi tiga:

Jenis Kontrol	Fungsi	Analogi	Contoh
Preventif (Mencegah)	Mencegah terjadinya insiden sebelum terjadi.	Pagar, kunci pintu, satpam di pintu masuk.	Firewall, kebijakan kata sandi kuat, pelatihan kesadaran keamanan, otentikasi dua faktor (2FA).
Detektif (Mendeteksi)	Mendeteksi insiden yang sedang atau sudah terjadi.	Kamera CCTV, alarm, sensor gerak.	IDS (Intrusion Detection System), antivirus, audit log, monitoring sistem.
Korektif (Memperbaiki)	Memperbaiki dampak insiden dan memulihkan sistem ke kondisi normal.	Petugas pemadam kebakaran, tim medis, tim perbaikan.	Backup dan restore, disaster recovery plan, proses patch management.

Selain ketiga di atas, ada juga:

- **Deterrent (Menghalangi):** Kontrol yang secara psikologis menghalangi pelaku. Contoh: peringatan "Awas, area ini diawasi CCTV", kebijakan sanksi tegas.
- **Compensating (Kompensasi):** Kontrol alternatif yang diterapkan ketika kontrol utama tidak dapat diimplementasikan karena keterbatasan teknis atau biaya.

🕮 8.3 Klasifikasi Kontrol Berdasarkan Jenis

Klasifikasi yang lebih umum digunakan dalam manajemen keamanan adalah berdasarkan jenis atau sifat kontrolnya: **Administratif, Teknis, dan Fisik**.

8.3.1 Kontrol Administratif (Manajemen/SDM)

Kontrol administratif berfokus pada kebijakan, prosedur, dan perilaku manusia. Ini adalah fondasi dari keamanan, karena teknologi secanggih apa pun bisa dikalahkan oleh manusia yang ceroboh atau tidak patuh.

Contoh Kontrol Administratif:

- **Kebijakan Keamanan:** Dokumen resmi yang mengatur penggunaan aset TI (akan dibahas detail di Bab 9).
- **Prosedur:** Panduan langkah demi langkah untuk melakukan tugas-tugas keamanan (misal: prosedur *onboarding* dan *offboarding* karyawan).
- **Pelatihan dan Kesadaran Keamanan (Security Awareness Training):** Melatih karyawan untuk mengenali phishing, membuat kata sandi kuat, dan melaporkan insiden.
- **Pemisahan Tugas (Separation of Duties):** Memastikan tidak ada satu orang pun yang memiliki kendali penuh atas proses kritis. Misal: orang yang memesan barang tidak boleh sama dengan orang yang menyetujui pembayaran.
- **Rotasi Tugas (Job Rotation):** Mencegah kecurangan dengan memindahkan karyawan secara berkala.
- **Background Check:** Pemeriksaan latar belakang sebelum merekrut karyawan untuk posisi sensitif.

8.3.2 Kontrol Teknis (Logis/Teknologi)

Kontrol teknis diimplementasikan melalui perangkat keras, perangkat lunak, atau konfigurasi sistem. Ini adalah "teknologi" yang secara langsung melindungi aset digital.

Contoh Kontrol Teknis:

- **Kontrol Akses (Access Control):** Membatasi siapa yang dapat mengakses apa. Contoh: daftar kontrol akses (ACL), manajemen hak pengguna, otentikasi multi-faktor (MFA).

- **Kriptografi:** Enkripsi data (seperti di Bab 4), penggunaan TLS/SSL untuk komunikasi aman.
- **Firewall:** Memfilter lalu lintas jaringan berdasarkan aturan yang ditetapkan.
- **IDS/IPS (Intrusion Detection/Prevention System):** Memantau lalu lintas jaringan untuk mendeteksi/mencegah serangan.
- **Antivirus/Antimalware:** Mendeteksi dan menghapus perangkat lunak berbahaya.
- **Patch Management:** Proses untuk memastikan semua perangkat lunak selalu diperbarui dengan *patch* keamanan terbaru.
- **Logging dan Monitoring:** Mencatat semua aktivitas penting dalam sistem dan meninjaunya secara berkala untuk mendeteksi anomali.

8.3.3 Kontrol Fisik

Kontrol fisik melindungi aset, personel, dan fasilitas organisasi dari ancaman fisik.

Contoh Kontrol Fisik:

- **Keamanan Perimeter:** Pagar, pintu gerbang, pos satpam.
- **Kontrol Akses Fisik:** Kartu akses, biometrik (sidik jari, retina), kunci ruangan.
- **Pengawasan:** Kamera CCTV, petugas keamanan berpatroli.
- **Perlindungan Lingkungan:** Detektor asap, sistem pemadam kebakaran (sprinkler, APAR), sensor banjir, pendingin ruangan (AC) untuk server.
- **Keamanan Perangkat Keras:** Pengunci kabel laptop, lemari/server rack yang terkunci.

8.4 Studi Kasus: Merancang Kontrol Keamanan

Mari kita kembali ke contoh UKM "TokoOnline" dari Bab 7. Kita telah mengidentifikasi tiga risiko prioritas tinggi. Sekarang, mari kita rancang kontrol keamanan yang sesuai.

Risiko Prioritas Tinggi	Jenis Kontrol yang Dapat Diterapkan	Contoh Spesifik
1. Database Pelanggan Dicuri	**Preventif Teknis:** Enkripsi data sensitif di database.	Mengenkripsi kolom nomor telepon dan alamat di database.
	Preventif Teknis: Kontrol akses ketat.	Hanya aplikasi web yang boleh mengakses database, tidak boleh akses langsung dari karyawan.
	Detektif Teknis: Audit log.	Mencatat semua akses ke database dan meninjau log secara berkala.
	Administratif: Kebijaku kata sandi.	Mewajibkan kata sandi kuat dan menggantinya secara berkala.
2. Website TokoOnline Down (DDoS)	**Preventif Teknis:** Proteksi DDoS.	Berlangganan layanan CDN seperti Cloudflare yang memiliki fitur mitigasi DDoS.
	Korektif Teknis: Redundansi.	Menggunakan lebih dari satu server (load balancing) sehingga jika satu diserang, yang lain masih bisa melayani.
3. Komputer Karyawan Terinfeksi Malware	**Preventif Teknis:** Antivirus.	Memasang dan memastikan antivirus selalu aktif dan diperbarui di semua komputer.
	Preventif Administratif: Pelatihan.	Melatih karyawan untuk tidak mengklik tautan mencurigakan atau mengunduh file dari sumber tidak dikenal.
	Detektif Teknis: Monitoring endpoint.	Menggunakan software untuk memantau aktivitas mencurigakan di komputer karyawan.
	Korektif Teknis: Backup.	Memastikan data penting di komputer karyawan di-backup secara otomatis ke server pusat.

Pertanyaan Evaluasi: Apakah kontrol-kontrol di atas sudah cukup? Mungkin belum. Inilah esensi *defense in depth*. Semakin banyak lapisan kontrol yang relevan, semakin kecil kemungkinan serangan berhasil.

🕮 8.5 Memilih dan Mengevaluasi Kontrol

Tidak semua kontrol cocok untuk semua organisasi. Pemilihan kontrol harus mempertimbangkan beberapa faktor:

1. **Kesesuaian dengan Risiko:** Kontrol harus secara langsung menangani risiko yang telah diidentifikasi. Jangan memasang kontrol "canggih" untuk risiko yang tidak ada.
2. **Biaya:** Biaya implementasi kontrol (pembelian, pemeliharaan, pelatihan) harus sebanding dengan nilai aset yang dilindungi. Jangan menghabiskan Rp 100 juta untuk melindungi aset senilai Rp 50 juta.
3. **Kemudahan Implementasi:** Apakah organisasi memiliki sumber daya dan keahlian untuk menerapkan kontrol tersebut?
4. **Dampak pada Pengguna:** Apakah kontrol akan sangat mengganggu produktivitas karyawan? Kontrol yang terlalu menyulitkan akan cenderung dihindari atau dimatikan oleh pengguna.
5. **Efektivitas:** Seberapa efektif kontrol tersebut dalam mengurangi risiko? Apakah ada bukti atau studi kasus yang mendukung?

Evaluasi kontrol harus dilakukan secara berkala. Apakah kontrol masih berfungsi seperti yang diharapkan? Apakah ada kontrol baru yang lebih efektif? Apakah ancaman baru muncul yang membuat kontrol lama menjadi usang?

🗝 8.6 Rangkuman

1. **Kontrol keamanan** adalah tindakan nyata untuk mengelola risiko.
2. Berdasarkan fungsi, kontrol dibagi menjadi: **Preventif** (mencegah), **Detektif** (mendeteksi), **Korektif** (memperbaiki).
3. Berdasarkan jenis, kontrol dibagi menjadi: **Administratif** (kebijakan, manusia), **Teknis** (teknologi), dan **Fisik** (lingkungan).
4. **Defense in depth** (pertahanan berlapis) adalah prinsip menggunakan kombinasi berbagai jenis kontrol untuk menciptakan keamanan yang tangguh.
5. Pemilihan kontrol harus mempertimbangkan kesesuaian risiko, biaya, kemudahan, dampak pada pengguna, dan efektivitas.

✍ 8.7 Latihan Soal

1. Sebutkan dan jelaskan masing-masing satu contoh kontrol preventif, detektif, dan korektif yang bisa diterapkan untuk melindungi data di laptop karyawan yang sering dibawa ke luar kantor.
2. Apa yang dimaksud dengan *defense in depth*? Mengapa prinsip ini penting?
3. Sebuah perusahaan memutuskan untuk memasang biometric fingerprint scanner di pintu masuk ruang server. Termasuk jenis kontrol apa (berdasarkan fungsi dan berdasarkan jenis) tindakan ini? Jelaskan.
4. Mengapa kontrol administratif (seperti pelatihan karyawan) sering dianggap sama pentingnya dengan kontrol teknis canggih?

📝 8.8 Tugas Mandiri (Bobot 2%)

Instruksi:

Gunakan hasil analisis risiko yang telah Anda buat pada Tugas Mandiri Bab 7 (untuk organisasi fiktif pilihan Anda). Jika Anda belum puas dengan hasil analisis di Bab 7, Anda dapat memperbaikinya terlebih dahulu.

Langkah Tugas:

1. Pilih **tiga risiko dengan prioritas tertinggi** dari hasil analisis Anda di Bab 7.
2. Untuk setiap risiko tersebut, rancanglah **minimal tiga kontrol keamanan** yang saling melengkapi (usahakan mencakup kombinasi kontrol administratif, teknis, dan fisik jika memungkinkan).
3. Untuk setiap kontrol yang Anda usulkan, jelaskan:
    - **Jenis kontrol** (berdasarkan fungsi: preventif/detektif/korektif, dan berdasarkan jenis: administratif/teknis/fisik).
    - **Bagaimana kontrol tersebut bekerja** secara singkat.
    - **Bagaimana kontrol tersebut mengurangi risiko** (apakah mengurangi likelihood, mengurangi impact, atau keduanya?).
4. Berikan **evaluasi singkat** mengenai efektivitas dan kemungkinan tantangan implementasi dari setiap kontrol yang Anda usulkan.

Format Penugasan:

- Laporan dalam format PDF, maksimal 3 halaman.
- Gunakan tabel untuk menyajikan kontrol yang dirancang agar mudah dibaca.

BAB 9
KEBIJAKAN KEAMANAN INFORMASI

🎯 Kemampuan Akhir (Sub-CPMK 3.3)

Setelah mempelajari bab ini, mahasiswa mampu:

1. Menjelaskan hirarki dokumen keamanan informasi (kebijakan, standar, prosedur, pedoman).
2. Membedakan berbagai jenis kebijakan keamanan (EISP, ISSP, SysSP).
3. Menjelaskan struktur kebijakan keamanan yang efektif.
4. Menyusun kebijakan keamanan sederhana untuk organisasi skala kecil, seperti *Acceptable Use Policy* (AUP) atau *Password Policy*.

🕮 9.1 Pendahuluan: Aturan Main dalam Organisasi

Bayangkan sebuah negara tanpa hukum. Kekacauan akan terjadi. Tidak ada yang tahu apa yang boleh dan tidak boleh dilakukan, tidak ada sanksi bagi pelanggar, dan tidak ada panduan bagi aparat penegak hukum.

Demikian pula dengan organisasi. Teknologi keamanan tercanggih sekalipun (firewall, enkripsi, antivirus) tidak akan berfungsi optimal jika tidak didukung oleh **aturan main** yang jelas. Aturan main inilah yang disebut **kebijakan keamanan informasi**.

Kebijakan keamanan informasi adalah dokumen formal yang berisi pernyataan, aturan, dan praktik yang mengatur bagaimana organisasi mengelola, melindungi, dan mendistribusikan aset informasinya. Kebijakan menjembatani visi manajemen puncak dengan tindakan teknis di lapangan.

🕮 9.2 Hirarki Dokumen Keamanan

Kebijakan tidak berdiri sendiri. Ia berada dalam sebuah hirarki dokumen yang saling melengkapi. Memahami hirarki ini penting agar tidak terjadi kebingungan antara "apa yang harus dicapai" dan "bagaimana cara mencapainya".

Tingkat	Jenis Dokumen	Deskripsi	Analogi
Tingkat 1 (Strategis)	**Kebijakan (Policy)**	Pernyataan tingkat tinggi tentang tujuan, niat, dan arahan manajemen. Menjawab pertanyaan **"APA"** yang ingin dicapai. Bersifat umum dan mengikat.	Undang-Undang Dasar (UUD). Menyatakan bahwa "setiap warga negara berhak mendapatkan pendidikan."
Tingkat 2 (Taktis)	**Standar (Standard)**	Persyaratan wajib yang spesifik, terukur, dan seragam. Menjawab pertanyaan **"APA"** yang harus dipenuhi secara teknis.	Peraturan Pemerintah (PP). Menetapkan bahwa "standar kelulusan siswa adalah nilai minimal 70."
Tingkat 3 (Operasional)	**Prosedur (Procedure)**	Panduan langkah demi langkah yang rinci tentang **"BAGAIMANA"** melaksanakan tugas tertentu.	Instruksi teknis/SOP. "Langkah-langkah mendaftar ujian nasional: 1. Login ke portal, 2. Isi formulir, 3. Unggah foto."
Tingkat 4 (Pendukung)	**Pedoman (Guideline)**	Rekomendasi atau saran praktik terbaik. Bersifat tidak wajib, tetapi sangat disarankan.	Panduan belajar. "Siswa disarankan belajar minimal 2 jam sehari untuk meraih hasil optimal."

Hubungan Antar Dokumen:

- **Kebijakan** adalah fondasi. Tanpa kebijakan, standar dan prosedur tidak memiliki legitimasi.
- **Standar** membuat kebijakan menjadi terukur. Kebijakan "kata sandi harus aman" diterjemahkan menjadi standar "kata sandi minimal 8 karakter, kombinasi huruf besar, huruf kecil, angka, dan simbol".
- **Prosedur** membuat standar dapat diimplementasikan. Standar kata sandi di atas diimplementasikan melalui prosedur "mengganti kata sandi di sistem setiap 90 hari".
- **Pedoman** membantu orang melakukan hal yang benar, meskipun tidak wajib.

🕮 9.3 Jenis-Jenis Kebijakan Keamanan Informasi

Dalam praktiknya, kebijakan keamanan informasi dapat dibagi menjadi tiga tingkatan berdasarkan cakupan dan fokusnya, seperti yang dikemukakan oleh Whitman & Mattord (2021).

9.3.1 EISP (Enterprise Information Security Policy)

EISP adalah kebijakan tingkat tertinggi. Dokumen ini mendefinisikan visi, misi, dan arahan strategis keamanan informasi di seluruh organisasi. EISP menjawab pertanyaan: **"Mengapa keamanan informasi penting bagi organisasi ini dan apa tujuan utamanya?"**

Karakteristik EISP:

- Disusun oleh manajemen puncak (direksi, dewan direktur).
- Bersifat jangka panjang dan relatif stabil.
- Menjelaskan komitmen manajemen terhadap keamanan informasi.
- Menetapkan kerangka kerja untuk kebijakan dan standar di bawahnya.
- Biasanya singkat (2-5 halaman) dan ditulis dalam bahasa non-teknis.

Contoh Isi EISP:

- **Pernyataan Tujuan:** "PT Maju Jaya berkomitmen untuk melindungi kerahasiaan, integritas, dan ketersediaan aset informasinya guna mendukung kelangsungan bisnis dan kepuasan pelanggan."
- **Ruang Lingkup:** Berlaku untuk seluruh karyawan, kontraktor, mitra bisnis, dan pihak ketiga yang memiliki akses ke aset informasi perusahaan.
- **Prinsip Dasar:** Semua aset informasi adalah milik perusahaan. Penggunaan aset informasi harus sesuai dengan tujuan bisnis. Setiap insiden keamanan wajib dilaporkan.
- **Penegakan dan Sanksi:** Pelanggaran terhadap kebijakan ini dapat mengakibatkan tindakan disipliner, hingga pemutusan hubungan kerja dan tuntutan hukum.

9.3.2 ISSP (Issue-Specific Security Policy)

ISSP adalah kebijakan yang membahas isu atau topik keamanan tertentu secara lebih rinci. ISSP menjawab pertanyaan: **"Apa aturan spesifik untuk isu tertentu?"**

Karakteristik ISSP:

- Dikembangkan oleh manajemen menengah atau tim keamanan dengan persetujuan manajemen puncak.
- Fokus pada satu area atau isu.
- Lebih detail dan teknis daripada EISP.
- Dapat diperbarui lebih sering mengikuti perkembangan teknologi dan ancaman.

Contoh ISSP yang Umum:

- **Kebijakan Penggunaan yang Dapat Diterima (Acceptable Use Policy/AUP):** Mengatur penggunaan aset TI perusahaan seperti internet, email, dan komputer. Melarang aktivitas seperti mengakses situs pornografi, mengirim email spam, atau menggunakan software bajakan.
- **Kebijakan Kata Sandi (Password Policy):** Mengatur persyaratan pembuatan, penggunaan, dan penggantian kata sandi. (Minimal panjang, kompleksitas, masa berlaku, larangan menggunakan kata sandi yang sama untuk akun pribadi dan kantor).

- **Kebijakan Email (Email Policy):** Mengatur penggunaan email kantor, termasuk larangan mengirim informasi rahasia melalui email pribadi, aturan tentang *forwarding* email, dan penyimpanan arsip email.
- **Kebijakan Remote Access:** Mengatur bagaimana karyawan dapat mengakses jaringan kantor dari luar (misal: wajib menggunakan VPN, perangkat yang digunakan harus memenuhi standar keamanan).

9.3.3 SysSP (System-Specific Security Policy)

SysSP adalah kebijakan yang sangat teknis dan spesifik untuk suatu sistem, aplikasi, atau perangkat tertentu. SysSP menjawab pertanyaan: **"Bagaimana aturan keamanan dikonfigurasi pada sistem ini?"**

SysSP seringkali hadir dalam dua bentuk:

1. **Prosedur Manajemen Sistem:** Dokumen tertulis yang menjelaskan bagaimana sistem tertentu harus dikelola secara aman. Contoh: "Prosedur *hardening* server web", "Prosedur konfigurasi firewall", "Prosedur backup database".
2. **Konfigurasi Teknis:** Aturan-aturan yang secara teknis diimplementasikan pada sistem. Ini bisa berupa *access control lists* (ACL) pada router, aturan pada firewall, atau setelan keamanan pada sistem operasi.

SysSP adalah ujung tombak implementasi keamanan. EISP dan ISSP adalah "apa" dan "mengapa", SysSP adalah "bagaimana" yang sesungguhnya dalam bahasa mesin.

🕮 9.4 Struktur Kebijakan yang Efektif

Sebuah kebijakan keamanan yang baik harus memiliki struktur yang jelas agar mudah dipahami dan diimplementasikan. Berikut adalah elemen-elemen yang biasanya ada dalam sebuah dokumen kebijakan (terutama ISSP):

1. **Judul dan Nomor Dokumen:** Memudahkan identifikasi dan pengarsipan.
2. **Pendahuluan:**
    - **Tujuan:** Menjelaskan mengapa kebijakan ini dibuat. Mengaitkan dengan tujuan bisnis dan EISP.

- **Ruang Lingkup:** Menjelaskan kepada siapa kebijakan ini berlaku (seluruh karyawan, bagian tertentu, kontraktor) dan pada sistem apa saja.
- **Definisi:** Menjelaskan istilah-istilah kunci yang digunakan dalam kebijakan agar tidak ambigu.

3. **Isi Kebijakan (Pernyataan Kebijakan):**
   - Bagian inti yang berisi aturan-aturan spesifik.
   - Ditulis dengan bahasa yang jelas, tegas, dan tidak ambigu. Gunakan kata "harus", "wajib", "dilarang", bukan kata "sebaiknya".
   - Contoh (dalam *Password Policy*): "Kata sandi harus terdiri dari minimal 8 karakter. Kata sandi wajib mengandung setidaknya satu huruf besar, satu huruf kecil, satu angka, dan satu simbol."
4. **Penegakan dan Sanksi:**
   - Menjelaskan apa konsekuensi jika kebijakan dilanggar. Ini memberikan "gigi" pada kebijakan.
   - Contoh: "Pelanggaran terhadap kebijakan ini akan dikenakan sanksi disipliner sesuai dengan Peraturan Perusahaan, mulai dari teguran tertulis hingga pemutusan hubungan kerja."
5. **Tanggung Jawab:**
   - Menjelaskan siapa yang bertanggung jawab atas implementasi, sosialisasi, dan penegakan kebijakan.
6. **Informasi Terkait:**
   - Referensi ke dokumen lain yang terkait (misal: EISP, standar teknis, prosedur).
7. **Riwayat Revisi:**
   - Mencatat kapan kebijakan dibuat, direview, dan direvisi, serta oleh siapa.
8. **Tanda Tangan Pengesahan:**
   - Ditandatangani oleh pejabat berwenang (misal: Direktur Utama, Direktur TI) untuk menunjukkan dukungan manajemen puncak.

💡 9.5 Workshop: Menyusun Kebijakan Sederhana

Mari kita praktikkan menyusun dua jenis kebijakan ISSP yang paling umum.

Skenario 1: Menyusun Acceptable Use Policy (AUP) untuk UKM
Bayangkan Anda adalah konsultan keamanan untuk UKM "WarungTekno" yang baru saja berkembang dan memiliki 20 karyawan. Mereka belum pernah memiliki kebijakan tertulis. Buatlah draf AUP sederhana.

Kerangka AUP WarungTekno:

KEBIJAKAN PENGGUNAAN ASET TI (AUP)
PT WarungTekno
Nomor Dokumen: AUP/WT/001

1. Tujuan

Kebijakan ini bertujuan untuk memastikan penggunaan aset teknologi informasi (TI) Perusahaan, termasuk komputer, email, dan akses internet, dilakukan secara bijak, etis, dan aman, serta tidak mengganggu produktivitas kerja dan keamanan informasi Perusahaan.

2. Ruang Lingkup
Kebijakan ini berlaku bagi seluruh karyawan tetap, karyawan kontrak, dan pihak ketiga yang memiliki akses ke aset TI PT WarungTekno.

3. Definisi

- **Aset TI:** Semua perangkat keras (komputer, laptop, printer), perangkat lunak, akun email, dan akses internet yang disediakan oleh Perusahaan.
- **Informasi Rahasia:** Data yang tidak dipublikasikan, seperti data pelanggan, laporan keuangan, dan rencana bisnis.

4. Kebijakan Penggunaan

- **Penggunaan Internet:**
    - Akses internet terutama untuk tujuan bisnis. Penggunaan pribadi yang wajar (misal: mengecek media sosial saat istirahat) diperbolehkan, asalkan tidak mengganggu pekerjaan dan tidak melanggar hukum.

    - **DILARANG** mengakses, mengunduh, atau menyebarluaskan materi pornografi, perjudian, konten ilegal, atau perangkat lunak bajakan.
- **Penggunaan Email:**
    - Akun email Perusahaan adalah untuk komunikasi bisnis.
    - **DILARANG** mengirim email yang mengandung pelecehan, ancaman, atau diskriminasi.
    - **DILARANG** mengirim informasi rahasia Perusahaan ke alamat email pribadi.
    - Waspada terhadap email phishing. Jangan mengklik tautan atau membuka lampiran dari pengirim yang tidak dikenal.
- **Keamanan Perangkat:**
    - Karyawan bertanggung jawab atas keamanan perangkat yang digunakan.
    - Laporkan segera jika perangkat hilang atau dicuri.
    - Jangan menginstal perangkat lunak tanpa izin dari Divisi TI.

5. Sanksi

Pelanggaran terhadap kebijakan ini dapat mengakibatkan tindakan disipliner, mulai dari teguran lisan, pemutusan akses, hingga pemutusan hubungan kerja, sesuai dengan beratnya pelanggaran.

6. Tanggung Jawab

Divisi TI bertanggung jawab untuk mensosialisasikan dan menegakkan kebijakan ini. Seluruh karyawan bertanggung jawab untuk mematuhinya.

Skenario 2: Menyusun Password Policy untuk UKM

Lanjutkan dengan kebijakan kata sandi.

KEBIJAKAN KATA SANDI (PASSWORD POLICY)

PT WarungTekno

Nomor Dokumen: PWD/WT/001

1. Tujuan

Kebijakan ini bertujuan untuk menetapkan standar pembuatan, penggunaan, dan perlindungan kata sandi guna mengamankan akses ke sistem dan informasi Perusahaan.

2. Ruang Lingkup

Berlaku untuk semua akun pengguna yang digunakan untuk mengakses sistem PT WarungTekno, termasuk akun email, akun jaringan, dan akun aplikasi internal.

3. Kebijakan Pembuatan Kata Sandi

- **Panjang Minimal:** Kata sandi harus memiliki panjang minimal 8 karakter.
- **Kompleksitas:** Kata sandi wajib mengandung setidaknya tiga dari empat kategori berikut: huruf besar (A-Z), huruf kecil (a-z), angka (0-9), dan karakter khusus (!@#$%^&*).
- **Larangan:** Kata sandi TIDAK BOLEH menggunakan informasi pribadi yang mudah ditebak (nama, tanggal lahir, nomor telepon) atau kata-kata yang ada dalam kamus.

4. Kebijakan Penggunaan dan Perlindungan

- **Kerahasiaan:** Kata sandi bersifat rahasia dan TIDAK BOLEH dibagikan kepada siapa pun, termasuk rekan kerja atau pihak yang mengaku dari TI. Petugas TI tidak akan pernah meminta kata sandi Anda.
- **Penyimpanan:** Jangan menulis kata sandi di kertas atau menyimpannya dalam file tidak terenkripsi di komputer.
- **Autentikasi Dua Faktor (2FA):** Jika tersedia, wajib mengaktifkan 2FA untuk menambah lapisan keamanan.

5. Sanksi

Pelanggaran terhadap kebijakan ini, seperti membagikan kata sandi, akan dikenakan sanksi disipliner.

🗝 9.6 Rangkuman

1. **Kebijakan keamanan informasi** adalah aturan formal yang mengelola, melindungi, dan mendistribusikan aset informasi.
2. Hirarki dokumen keamanan terdiri dari: **Kebijakan** (apa tujuan), **Standar** (apa yang harus dipenuhi), **Prosedur** (bagaimana melakukannya), dan **Pedoman** (saran praktik terbaik).

3. Tiga jenis kebijakan utama: **EISP** (strategis, enterprise), **ISSP** (taktis, per isu), dan **SysSP** (teknis, per sistem).
4. Kebijakan yang efektif memiliki struktur yang jelas: tujuan, ruang lingkup, definisi, pernyataan kebijakan, penegakan/sanksi, dan tanggung jawab.
5. Contoh ISSP yang umum adalah **Acceptable Use Policy (AUP)** dan **Password Policy**.
6. Kebijakan harus dikomunikasikan kepada seluruh karyawan dan ditegakkan secara konsisten.

✍ 9.7 Latihan Soal

1. Jelaskan perbedaan antara EISP, ISSP, dan SysSP. Berikan contoh topik untuk masing-masing.
2. Apa perbedaan antara kebijakan (policy) dan prosedur (procedure)? Mengapa sebuah organisasi membutuhkan keduanya?
3. Sebutkan lima elemen penting yang harus ada dalam sebuah dokumen ISSP.
4. Mengapa dukungan manajemen puncak sangat penting dalam implementasi kebijakan keamanan?

📝 9.8 Tugas Mandiri (Bobot 2.5%)

Instruksi:
Susunlah sebuah draf kebijakan keamanan sederhana untuk organisasi fiktif pilihan Anda (bisa UKM, sekolah, atau organisasi nirlaba). Pilih **salah satu** dari dua jenis kebijakan berikut:

1. **Acceptable Use Policy (AUP):** Kebijakan penggunaan internet, email, dan perangkat TI.
2. **Password Policy:** Kebijakan tentang pembuatan dan penggunaan kata sandi.

Langkah Tugas:

1. **Identifikasi Organisasi:** Sebutkan secara singkat profil organisasi fiktif Anda (nama, bidang usaha, jumlah karyawan).
2. **Susun Kebijakan:** Buatlah dokumen kebijakan dengan struktur yang profesional, mencakup setidaknya elemen-elemen berikut:
    - Judul dan Nomor Dokumen (buat sendiri formatnya)
    - Tujuan
    - Ruang Lingkup
    - Definisi (jika diperlukan, jelaskan istilah teknis)
    - Isi Kebijakan (pernyataan aturan yang jelas dan spesifik)
    - Penegakan dan Sanksi
    - Tanggung Jawab
    - Tanggal Efektif dan Tanda Tangan Pengesahan (buat fiktif)
3. **Justifikasi:** Tambahkan satu paragraf singkat di akhir dokumen yang menjelaskan **mengapa** kebijakan yang Anda buat penting untuk organisasi fiktif tersebut.

Format Penugasan:

- Dokumen kebijakan dalam format PDF, dibuat senyata mungkin (gunakan kop surat fiktif jika mau).
- Panjang bebas, tetapi pastikan semua elemen penting tercakup.
- Gunakan bahasa yang formal, jelas, dan tidak ambigu.

📚 DAFTAR PUSTAKA

- Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.
- ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization. (Untuk konteks kontrol dan kebijakan).
- NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*. National Institute of Standards and Technology.
- Kim, D., & Solomon, M. G. (2021). *Fundamentals of Information Systems Security* (4th ed.). Jones & Bartlett Learning.

BAGIAN 4
KEAMANAN TEKNIS DAN ASPEK MANUSIA

BAB 10
KEAMANAN JARINGAN

🎯 Kemampuan Akhir (Sub-CPMK 4.1)

Setelah mempelajari bab ini (Pertemuan 11 dan 12), mahasiswa mampu:

1. Menjelaskan fungsi dan cara kerja perangkat keamanan jaringan: firewall, IDS/IPS, dan VPN.
2. Menganalisis konfigurasi firewall pada skenario jaringan tertentu.
3. Menjelaskan protokol jaringan aman seperti SSL/TLS, IPSec, dan SSH.
4. Menganalisis kelemahan arsitektur jaringan dan merekomendasikan perbaikan.
5. Menjelaskan konsep Zero Trust Architecture dan segmentasi jaringan.

🕮 10.1 Pendahuluan: Menjaga Gerbang Digital

Jika data adalah "harta karun" organisasi, maka jaringan adalah "jalan raya" tempat harta itu diangkut. Di jalan raya ini, ada berbagai macam pengguna: ada yang sah (karyawan, mitra), ada yang penasaran (wardriver), dan ada yang berniat jahat (peretas). Tugas seorang profesional keamanan adalah memastikan bahwa hanya kendaraan yang sah yang dapat melewati jalan raya, dan harta karun yang diangkut sampai ke tujuan dengan selamat tanpa dicuri atau dirusak di tengah jalan.

Keamanan jaringan adalah praktik untuk melindungi jaringan komputer dari penyusup, baik yang mencoba menyerang dari luar maupun dari dalam. Tujuannya adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan data yang ditransmisikan melalui jaringan.

🕮 10.2 Perangkat Keamanan Jaringan

Ada tiga perangkat utama yang menjadi fondasi keamanan jaringan tradisional: Firewall, IDS/IPS, dan VPN.

10.2.1 Firewall: Satpam di Pintu Gerbang

Firewall adalah sistem keamanan jaringan yang memantau dan mengontrol lalu lintas jaringan yang masuk dan keluar berdasarkan aturan keamanan yang telah ditetapkan. Firewall bertindak sebagai "satpam" yang memeriksa setiap paket data yang mencoba melewati pintu gerbang jaringan.

Analogi Sederhana:

Bayangkan sebuah klub malam eksklusif. Ada satpam di pintu masuk (firewall).
Satpam memiliki daftar aturan:

- Semua pengunjung harus menunjukkan KTP (memeriksa sumber).
- Pengunjung harus terdaftar di daftar tamu (memeriksa tujuan).
- Pengunjung tidak boleh membawa senjata tajam (memeriksa konten berbahaya).

  Hanya pengunjung yang memenuhi semua aturan yang diizinkan masuk. Sisanya ditolak.

Jenis-jenis Firewall:

Jenis Firewall	Cara Kerja	Kelebihan	Kekurangan
Packet Filtering Firewall	Memeriksa header paket IP (alamat asal, alamat tujuan, port). Keputusan allow/deny berdasarkan aturan sederhana.	Cepat, sederhana, murah.	Tidak bisa memeriksa konten paket. Mudah ditipu oleh paket yang tampak sah tetapi berisi muatan berbahaya.

Jenis Firewall	Cara Kerja	Kelebihan	Kekurangan
Stateful Inspection Firewall	Melacak status koneksi. Ia mengingat koneksi mana yang sudah diinisiasi dari dalam, dan hanya mengizinkan lalu lintas balasan yang sesuai.	Lebih aman dari packet filtering. Mencegah serangan yang memanfaatkan koneksi palsu.	Sedikit lebih lambat, tetapi masih sangat efisien.
Application (Proxy) Firewall	Memeriksa konten paket hingga ke lapisan aplikasi (misal: memeriksa perintah HTTP dalam lalu lintas web).	Sangat aman, mampu mendeteksi serangan di tingkat aplikasi (SQL injection, XSS).	Jauh lebih lambat karena harus memproses ulang koneksi. Bisa menjadi bottleneck.
Next-Generation Firewall (NGFW)	Menggabungkan kemampuan stateful inspection, application firewall, IPS, dan intelijen ancaman dalam satu perangkat.	Keamanan komprehensif, visibilitas lebih baik.	Mahal, kompleks dalam konfigurasi.

Contoh Aturan Firewall Sederhana (dalam notasi tabel):

No	Aksi	Sumber	Tujuan	Protokol	Port Tujuan	Keterangan
1	Allow	192.168.1.0/24 (LAN Internal)	Any	TCP	80, 443	Mengizinkan akses web (HTTP/HTTPS) dari LAN.
2	Allow	Any	203.0.113.5 (Server Web)	TCP	80, 443	Mengizinkan akses publik ke server web.
3	Deny	Any	192.168.1.10 (Server Database)	Any	Any	Melarang semua akses dari luar ke server database.
4	Allow	192.168.1.0/24	192.168.1.10 (Server DB)	TCP	3306	Hanya mengizinkan aplikasi dari LAN mengakses database (port MySQL).
5	Deny	Any	Any	Any	Any	Blokir semua lalu lintas lainnya (default deny).

Prinsip penting dalam konfigurasi firewall:

- **Default Deny:** Aturan terakhir harus selalu "Deny All" (blokir semua). Hanya lalu lintas yang secara eksplisit diizinkan oleh aturan sebelumnya yang boleh lewat.
- **Least Privilege:** Berikan akses seminimal mungkin yang diperlukan untuk menjalankan fungsi bisnis.

10.2.2 IDS dan IPS: Sistem Deteksi dan Pencegahan

Firewall adalah penjaga di pintu gerbang. Namun, bagaimana jika penyerang berhasil melewati firewall? Atau bagaimana jika serangan datang dari dalam jaringan (insider threat)? Di sinilah peran **IDS** dan **IPS**.

- **IDS (Intrusion Detection System):** Sistem yang memantau lalu lintas jaringan dan aktivitas sistem untuk mencari tanda-tanda serangan. Jika mendeteksi sesuatu yang mencurigakan, IDS akan **mengirimkan peringatan (alert)** kepada administrator. IDS bersifat **pasif**. Ibarat kamera CCTV: merekam dan memberi tahu satpam jika ada yang mencurigakan, tetapi tidak bisa menghentikan pencuri secara langsung.
- **IPS (Intrusion Prevention System):** Sistem yang bekerja seperti IDS, tetapi dapat mengambil tindakan **aktif** untuk mencegah serangan. Jika mendeteksi lalu lintas berbahaya, IPS dapat langsung **memblokir koneksi** tersebut. IPS adalah evolusi dari IDS.

Analogi Sederhana:

- **IDS:** Satpam yang melihat monitor CCTV. Ketika melihat orang mencoba memanjat pagar, ia berteriak, "Hei, ada yang memanjat pagar!" tetapi tidak bisa berbuat apa-apa selain menunggu tim datang.
- **IPS:** Satpam yang melihat monitor dan langsung menekan tombol yang mengaktifkan pagar listrik, sehingga orang itu tidak bisa masuk.

Metode Deteksi IDS/IPS:

1. **Signature-Based Detection (Deteksi Berbasis Tanda Tangan):** Membandingkan lalu lintas dengan database pola serangan yang dikenal (signature). Mirip dengan antivirus. Efektif untuk serangan yang sudah dikenal, tetapi tidak bisa mendeteksi serangan baru (zero-day).

2. **Anomaly-Based Detection (Deteksi Berbasis Anomali):** Membangun model perilaku "normal" jaringan. Jika ada lalu lintas yang menyimpang dari normal (misal: traffic tiba-tiba melonjak drastis di tengah malam), sistem akan memberi peringatan. Mampu mendeteksi serangan baru, tetapi sering menghasilkan *false positive* (peringatan palsu).
3. **Stateful Protocol Analysis:** Memahami protokol dan melacak status koneksi. Mendeteksi pelanggaran protokol yang mencurigakan.

10.2.3 VPN (Virtual Private Network)

VPN adalah teknologi yang menciptakan koneksi aman dan terenkripsi ("terowongan") melalui jaringan publik seperti internet. VPN memungkinkan pengguna jarak jauh (remote worker) atau kantor cabang untuk terhubung ke jaringan kantor pusat seolah-olah mereka berada langsung di dalam jaringan tersebut.

Analogi Sederhana:
Bayangkan Anda harus mengirimkan surat rahasia melalui kantor pos umum (internet). Anda tidak ingin surat itu dibaca orang. Anda memasukkan surat ke dalam amplop tertutup rapat (enkripsi) dan mengirimkannya melalui pos. Penerima di kantor lain memiliki kunci untuk membuka amplop tersebut. Amplop tertutup itulah VPN. Kantor pos tidak tahu isi surat Anda.

Manfaat VPN:

- **Kerahasiaan:** Semua data yang dikirim melalui VPN dienkripsi, sehingga tidak dapat disadap oleh pihak ketiga.
- **Autentikasi:** Memastikan bahwa pengguna yang terhubung adalah pengguna yang sah.
- **Akses Jarak Jauh yang Aman:** Karyawan dapat bekerja dari rumah atau kafe dengan aman.
- **Menyatukan Jaringan:** Menghubungkan beberapa kantor cabang menjadi satu jaringan virtual.

Jenis VPN Berdasarkan Implementasi:

1. **Site-to-Site VPN:** Menghubungkan seluruh jaringan di dua lokasi berbeda (misal: kantor pusat dan kantor cabang).

2. **Remote Access VPN:** Menghubungkan satu pengguna individu ke jaringan pusat (misal: karyawan yang bekerja dari rumah).
3. **SSL VPN:** VPN yang diakses melalui browser web, tanpa perlu instalasi software khusus. Cocok untuk akses cepat ke aplikasi web tertentu.

🕮 10.3 Protokol Jaringan Aman

Selain perangkat, protokol komunikasi juga harus aman. Beberapa protokol dirancang khusus untuk memberikan keamanan di berbagai lapisan.

10.3.1 SSL/TLS (Secure Sockets Layer / Transport Layer Security)

SSL/TLS adalah protokol kriptografi yang menyediakan komunikasi aman di atas internet. Protokol ini adalah fondasi dari **HTTPS**. TLS adalah penerus SSL (saat ini SSL sudah usang dan tidak aman).

Cara Kerja TLS :

1. **Handshake:** Klien dan server menyepakati versi TLS dan metode enkripsi yang akan digunakan.
2. **Autentikasi Server:** Server mengirimkan sertifikat digitalnya (dari CA) kepada klien untuk membuktikan identitasnya.
3. **Pertukaran Kunci:** Klien dan server bertukar kunci sesi (session key) menggunakan kriptografi asimetris.
4. **Enkripsi Data:** Semua data selanjutnya dienkripsi menggunakan kriptografi simetris dengan kunci sesi.

10.3.2 IPSec (Internet Protocol Security)

IPSec adalah kumpulan protokol untuk mengamankan komunikasi di lapisan IP. Berbeda dengan TLS yang bekerja di lapisan transport, IPSec bekerja di lapisan jaringan. IPSec sering digunakan untuk **VPN Site-to-Site**.

IPSec memiliki dua mode utama:

- **Transport Mode:** Hanya mengenkripsi payload data, bukan header IP. Digunakan untuk komunikasi end-to-end antara dua host.

- **Tunnel Mode:** Mengenkripsi seluruh paket IP asli dan membungkusnya dengan header IP baru. Ini adalah mode yang digunakan untuk VPN.

10.3.3 SSH (Secure Shell)

SSH adalah protokol untuk mengakses dan mengelola perangkat jaringan (server, router, switch) secara aman melalui jaringan yang tidak aman. SSH menggantikan protokol lama seperti Telnet yang mengirimkan semua data (termasuk kata sandi) dalam bentuk teks biasa (*plaintext*).

SSH menyediakan:

- Otentikasi yang kuat (menggunakan kata sandi atau kunci publik).
- Enkripsi semua sesi komunikasi.
- Kemampuan untuk membuat terowongan aman (port forwarding).

🕮 10.4 Arsitektur Jaringan Aman

Perangkat dan protokol saja tidak cukup. Arsitektur keseluruhan jaringan harus dirancang dengan prinsip keamanan.

10.4.1 Segmentasi Jaringan

Segmentasi jaringan adalah praktik membagi jaringan besar menjadi beberapa sub-jaringan yang lebih kecil (subnet) yang terisolasi. Tujuannya adalah untuk membatasi pergerakan penyerang jika berhasil menembus satu bagian jaringan.

Analogi Sederhana:
Bayangkan sebuah kapal laut. Kapal modern memiliki sekat-sekat kedap air di lambungnya. Jika satu bagian bocor, air hanya akan membanjiri kompartemen itu, tidak seluruh kapal. Kapal tetap bisa mengapung. Segmentasi jaringan adalah "sekat kedap air" untuk jaringan.

Manfaat Segmentasi:

- **Membatasi Kerusakan:** Jika satu bagian jaringan (misal: WiFi tamu) diretas, penyerang tidak bisa langsung mengakses jaringan internal yang berisi data sensitif.

- **Meningkatkan Kinerja:** Mengurangi broadcast domain dan lalu lintas yang tidak perlu.
- **Memudahkan Kepatuhan:** Memisahkan data sensitif (misal: data kartu kredit untuk PCI DSS) ke segmen terpisah memudahkan audit.

10.4.2 DMZ (Demilitarized Zone)

DMZ adalah subnet fisik atau logis yang memisahkan jaringan internal organisasi dari jaringan eksternal (internet). Server-server yang perlu diakses dari luar, seperti server web, server email, dan server DNS, ditempatkan di DMZ.

Prinsipnya:

- Jika server web di DMZ diretas, penyerang hanya berada di DMZ. Ia masih harus melewati firewall lagi untuk bisa masuk ke jaringan internal.
- Firewall mengatur lalu lintas:
  - Dari internet ke DMZ: Diizinkan hanya untuk layanan yang diperlukan (port 80/443 ke server web).
  - Dari DMZ ke internal: Dibatasi ketat atau dilarang sama sekali. Server web tidak boleh memulai koneksi ke server database di internal.
  - Dari internal ke DMZ: Diizinkan untuk keperluan pemeliharaan.

10.4.3 Zero Trust Architecture (ZTA)

Zero Trust Architecture adalah model keamanan yang muncul karena model keamanan perimeter tradisional (kastil-dan-parit) dianggap usang. Di era cloud, mobile, dan remote work, "parit" (firewall perimeter) sudah tidak relevan karena pengguna dan data berada di mana-mana.

Prinsip Dasar Zero Trust:

- **"Never trust, always verify" (Jangan pernah percaya, selalu verifikasi).** Jangan menganggap lalu lintas dari dalam jaringan lebih aman daripada dari luar.
- **Akses dengan hak minimal (Least Privilege):** Berikan akses hanya apa yang diperlukan, hanya ketika diperlukan.
- **Mikrosegmentasi:** Membagi jaringan menjadi segmen-segmen yang sangat kecil, bahkan hingga ke tingkat aplikasi atau workload. Setiap koneksi harus diautentikasi dan diotorisasi, terlepas dari asalnya.

- **Asumsi Pelanggaran (Assume Breach):** Rancang sistem dengan asumsi bahwa penyerang sudah ada di dalam jaringan. Fokus pada meminimalkan dampak dan mendeteksi pergerakan mereka.

Implementasi Zero Trust:
Tidak ada produk "Zero Trust" tunggal. Ini adalah arsitektur yang diimplementasikan melalui kombinasi teknologi:

- **Identity and Access Management (IAM):** Verifikasi identitas yang kuat, MFA wajib.
- **Microsegmentation:** Firewall virtual di dalam jaringan.
- **Endpoint Detection and Response (EDR):** Memantau perilaku endpoint.
- **Encryption:** Enkripsi data di mana pun berada.

💡 10.5 Studi Kasus: Analisis Arsitektur Jaringan

Skenario Awal: Arsitektur Jaringan Sederhana (Tidak Aman)
Bayangkan sebuah kantor kecil dengan 50 karyawan. Mereka memiliki satu router dari ISP yang berfungsi sebagai modem, firewall, dan switch. Semua perangkat terhubung dalam satu jaringan yang sama: komputer karyawan, server file, printer, dan server web perusahaan (yang di-host di kantor). Tidak ada DMZ, tidak ada segmentasi.

Analisis Kelemahan:

1. **Tidak ada DMZ:** Server web perusahaan yang diakses dari internet berada di jaringan yang sama dengan komputer karyawan. Jika server web diretas, penyerang langsung memiliki akses ke semua komputer di LAN.
2. **Tidak ada segmentasi:** Jika satu komputer karyawan terinfeksi malware, malware tersebut dapat dengan mudah menyebar ke server file dan seluruh jaringan.
3. **WiFi tamu tidak dipisah:** WiFi untuk tamu kemungkinan besar adalah jaringan yang sama dengan karyawan. Tamu yang tidak dikenal bisa mengakses sumber daya internal.

4. **Single point of failure:** Jika router mati, seluruh internet dan akses antar perangkat terputus.

Rekomendasi Perbaikan (Arsitektur yang Lebih Aman)

1. **Tambahkan Firewall Khusus:** Ganti router ISP dengan firewall dedicated (misal: Fortinet, pfSense) yang memiliki kemampuan lebih baik.
2. **Buat DMZ:** Tempatkan server web di DMZ. Konfigurasi firewall:
    - Izinkan lalu lintas HTTP/HTTPS dari internet ke server web di DMZ.
    - Izinkan lalu lintas dari server web di DMZ ke server database di internal **hanya jika** server web membutuhkan akses database (dan batasi portnya). Jangan izinkan sebaliknya.
3. **Segmentasi Jaringan Internal:**
    - Buat VLAN terpisah: VLAN untuk karyawan, VLAN untuk server, VLAN untuk printer, VLAN untuk WiFi tamu.
    - Atur firewall antar VLAN: Karyawan boleh mengakses printer (port tertentu), tetapi tidak boleh mengakses server secara langsung. WiFi tamu hanya boleh akses internet, dilarang sama sekali mengakses jaringan internal.
4. **Terapkan VPN untuk Akses Jarak Jauh:** Jika ada karyawan yang bekerja dari luar, wajibkan menggunakan VPN untuk mengakses jaringan internal.
5. **Redundansi:** Pertimbangkan untuk menambah koneksi internet cadangan dari ISP lain.

🗝 10.6 Rangkuman

1. **Firewall** adalah satpam di pintu gerbang jaringan yang memfilter lalu lintas berdasarkan aturan. Jenisnya: Packet Filtering, Stateful Inspection, Application Firewall, NGFW.
2. **IDS/IPS** memantau lalu lintas untuk mendeteksi serangan. IDS memberi peringatan, IPS langsung memblokir.
3. **VPN** menciptakan terowongan terenkripsi melalui internet untuk akses jarak jauh yang aman.

4. Protokol aman seperti **SSL/TLS**, **IPSec**, dan **SSH** mengenkripsi komunikasi di berbagai lapisan.
5. Arsitektur jaringan yang baik menerapkan **segmentasi**, **DMZ**, dan idealnya mengadopsi prinsip **Zero Trust**: tidak ada yang dipercaya secara otomatis, semua harus diverifikasi.

✍ 10.7 Latihan Soal

1. Jelaskan perbedaan antara firewall stateful inspection dan application firewall. Dalam skenario apa application firewall lebih diperlukan?
2. Seorang administrator menemukan banyak peringatan dari IDS, tetapi setelah diselidiki, sebagian besar adalah alarm palsu (false positive). Apa yang harus dilakukan administrator?
3. Mengapa menempatkan server web di jaringan internal yang sama dengan komputer karyawan adalah praktik yang sangat buruk?
4. Jelaskan prinsip "Never trust, always verify" dalam konteks Zero Trust Architecture.

📝 10.8 Tugas Mandiri 1 (Bobot 2%)

Instruksi:
Analisis sebuah skenario konfigurasi firewall.

Skenario:
Sebuah perusahaan memiliki jaringan internal 192.168.1.0/24. Mereka memiliki server web di IP 192.168.1.10 (port 80 dan 443) yang harus dapat diakses dari internet. Mereka juga memiliki server database di IP 192.168.1.20 (port 3306) yang hanya boleh diakses oleh server web. Karyawan di jaringan internal harus bisa mengakses internet.

Buatlah **tabel aturan firewall** (seperti contoh di sub-bab 10.2.1) yang menerapkan:

1. Akses publik ke server web.
2. Akses server web ke server database.
3. Akses internet untuk karyawan.
4. Prinsip default deny (blokir semua lalu lintas lainnya).

Setelah membuat tabel, jelaskan secara singkat **mengapa** aturan tersebut diperlukan dan **ancaman apa** yang dapat dicegah oleh aturan tersebut.

Format Penugasan:

- Laporan dalam format PDF.

📝 10.9 Tugas Mandiri 2 (Bobot 2%)

Instruksi:
Analisis desain arsitektur jaringan sebuah organisasi fiktif.

Skenario:
Sebuah universitas memiliki tiga entitas:

- **Jaringan Akademik:** Untuk mahasiswa dan dosen (akses internet, akses ke sistem informasi akademik).
- **Jaringan Administrasi:** Untuk staf administrasi yang mengelola data sensitif mahasiswa (data pribadi, nilai, keuangan).
- **Jaringan Server:** Berisi server aplikasi dan server database.
- **WiFi Tamu:** Untuk pengunjung.

Saat ini, semua jaringan tersebut tergabung dalam satu jaringan besar tanpa pemisahan. Anda diminta sebagai konsultan untuk merancang ulang arsitektur jaringannya.

Langkah Tugas:

1. **Gambarkan Arsitektur Usulan:** Buatlah diagram sederhana (bisa dengan tangan lalu difoto, atau pakai tools draw.io) yang menunjukkan bagaimana Anda akan memisahkan keempat entitas tersebut.

2. **Jelaskan Segmentasi:** Jelaskan bagaimana Anda akan menerapkan segmentasi (VLAN) dan DMZ (jika diperlukan).
3. **Aturan Firewall:** Sebutkan setidaknya 3 aturan firewall utama yang akan Anda terapkan untuk mengatur lalu lintas antar segmen.
4. **Rekomendasi Zero Trust:** Berikan satu rekomendasi sederhana berdasarkan prinsip Zero Trust yang dapat diterapkan di lingkungan universitas ini.

Format Penugasan:

- Laporan dalam format PDF, dilengkapi dengan diagram.

BAB 11
KEAMANAN APLIKASI

🎯 Kemampuan Akhir (Sub-CPMK 4.2)

Setelah mempelajari bab ini, mahasiswa mampu:

1. Mengidentifikasi berbagai jenis kerentanan keamanan pada aplikasi web berdasarkan OWASP Top 10.
2. Menjelaskan dampak dari setiap kerentanan terhadap organisasi.
3. Merekomendasikan langkah-langkah perbaikan dan praktik secure coding untuk mencegah kerentanan.

🕮 11.1 Pendahuluan: Titik Paling Lemah

Firewall, IDS, VPN, dan enkripsi telah dipasang dengan sempurna. Jaringan diperkuat seperti benteng. Namun, bagaimana jika penyerang tidak perlu menembus benteng? Bagaimana jika mereka bisa masuk melalui pintu depan dengan berpura-pura menjadi tamu, lalu menemukan bahwa pintu itu sebenarnya tidak terkunci dengan benar?

Dalam banyak kasus, **aplikasi web** adalah pintu depan yang paling mudah dimasuki penyerang. Aplikasi web harus dapat diakses oleh publik (pengguna, pelanggan), sehingga secara default ia terbuka untuk interaksi. Jika aplikasi itu sendiri memiliki cacat (bug) dalam kode programnya, penyerang dapat memanfaatkannya untuk mencuri data, merusak sistem, atau bahkan mengambil alih server.

Keamanan aplikasi adalah praktik mengamankan perangkat lunak dari kerentanan sepanjang siklus hidupnya, mulai dari desain, pengembangan, hingga deployment dan pemeliharaan.

🕮 11.2 OWASP Top 10

OWASP (Open Web Application Security Project) adalah organisasi nirlaba global yang fokus pada peningkatan keamanan perangkat lunak. Setiap beberapa tahun, OWASP merilis **OWASP Top 10**, sebuah daftar 10 risiko keamanan aplikasi web paling kritis berdasarkan data dari ribuan organisasi dan para ahli.

Daftar ini adalah "standar de facto" untuk kesadaran keamanan aplikasi. Sebagai profesional TI, Anda harus memahami setidaknya risiko-risiko utama ini. Berikut adalah OWASP Top 10 versi 2021 (yang terbaru saat bahan ajar ini disusun).

Peringkat	Kerentanan	Deskripsi Singkat
A01:2021	**Broken Access Control**	Kegagalan dalam membatasi akses pengguna. Pengguna bisa melihat atau mengubah data milik orang lain, atau menjalankan fungsi admin tanpa izin.
A02:2021	**Cryptographic Failures**	Kegagalan kriptografi, sebelumnya disebut "Sensitive Data Exposure". Data sensitif tidak dilindungi dengan enkripsi yang tepat, atau enkripsi yang digunakan sudah usang/lemah.
A03:2021	**Injection**	Data tidak tepercaya (dari input pengguna) dikirim ke interpreter sebagai bagian dari perintah atau query. Contoh: SQL Injection, NoSQL Injection, OS Command Injection.
A04:2021	**Insecure Design**	Cacat pada desain arsitektur aplikasi. Risiko ini lebih ke "kesalahan konsep" daripada kesalahan implementasi kode.
A05:2021	**Security Misconfiguration**	Konfigurasi keamanan yang salah atau tidak aman. Contoh: default password masih aktif, directory listing diaktifkan, server menampilkan pesan error yang terlalu detail.
A06:2021	**Vulnerable and Outdated Components**	Menggunakan komponen perangkat lunak (library, framework) yang memiliki kerentanan yang diketahui atau sudah usang.

Peringkat	Kerentanan	Deskripsi Singkat
A07:2021	**Identification and Authentication Failures**	Kegagalan dalam fungsi identifikasi dan autentikasi. Contoh: sistem membiarkan serangan brute force, kata sandi lemah, session management yang buruk.
A08:2021	**Software and Data Integrity Failures**	Kegagalan integritas perangkat lunak dan data. Kode atau data tidak diverifikasi keasliannya. Contoh: aplikasi mengandalkan plugin dari sumber tidak tepercaya tanpa verifikasi.
A09:2021	**Security Logging and Monitoring Failures**	Kurangnya pencatatan (logging) dan pemantauan. Jika serangan terjadi, tidak ada catatan sehingga tidak terdeteksi dan tidak bisa diinvestigasi.
A10:2021	**Server-Side Request Forgery (SSRF)**	Penyerang dapat membuat aplikasi mengakses sumber daya internal atau eksternal yang tidak seharusnya dapat diakses, melalui server aplikasi.

🕮 11.3 Analisis Mendalam Tiga Kerentanan Kritis

Dari 10 kerentanan di atas, tiga yang paling sering dieksploitasi dan paling berbahaya adalah **Injection**, **Broken Access Control**, dan **Cryptographic Failures** (terutama terkait data sensitif).

11.3.1 Injection (Kelas A03)

Injection terjadi ketika data yang dimasukkan pengguna dikirim ke interpreter (misal: database SQL, sistem operasi) tanpa melalui proses pembersihan (sanitasi) atau validasi yang benar. Akibatnya, penyerang dapat mengirimkan perintah berbahaya yang dieksekusi oleh interpreter.

Contoh SQL Injection pada Halaman Login:

Bayangkan sebuah aplikasi memiliki query SQL untuk memeriksa login:

```
SELECT * FROM users WHERE username = 'username' AND password = 'password'
```

Kode program (PHP) yang tidak aman mungkin seperti ini:

```
$username = $_POST['username'];
$password = $_POST['password'];
```

```
$query = "SELECT * FROM users WHERE username = '$username' AND password = '$passwo
rd'";
```

Jika penyerang memasukkan username: `admin' --` (dengan tanda kutip tunggal dan dua garis strip), maka query menjadi:

```
SELECT * FROM users WHERE username = 'admin' -- ' AND password = 'apa saja'
```

Tanda `--` dalam SQL adalah komentar. Database akan mengabaikan sisa query setelahnya. Jadi, query hanya akan memeriksa username 'admin' tanpa peduli password. Penyerang berhasil login sebagai admin tanpa mengetahui passwordnya.

Dampak:

- Pencurian data (seluruh database bisa di-dump).
- Penghapusan atau perubahan data.
- Dalam kasus ekstrem, mengambil alih server (jika menggunakan OS Command Injection).

Pencegahan:

- **Gunakan Parameterized Queries (Prepared Statements):** Ini adalah pertahanan utama. Dengan prepared statements, kode SQL dipisahkan dari data. Data hanya diperlakukan sebagai nilai, bukan bagian dari perintah SQL.
- **Input Validation:** Validasi input di sisi server. Pastikan input sesuai dengan format yang diharapkan.
- **Prinsip Least Privilege:** Akun database yang digunakan aplikasi sebaiknya tidak memiliki hak untuk membuat, mengubah, atau menghapus tabel.

11.3.2 Broken Access Control (Kelas A01)

Broken Access Control berarti aplikasi tidak menerapkan pembatasan akses dengan benar. Pengguna biasa bisa melakukan hal-hal yang seharusnya hanya bisa dilakukan oleh administrator.

Contoh Skenario:

- **Insecure Direct Object References (IDOR):** Sebuah aplikasi menampilkan detail faktur dengan URL: `https://toko.com/faktur?id=12345`. Seorang pengguna login dan melihat faktur miliknya dengan ID 12345. Karena penasaran, ia mengganti URL menjadi `...?id=12346`. Ternyata, ia bisa melihat faktur milik

pengguna lain. Aplikasi gagal memeriksa apakah pengguna yang login berhak mengakses faktur dengan ID tersebut.

- **Privilege Escalation:** Seorang pengguna biasa mencoba mengakses halaman admin (`/admin`). Karena aplikasi tidak memeriksa peran (role) pengguna, ia berhasil masuk ke panel admin.

Dampak:

- Kebocoran data pengguna lain.
- Pengguna biasa dapat menjalankan fungsi administratif (menghapus pengguna, mengubah konfigurasi).

Pencegahan:

- **Terapkan Kontrol Akses di Sisi Server:** Jangan pernah mengandalkan kontrol yang hanya ada di sisi klien (seperti menyembunyikan tombol admin dengan JavaScript).
- **Gunakan Sistem Otorisasi yang Kuat:** Framework seperti Spring Security (Java), ASP.NET Identity, atau Django Guardian menyediakan mekanisme untuk mengelola hak akses.
- **Deny by Default:** Secara default, semua akses harus ditolak. Akses hanya diberikan secara eksplisit untuk pengguna dengan peran tertentu.
- **Cek Otorisasi untuk Setiap Request:** Setiap kali ada permintaan akses ke data atau fungsi, aplikasi harus memeriksa apakah pengguna yang sedang login memang memiliki hak untuk melakukannya.

11.3.3 Cryptographic Failures (Kelas A02)

Sebelumnya bernama "Sensitive Data Exposure". Ini terjadi ketika data sensitif tidak dilindungi dengan baik. Perhatikan, ini bukan hanya tentang tidak menggunakan enkripsi, tetapi juga tentang menggunakan enkripsi yang lemah atau implementasi yang salah.

Contoh Skenario:

- Situs web masih menggunakan HTTP, bukan HTTPS, sehingga semua data (termasuk kata sandi dan nomor kartu kredit) dikirim dalam bentuk teks biasa.
- Database menyimpan kata sandi dalam bentuk plaintext, bukan hash.
- Menggunakan algoritma hash yang sudah usang seperti MD5 atau SHA-1 untuk menyimpan kata sandi.

- Sertifikat SSL sudah kadaluarsa atau menggunakan enkripsi lemah.

Dampak:

- Pencurian data sensitif (kata sandi, data pribadi, data keuangan) yang dapat digunakan untuk penipuan identitas atau dijual di pasar gelap.

Pencegahan:

- **Gunakan HTTPS di Seluruh Situs:** Wajibkan semua komunikasi melalui HTTPS.
- **Enkripsi Data Sensitif di Penyimpanan:** Enkripsi data seperti nomor KTP, data medis, data keuangan di database.
- **Hash Kata Sandi dengan Kuat:** Gunakan fungsi hash yang dirancang khusus untuk kata sandi, seperti **bcrypt**, **Argon2**, atau **PBKDF2**. Fungsi-fungsi ini lambat dan memiliki "garam" (salt) otomatis untuk mencegah serangan tabel pelangi (rainbow table).
- **Jangan Menyimpan Data yang Tidak Perlu:** Jika Anda tidak perlu menyimpan nomor kartu kredit, jangan simpan. Semakin sedikit data sensitif yang disimpan, semakin kecil risikonya.

🕮 11.4 Prinsip Dasar Secure Coding

Menulis kode yang aman adalah tanggung jawab setiap pengembang. Berikut adalah beberapa prinsip dasar *secure coding* yang dapat mencegah banyak kerentanan:

1. **Validasi Input (Input Validation):** Selalu validasi input dari pengguna di sisi server. Asumsikan semua input berbahaya. Periksa tipe data, panjang, format, dan rentang nilai. Gunakan "allow list" (daftar yang diizinkan) daripada "block list".
2. **Output Encoding:** Saat menampilkan data yang berasal dari input pengguna (misal: komentar di forum), encode output tersebut sehingga tidak dieksekusi sebagai kode oleh browser. Ini mencegah serangan **Cross-Site Scripting (XSS)** .
3. **Parameterized Queries:** Gunakan prepared statements untuk semua query database untuk mencegah SQL Injection.

4. **Autentikasi dan Manajemen Sesi yang Kuat:** Terapkan kebijakan kata sandi kuat. Gunakan mekanisme yang aman untuk mengelola sesi pengguna. Jangan menampilkan token sesi di URL. Logout setelah periode tidak aktif.
5. **Prinsip Hak Minimal:** Kode aplikasi harus berjalan dengan hak akses seminimal mungkin. Jika aplikasi hanya perlu membaca database, jangan berikan hak menulis.
6. **Jangan Percaya pada Apa Pun dari Klien:** Semua data dari sisi klien (cookie, parameter URL, data form) dapat dimanipulasi oleh penyerang. Selalu validasi dan periksa di sisi server.
7. **Kelola Kerentanan Komponen:** Secara teratur perbarui semua library, framework, dan plugin yang digunakan. Pantau database kerentanan (seperti CVE) untuk komponen yang Anda gunakan.

💡 11.5 Studi Kasus: Identifikasi Kerentanan pada Aplikasi Web Fiktif

Bayangkan sebuah aplikasi web sederhana untuk memesan makanan online, "MakanYuk". Berikut adalah beberapa skenario yang mungkin mengandung kerentanan.

Skenario 1: SQL Injection pada Pencarian

Fitur: Pengguna dapat mencari restoran berdasarkan nama.

URL: `https://makanyuk.com/cari?nama=Padang`

Kode (tidak aman): `SELECT * FROM restoran WHERE nama LIKE '%" + request.getParameter("nama") + "%'`

Aksi Penyerang: Penyerang mengirimkan `nama=Padang'; DROP TABLE restoran; --`

Dampak: Seluruh tabel restoran bisa terhapus. (Injection)

Skenario 2: IDOR pada Detail Pesanan

Fitur: Pengguna dapat melihat detail pesanan mereka.

URL: `https://makanyuk.com/pesanan?id=5001`

Aksi Penyerang: Setelah login dengan akunnya, penyerang mencoba mengubah ID

menjadi 5000, 5002, dst.
Dampak: Jika aplikasi tidak memeriksa kepemilikan, penyerang bisa melihat detail pesanan (nama, alamat, nomor telepon) pelanggan lain. (Broken Access Control)

Skenario 3: Kata Sandi Lemah
Fitur: Pendaftaran akun baru.
Aksi: Pengguna mendaftar dengan kata sandi "123456". Sistem menerimanya.
Dampak: Akun mudah dibobol dengan serangan brute force. (Identification and Authentication Failures)

Skenario 4: Tidak Ada Logging
Fitur: Semua fitur di atas.
Aksi: Penyerang mencoba mengexploitasi celah-celah di atas, berhasil atau gagal.
Dampak: Tim pengembang tidak tahu bahwa ada upaya serangan karena tidak ada log. Jika serangan berhasil, mereka tidak tahu apa yang terjadi dan bagaimana cara memperbaikinya. (Security Logging and Monitoring Failures)

🗝 11.6 Rangkuman

1. **OWASP Top 10** adalah daftar 10 risiko keamanan aplikasi web paling kritis. Ini adalah panduan penting bagi pengembang dan profesional keamanan.
2. Tiga kerentanan yang paling sering dieksploitasi:
    - **Injection:** Memasukkan perintah berbahaya ke interpreter (SQL Injection).
    - **Broken Access Control:** Gagal membatasi akses pengguna (IDOR, privilege escalation).
    - **Cryptographic Failures:** Gagal melindungi data sensitif dengan enkripsi yang tepat.
3. Prinsip **secure coding** seperti validasi input, parameterized queries, dan hak minimal adalah fondasi untuk mencegah kerentanan.
4. Keamanan aplikasi adalah tanggung jawab bersama, bukan hanya tim keamanan, tetapi juga pengembang dan arsitek sistem.

✍ 11.7 Latihan Soal

1. Jelaskan apa itu SQL Injection dan bagaimana cara mencegahnya.
2. Seorang pengguna dapat melihat halaman profil pengguna lain hanya dengan mengganti angka di URL. Kerentanan OWASP apa yang terjadi? Jelaskan.
3. Mengapa menyimpan kata sandi dalam bentuk hash (seperti bcrypt) lebih baik daripada mengenkripsinya?
4. Sebutkan tiga prinsip secure coding yang paling penting menurut Anda, dan jelaskan mengapa.

📝 11.8 Tugas Mandiri (Bobot 2%)

Instruksi:
Lakukan analisis kerentanan pada sebuah aplikasi web fiktif.

Skenario:
Aplikasi "SimpleNotes" adalah aplikasi web untuk membuat catatan pribadi. Fiturnya:

- Pengguna harus login dengan username dan password.
- Setelah login, pengguna dapat membuat, melihat, mengedit, dan menghapus catatan mereka sendiri.
- Catatan disimpan di database dengan struktur: `id_catatan`, `judul`, `isi`, `username_pemilik`.
- URL untuk melihat catatan: `https://simplenotes.com/lihat.php?id=123`

Tugas:
Identifikasi **minimal 5 potensi kerentanan** yang mungkin ada pada aplikasi "SimpleNotes" berdasarkan OWASP Top 10. Untuk setiap kerentanan yang Anda identifikasi:

1. **Sebutkan Kode OWASP-nya** (misal: A03:2021 - Injection).

2. **Jelaskan Skenario Serangan:** Bagaimana penyerang dapat mengeksploitasi kerentanan ini pada aplikasi SimpleNotes? Berikan contoh konkret (misal: URL yang dimodifikasi, input tertentu).
3. **Jelaskan Dampak:** Apa yang bisa terjadi jika serangan berhasil?
4. **Berikan Rekomendasi Perbaikan:** Langkah konkret apa yang harus dilakukan pengembang untuk mencegah kerentanan ini (mengacu pada prinsip secure coding)?

Format Penugasan:

- Laporan dalam format PDF, disajikan dalam bentuk tabel untuk memudahkan pembacaan.

No	Kerentanan (Kode OWASP)	Skenario Serangan	Dampak	Rekomendasi Perbaikan
1	A03:2021 - Injection	...	...	...

BAB 12
ASPEK HUKUM, ETIKA, DAN KEPATUHAN

🎯 Kemampuan Akhir (Sub-CPMK 4.3)

Setelah mempelajari bab ini (Pertemuan 14 dan 15), mahasiswa mampu:

1. Menjelaskan ketentuan utama dalam UU ITE dan UU Perlindungan Data Pribadi (UU PDP) di Indonesia.
2. Menganalisis kasus pelanggaran hukum siber (cyber crime) berdasarkan regulasi yang berlaku.
3. Mengevaluasi dilema etika yang muncul dalam praktik keamanan informasi, seperti whistleblowing dan ethical hacking.
4. Menjelaskan implikasi kepatuhan terhadap regulasi dan standar dalam organisasi.

🕮 12.1 Pendahuluan: Dunia Maya Bukan Dunia Tanpa Hukum

Di masa-masa awal internet, banyak orang berpikir bahwa dunia maya adalah "Wild West", sebuah wilayah tanpa hukum di mana segala sesuatu diperbolehkan. Anggapan ini salah. Aktivitas di dunia maya memiliki konsekuensi di dunia nyata, dan semakin lama, semakin banyak regulasi yang dibuat untuk mengatur perilaku di ruang digital.

Sebagai profesional keamanan informasi, Anda tidak hanya perlu memahami teknologi, tetapi juga **kerangka hukum dan etika** yang mengatur profesi Anda. Melanggar hukum, meskipun dengan niat baik (misal: "menguji" keamanan sistem orang lain tanpa izin), tetap memiliki konsekuensi pidana.

Bab ini akan membahas dua regulasi terpenting di Indonesia: **UU ITE** dan **UU PDP**, serta dilema etika yang sering dihadapi para profesional keamanan.

🕮 12.2 Regulasi di Indonesia: UU ITE

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) adalah payung hukum utama untuk aktivitas di ruang digital di Indonesia. UU ini pertama kali disahkan pada tahun 2008 (UU No. 11 Tahun 2008) dan telah direvisi pada tahun 2016 (UU No. 19 Tahun 2016) dan terakhir pada tahun 2024 dengan Perppu Cipta Kerja yang kemudian menjadi UU.

UU ITE mengatur berbagai aspek, termasuk:

- Pengakuan tanda tangan elektronik dan dokumen elektronik sebagai alat bukti hukum yang sah.
- Penyelenggaraan Sertifikasi Elektronik dan Sistem Elektronik.
- Larangan dan sanksi pidana untuk berbagai tindakan siber (cyber crime).

12.2.1 Pasal-Pasal Penting dalam UU ITE (Terkait Cyber Crime)

Beberapa pasal dalam UU ITE yang paling relevan dengan keamanan informasi dan sering menjadi dasar penuntutan kasus siber:

Pasal	Tindakan yang Dilarang	Ancaman Pidana
Pasal 30	**Akses Ilegal:** Dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.	Pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp 600 juta.
Pasal 31	**Intersepsi/Penyadapan Ilegal:** Dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.	Pidana penjara paling lama 10 tahun dan/atau denda paling banyak Rp 800 juta.
Pasal 32	**Perusakan/Perubahan Data:** Dengan sengaja dan tanpa hak atau melawan hukum memindahkan, mentransfer, merusak, mengubah, atau menghilangkan informasi elektronik milik orang lain.	Pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp 2 miliar.

Pasal	Tindakan yang Dilarang	Ancaman Pidana
Pasal 33	**Gangguan Sistem:** Dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang menyebabkan sistem elektronik terganggu atau tidak berfungsi (misal: serangan DDoS).	Pidana penjara paling lama 10 tahun dan/atau denda paling banyak Rp 10 miliar.
Pasal 35	**Pemalsuan Data:** Dengan sengaja dan tanpa hak atau melawan hukum membuat informasi elektronik palsu atau memanipulasi informasi elektronik seolah-olah data yang otentik.	Pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp 12 miliar.
Pasal 27 Ayat (1)	**Konten Ilegal (Kesusilaan):** Dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya informasi elektronik yang memiliki muatan melanggar kesusilaan.	Pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp 1 miliar.
Pasal 27 Ayat (3)	**Konten Ilegal (Penghinaan/Pencemaran Nama Baik):** Dengan sengaja dan tanpa hak mendistribusikan informasi elektronik yang ditujukan untuk menyerang kehormatan atau nama baik seseorang.	Pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp 750 juta.
Pasal 28 Ayat (1)	**Berita Bohong (Hoax) yang Menyesatkan:** Dengan sengaja menyebarkan berita bohong yang menyebabkan kerugian konsumen.	Pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp 1 miliar.
Pasal 28 Ayat (2)	**Ujaran Kebencian:** Dengan sengaja menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu/kelompok masyarakat berdasarkan SARA.	Pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp 1 miliar.

Penting: Pasal-pasal tentang penghinaan dan pencemaran nama baik (Pasal 27 Ayat 3) adalah pasal yang paling kontroversial dan sering disebut sebagai "pasal karet". Penerapannya harus sangat hati-hati dan idealnya untuk delik aduan, bukan delik biasa.

🕮 12.3 Regulasi di Indonesia: UU Perlindungan Data Pribadi (UU PDP)

Setelah bertahun-tahun dinantikan, Indonesia akhirnya memiliki **Undang-Undang Perlindungan Data Pribadi (UU PDP)** yaitu UU No. 27 Tahun 2022. UU ini memberikan kerangka hukum yang komprehensif untuk melindungi data pribadi warga negara.

12.3.1 Definisi Data Pribadi

UU PDP membagi data pribadi menjadi dua jenis:

Jenis Data Pribadi	Contoh
Data Pribadi Bersifat Spesifik (Lebih sensitif, perlindungan lebih ketat)	Data kesehatan, data biometrik (sidik jari, wajah), data genetika, kehidupan/orientasi seksual, pandangan politik, catatan kriminal, data anak.
Data Pribadi Bersifat Umum	Nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang. (Dalam praktiknya, data seperti nomor telepon, alamat email, alamat rumah, nomor KTP juga termasuk dalam kategori yang dilindungi).

12.3.2 Hak-Hak Pemilik Data Pribadi

UU PDP memberikan sejumlah hak kepada subjek data (pemilik data pribadi), antara lain:

- Hak untuk mendapatkan informasi tentang kejelasan identitas, kepentingan, dan tujuan pemrosesan data.
- Hak untuk melengkapi, memperbarui, dan/atau memperbaiki kesalahan data.
- Hak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadinya.
- Hak untuk menarik persetujuan yang telah diberikan.
- Hak untuk menggugat dan menerima ganti rugi atas pelanggaran data pribadi.

12.3.3 Kewajiban Pengendali Data (Organisasi)

Bagi organisasi yang mengumpulkan dan memproses data pribadi (disebut Pengendali Data), UU PDP mewajibkan untuk:

1. **Memiliki Dasar Pemrosesan yang Sah:** Data hanya boleh diproses jika ada persetujuan eksplisit dari pemilik data, atau untuk memenuhi kewajiban kontrak/hukum.
2. **Menjaga Kerahasiaan Data:** Wajib melindungi dan menjaga kerahasiaan data pribadi yang diproses.
3. **Mencatat dan Mendokumentasikan:** Wajib mencatat seluruh aktivitas pemrosesan data pribadi.
4. **Memberitahukan Jika Terjadi Kebocoran:** Dalam hal terjadi kegagalan pelindungan data pribadi (bocor), Pengendali Data wajib memberitahukan secara tertulis kepada pemilik data dan kepada lembaga pengawas (nanti akan dibentuk) paling lambat 3 x 24 jam.
5. **Menunjuk Petugas Pelindungan Data Pribadi:** Untuk jenis pemrosesan tertentu (skala besar, data sensitif), wajib menunjuk pejabat atau petugas yang mengurusi PDP.

12.3.4 Sanksi

UU PDP mengatur sanksi yang berat bagi pelanggar, baik berupa sanksi administratif (teguran tertulis, denda administratif) maupun sanksi pidana.

- **Denda Administratif:** Maksimal 2% dari pendapatan tahunan terhadap pelanggaran tertentu.
- **Pidana Penjara:** Untuk pelanggaran seperti memperoleh/mengumpulkan data pribadi secara ilegal (penjara maksimal 5 tahun), atau memalsukan data pribadi (penjara maksimal 6 tahun).

Implikasi bagi Profesional Keamanan:

UU PDP membuat keamanan informasi bukan lagi sekadar pilihan, tetapi **kewajiban hukum**. Jika organisasi lalai sehingga terjadi kebocoran data, organisasi dan pengurusnya dapat dikenai sanksi pidana dan denda besar. Ini adalah alasan bisnis yang kuat untuk berinvestasi pada keamanan.

🕮 12.4 Cyber Crime dan Tantangan Penegakan Hukum

Cyber crime atau kejahatan siber adalah semua tindakan ilegal yang menggunakan komputer, jaringan, atau perangkat digital sebagai alat, target, atau tempat kejahatan.

Klasifikasi Cyber Crime:

1. **Kejahatan di mana komputer menjadi target:** Hacking, DDoS, malware, defacement website. (Ini yang paling relevan dengan Pasal 30-35 UU ITE).
2. **Kejahatan di mana komputer menjadi alat:** Penipuan online (phishing), carding, pencurian identitas, penyebaran konten ilegal (Pasal 27-29 UU ITE).
3. **Kejahatan di mana komputer menjadi tempat:** Forum gelap (dark web) untuk jual beli narkoba, senjata, data curian.

Tantangan Penegakan Hukum Siber di Indonesia:

- **Yurisdiksi:** Penyerang bisa berada di negara lain, menyulitkan proses penyelidikan dan penangkapan.
- **Anonimitas:** Penyerang menggunakan teknologi seperti VPN, Tor, dan proxy untuk menyembunyikan identitas.
- **Alat Bukti Digital:** Barang bukti digital mudah diubah, dihapus, atau dipindahkan. Diperlukan ahli forensik digital untuk mengamankannya.
- **Literasi Hukum dan Teknologi:** Aparat penegak hukum (polisi, jaksa, hakim) perlu pemahaman yang memadai tentang teknologi untuk menangani kasus siber secara efektif.

🕮 12.5 Etika Profesional dalam Keamanan Informasi

Selain hukum, ada batasan lain yang lebih samar tetapi sama pentingnya: **etika**. Etika adalah prinsip moral yang membedakan antara perilaku yang benar dan salah. Seorang profesional keamanan informasi sering menghadapi situasi di mana hukum diam, tetapi hati nurani berbicara.

12.5.1 Dilema Etika dalam Keamanan Informasi

Dilema 1: Ethical Hacking vs. Hacking Ilegal

- **Situasi:** Seorang mahasiswa menemukan celah keamanan di situs web universitasnya. Ia dapat dengan mudah mengexploitasi celah itu untuk mengubah nilai atau mencuri data.
- **Pertanyaan Etis:** Apakah cukup dengan melaporkan celah itu kepada administrator? Atau apakah ia perlu "membuktikan" dengan mencoba masuk (tetapi tidak merusak) agar laporannya dianggap serius? Di mana batas antara penelitian keamanan yang etis dan akses ilegal (Pasal 30 UU ITE)?
- **Panduan Etis: Responsible Disclosure.** Seorang periset etis (white hat) akan melaporkan temuan kerentanan kepada pemilik sistem secara pribadi, memberikan waktu yang cukup untuk memperbaikinya, dan tidak mempublikasikannya sebelum diperbaiki. Ia **tidak akan** mengexploitasi celah untuk keuntungan pribadi atau merusak data.

Dilema 2: Whistleblowing

- **Situasi:** Seorang karyawan di sebuah perusahaan fintech mengetahui bahwa perusahaan secara diam-diam menjual data pribadi pelanggan kepada pihak ketiga tanpa persetujuan, melanggar UU PDP. Manajemen menolak untuk berhenti.
- **Pertanyaan Etis:** Apakah karyawan tersebut harus membocorkan informasi ini ke publik (whistleblowing) untuk melindungi pelanggan, meskipun itu berarti melanggar kontrak kerja dan berpotensi merusak perusahaannya? Atau apakah ia harus diam saja?
- **Panduan Etis:** Whistleblowing adalah dilema besar. Umumnya, langkah yang etis adalah mencoba menyelesaikan masalah secara internal terlebih dahulu. Jika gagal, dan dampak pelanggaran sangat serius (membahayakan banyak orang, melanggar hukum), maka whistleblowing dapat dipertimbangkan, tetapi harus siap dengan konsekuensinya.

Dilema 3: Pemantauan Karyawan (Privacy vs. Security)

- **Situasi:** Perusahaan ingin memasang software yang merekam semua aktivitas karyawan di komputer kantor, termasuk email, chat, dan situs yang dikunjungi. Tujuannya untuk mencegah kebocoran data.

- **Pertanyaan Etis:** Sejauh mana perusahaan boleh melanggar privasi karyawan demi keamanan?
- **Panduan Etis:** Keseimbangan. Kebijakan pemantauan harus diungkapkan secara transparan kepada karyawan (misal: dalam AUP). Pemantauan harus proporsional dan untuk tujuan bisnis yang sah, bukan untuk mengintimidasi. Idealnya, pemantauan fokus pada aktivitas yang berisiko, bukan pada semua detail.

12.5.2 Kode Etik Profesional

Organisasi profesi keamanan informasi, seperti **(ISC)²** (International Information System Security Certification Consortium), memiliki kode etik yang harus dipatuhi oleh para anggotanya. Kode etik (ISC)² memiliki empat kanon utama, yang harus dipatuhi dalam urutan prioritas:

1. **Lindungi masyarakat, kepentingan umum, dan kepercayaan publik.**
2. **Bertindaklah dengan cara yang terhormat, jujur, adil, bertanggung jawab, dan patuh hukum.**
3. **Berikan pelayanan yang tekun dan kompeten kepada pemberi kerja/pelanggan.**
4. **Kembangkan dan tingkatkan profesi.**

Prioritas pertama adalah masyarakat umum. Ini berarti, jika ada konflik antara kepentingan perusahaan dan keselamatan publik, seorang profesional beretika harus memprioritaskan publik.

💡 12.6 Studi Kasus: Analisis Pelanggaran Hukum Siber

Kasus 1: Peretasan Situs Pemerintah (Pasal 30 UU ITE)

Kronologi: Seorang hacker berinisial "Jaka" berhasil masuk ke situs resmi sebuah kementerian dan mengubah halaman utama (deface) menjadi pesan protes politik. Ia hanya mengubah tampilan, tidak mencuri data. Ia kemudian memposting tangkapan layar di media sosial.

Analisis:

- **Tindakan:** Mengakses sistem elektronik milik pemerintah tanpa hak (Pasal 30 UU ITE). Memindahkan/mengubah informasi elektronik (Pasal 32 UU ITE).
- **Dampak:** Reputasi kementerian tercoreng, masyarakat sempat tidak bisa mengakses informasi resmi.
- **Putusan (Hipotetis):** Jaka dapat dituntut dengan Pasal 30 dan 32 UU ITE. Ancaman hukuman penjara hingga 8 tahun. Motif protes politik mungkin menjadi pertimbangan hakim, tetapi tidak menghapus unsur pidana.

Kasus 2: Jual Beli Data Pribadi (UU PDP dan UU ITE)

Kronologi: Seorang oknum karyawan call center sebuah perusahaan e-commerce menjual data ribuan pelanggan (nama, nomor telepon, alamat) kepada pihak ketiga yang diduga adalah penipu. Data dijual melalui forum online.

Analisis:

- **Tindakan:** Mengakses dan mengambil data pribadi tanpa hak (melanggar UU PDP). Mendistribusikan informasi elektronik yang tidak berhak didistribusikan (Pasal 32 UU ITe).
- **Dampak:** Pelanggan korban penipuan. Perusahaan kehilangan kepercayaan dan dikenai sanksi oleh regulator.
- **Putusan (Hipotetis):** Karyawan dapat dituntut pidana berdasarkan UU PDP (memperoleh/mengumpulkan data pribadi secara ilegal) dan UU ITE. Perusahaan juga dapat dikenai sanksi administratif berat karena gagal menjaga kerahasiaan data.

Kasus 3: Ujaran Kebencian di Media Sosial (Pasal 28 Ayat 2 UU ITE)

Kronologi: Seorang pengguna media sosial membuat dan menyebarkan konten yang mengandung hasutan kebencian terhadap kelompok agama tertentu, yang memicu keributan di dunia nyata.

Analisis:

- **Tindakan:** Sengaja menyebarkan informasi yang menimbulkan rasa kebencian berdasarkan SARA.
- **Dampak:** Perpecahan sosial, potensi konflik horizontal.

- **Putusan (Hipotetis):** Pelaku dapat dituntut dengan Pasal 28 Ayat (2) UU ITE dengan ancaman penjara hingga 6 tahun.

🗝 12.7 Rangkuman

1. **UU ITE** adalah payung hukum utama untuk aktivitas digital di Indonesia, mengatur akses ilegal (Pasal 30), penyadapan (Pasal 31), perusakan data (Pasal 32), dan konten ilegal (Pasal 27-29).
2. **UU PDP** (UU No. 27/2022) memberikan perlindungan komprehensif bagi data pribadi. Organisasi wajib menjaga kerahasiaan data, memberitahu jika terjadi kebocoran, dan dapat dikenai sanksi berat jika lalai.
3. **Cyber crime** adalah kejahatan yang menggunakan komputer sebagai target, alat, atau tempat.
4. **Etika profesional** sangat penting. Dilema seperti *ethical hacking*, *whistleblowing*, dan pemantauan karyawan membutuhkan pertimbangan moral yang matang.
5. Kode etik profesi, seperti dari $(ISC)^2$, menempatkan **perlindungan masyarakat dan kepentingan publik** sebagai prioritas tertinggi.

✍ 12.8 Latihan Soal

1. Sebutkan tiga pasal dalam UU ITE yang mengatur tentang akses ilegal dan jelaskan ancaman pidananya.
2. Apa yang dimaksud dengan "data pribadi bersifat spesifik" dalam UU PDP? Berikan tiga contoh.
3. Seorang teman Anda menemukan celah keamanan di situs web kampus. Ia ingin mencoba masuk "iseng-iseng" untuk membuktikan bahwa celah itu benar-benar bisa dieksploitasi. Nasihat apa yang akan Anda berikan berdasarkan etika dan hukum?
4. Jelaskan dilema antara keamanan dan privasi dalam konteks pemantauan karyawan. Bagaimana seharusnya perusahaan menyikapinya?

📝 12.9 Tugas Mandiri 1 (Bobot 2%)

Instruksi:
Analisis sebuah kasus pelanggaran hukum siber.

Langkah Tugas:

1. Carilah **satu berita kasus** (dari media online terpercaya) tentang pelanggaran yang terkait dengan UU ITE atau UU PDP di Indonesia dalam 2 tahun terakhir.
2. Buatlah ringkasan kasus (apa yang terjadi, siapa pelaku, siapa korban, kronologi singkat).
3. Identifikasi **pasal-pasal dalam UU ITE atau UU PDP** yang dilanggar berdasarkan tindakan dalam kasus tersebut. Jelaskan mengapa pasal itu relevan.
4. Analisis **dampak** dari kasus tersebut terhadap korban dan masyarakat.
5. Berikan **pendapat Anda** tentang putusan (jika sudah ada putusan) atau tentang bagaimana kasus tersebut seharusnya ditangani.

Format Penugasan:

- Laporan dalam format PDF, maksimal 2 halaman.
- Sertakan tautan/link berita asli.

📝 12.10 Tugas Mandiri 2 (Bobot 2%)

Instruksi:
Tugas ini adalah tugas kelompok untuk presentasi. Bentuk kelompok (3-4 orang). Pilih salah satu topik tren keamanan terkini berikut:

1. **Keamanan AI (Artificial Intelligence):** Ancaman dan peluang keamanan dari penggunaan AI (misal: AI untuk serangan phishing yang lebih canggih, atau AI untuk deteksi ancaman).

2. **Keamanan IoT (Internet of Things):** Tantangan keamanan pada perangkat pintar (smart home, perangkat medis terhubung) dan bagaimana melindunginya.
3. **Keamanan Cloud:** Tanggung jawab bersama (shared responsibility model) antara penyedia cloud dan pengguna, serta risiko keamanan spesifik cloud.
4. **Tantangan Kepatuhan di Era Digital:** Bagaimana organisasi mempersiapkan diri untuk mematuhi UU PDP dan regulasi global seperti GDPR (jika beroperasi secara internasional).

Langkah Tugas:

1. **Riset:** Kumpulkan informasi tentang topik pilihan Anda dari sumber terpercaya (jurnal, laporan industri, artikel ahli).
2. **Buat Slide Presentasi:** Siapkan presentasi dengan struktur:
   - **Pendahuluan:** Apa topiknya dan mengapa penting?
   - **Analisis:** Jelaskan secara mendalam tentang topik tersebut. Untuk topik AI/IoT/Cloud: apa saja ancaman utamanya? Bagaimana cara mitigasinya? Untuk topik kepatuhan: apa saja tantangan implementasi UU PDP? Apa yang harus dilakukan organisasi?
   - **Implikasi:** Bagaimana tren ini mempengaruhi praktik keamanan informasi di masa depan? Apa implikasi kepatuhannya terhadap regulasi?
   - **Studi Kasus (opsional):** Berikan contoh nyata jika ada.
   - **Kesimpulan dan Rekomendasi.**
3. **Presentasikan:** Siapkan presentasi selama 10-15 menit per kelompok. Semua anggota harus berbicara.

Penilaian:

- **Kualitas Presentasi (40%):** Kejelasan, sistematika, komunikasi, media yang menarik.
- **Kedalaman Analisis Tren (30%):** Kemampuan menjelaskan tren, dampak, tantangan, dan peluang.
- **Implikasi Kepatuhan (30%):** Kemampuan mengaitkan tren dengan aspek kepatuhan terhadap regulasi/standar.

📚 DAFTAR PUSTAKA

- Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson. (Untuk bab jaringan)
- Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning. (Untuk bab jaringan dan etika)
- OWASP Foundation. (2021). *OWASP Top Ten - 2021*. The Open Web Application Security Project.
- Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Easttom, C. (2021). *Computer Security Fundamentals* (5th ed.). Pearson.
- Kim, D., & Solomon, M. G. (2021). *Fundamentals of Information Systems Security* (4th ed.). Jones & Bartlett Learning.
- $(ISC)^2$ Code of Ethics. Tersedia di situs web $(ISC)^2$.

PENUTUP

Selamat! Anda telah menyelesaikan seluruh materi dalam bahan ajar **Keamanan Sistem Informasi**. Perjalanan panjang ini telah membawa Anda dari fondasi paling dasar (CIA Triad) hingga ke aspek teknis (jaringan, aplikasi, kriptografi) dan non-teknis (manajemen risiko, kebijakan, hukum, etika).

Ingatlah bahwa keamanan informasi adalah **perjalanan, bukan tujuan akhir**. Ancaman terus berevolusi, teknologi terus berkembang, dan regulasi terus diperbarui. Sebagai lulusan program studi Manajemen Informatika, Anda diharapkan tidak hanya menjadi pengguna teknologi yang pasif, tetapi juga menjadi pemikir kritis yang mampu menganalisis risiko, merancang solusi, dan menjunjung tinggi etika profesi.

Teruslah belajar, teruslah ingin tahu, dan selalu ingat prinsip utama: **Lindungi data, lindungi manusia, lindungi kepercayaan.**

DAFTAR PUSTAKA

Buku Teks Utama

Easttom, C. (2021). *Computer Security Fundamentals* (5th ed.). Pearson.

Kim, D., & Solomon, M. G. (2021). *Fundamentals of Information Systems Security* (4th ed.). Jones & Bartlett Learning.

Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.

Vacca, J. R. (2020). *Computer and Information Security Handbook* (3rd ed.). Morgan Kaufmann.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.

Standar dan Framework

ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*. National Institute of Standards and Technology.

OWASP Foundation. (2021). *OWASP Top Ten - 2021*. The Open Web Application Security Project. Diambil dari https://owasp.org/Top10/

Regulasi dan Perundang-undangan

Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara RI Tahun 2016, No. 251. Sekretariat Negara. Jakarta.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara RI Tahun 2022, No. 196. Sekretariat Negara. Jakarta.

Sumber Pendukung dan Referensi Lainnya

(ISC)². (2024). *(ISC)² Code of Ethics*. Diambil dari https://www.isc2.org/Ethics

Dokumentasi dan publikasi dari berbagai penyedia layanan keamanan, otoritas sertifikat (seperti Let's Encrypt, DigiCert), dan organisasi riset keamanan.

GLOSARIUM

A

Access Control (Kontrol Akses)
Mekanisme untuk membatasi akses ke sumber daya (data, sistem, jaringan) hanya kepada pihak yang berwenang.

Ancaman (Threat)
Potensi penyebab insiden yang dapat mengakibatkan kerugian atau kerusakan pada aset informasi. (Bab 2)

Aset Informasi (Information Asset)
Segala sesuatu yang memiliki nilai bagi organisasi dan perlu dilindungi, termasuk data, perangkat lunak, perangkat keras, dan sumber daya manusia. (Bab 2, Bab 7)

Asimetris (Kriptografi)
Metode kriptografi yang menggunakan sepasang kunci berbeda: kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Contoh: RSA. (Bab 4)

AUP (Acceptable Use Policy)
Kebijakan yang mengatur penggunaan aset TI organisasi yang dapat diterima oleh karyawan. (Bab 9)

Availability (Ketersediaan)
Prinsip dalam CIA Triad yang memastikan informasi dan sistem dapat diakses oleh pihak berwenang saat dibutuhkan. (Bab 1)

B

Broken Access Control
Kerentanan keamanan aplikasi di mana mekanisme pembatasan akses tidak berfungsi dengan baik, memungkinkan pengguna mengakses data atau fungsi di luar haknya. (Bab 11)

C

CA (Certificate Authority)
Entitas tepercaya yang menerbitkan dan mengelola sertifikat digital. (Bab 6)

Chain of Trust (Rantai Kepercayaan)
Hierarki sertifikat digital yang menghubungkan sertifikat entitas akhir ke Root CA yang tepercaya. (Bab 6)

CIA Triad
Tiga pilar utama keamanan informasi: Confidentiality (Kerahasiaan), Integrity (Integritas), dan Availability (Ketersediaan). (Bab 1)

Ciphertext
Pesan yang telah dienkripsi dan tidak dapat dibaca secara langsung. (Bab 4)

Confidentiality (Kerahasiaan)
Prinsip dalam CIA Triad yang memastikan informasi hanya dapat diakses oleh pihak yang berwenang. (Bab 1)

Cryptographic Failures
Kerentanan akibat kegagalan dalam implementasi kriptografi, seperti penggunaan algoritma lemah atau tidak mengenkripsi data sensitif. (Bab 11)

D

DDoS (Distributed Denial of Service)
Serangan yang membanjiri server atau jaringan dengan lalu lintas palsu dari banyak sumber sehingga sistem tidak dapat melayani pengguna sah. (Bab 2)

Defense in Depth
Strategi keamanan berlapis yang menggunakan kombinasi berbagai jenis kontrol (administratif, teknis, fisik) untuk melindungi aset. (Bab 8)

Digital Signature (Tanda Tangan Digital)
Mekanisme kriptografi untuk membuktikan keaslian dan integritas dokumen elektronik, serta memberikan non-repudiasi. (Bab 5)

DMZ (Demilitarized Zone)
Subnet jaringan yang memisahkan jaringan internal dari internet, tempat server publik ditempatkan. (Bab 10)

E

EISP (Enterprise Information Security Policy)
Kebijakan keamanan tingkat tertinggi yang mendefinisikan visi, misi, dan arahan strategis keamanan informasi di seluruh organisasi. (Bab 9)

Enkripsi
Proses mengubah plaintext menjadi ciphertext menggunakan algoritma dan kunci. (Bab 4)

Ethical Hacking
Praktik menguji keamanan sistem dengan izin pemilik untuk menemukan kerentanan, berbeda dengan hacking ilegal. (Bab 12)

F

Firewall
Sistem keamanan jaringan yang memfilter lalu lintas berdasarkan aturan yang ditetapkan. (Bab 10)

H

Hash (Fungsi Hash)
Fungsi satu arah yang mengubah input dengan ukuran berapa pun menjadi output dengan ukuran tetap (nilai hash) yang unik untuk setiap input. (Bab 5)

HTTPS (Hypertext Transfer Protocol Secure)
Versi aman dari HTTP yang menggunakan enkripsi SSL/TLS untuk melindungi komunikasi antara browser dan server web. (Bab 4, Bab 6)

I

IDS (Intrusion Detection System)
Sistem yang memantau lalu lintas jaringan dan memberikan peringatan jika mendeteksi aktivitas mencurigakan. (Bab 10)

Integrity (Integritas)
Prinsip dalam CIA Triad yang memastikan informasi akurat, utuh, dan tidak diubah oleh pihak tidak berwenang. (Bab 1)

Injection
Kerentanan di mana data tidak tepercaya dikirim ke interpreter sebagai bagian dari perintah atau query. Contoh: SQL Injection. (Bab 11)

IPS (Intrusion Prevention System)
Sistem yang memantau lalu lintas jaringan dan secara aktif memblokir lalu lintas berbahaya. (Bab 10)

ISSP (Issue-Specific Security Policy)
Kebijakan yang membahas isu keamanan tertentu secara rinci, seperti kebijakan kata sandi atau kebijakan email. (Bab 9)

K

Kerentanan (Vulnerability)
Kelemahan dalam sistem, prosedur, atau kontrol yang dapat dieksploitasi oleh ancaman. (Bab 2)

Kriptografi
Seni dan ilmu menjaga kerahasiaan pesan dengan mengubahnya menjadi format yang tidak dapat dipahami. (Bab 4)

M

Malware (Malicious Software)
Perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mendapatkan akses tidak sah. (Bab 2)

Man-in-the-Middle (MitM)
Serangan di mana penyerang diam-diam menyadap dan berpotensi mengubah komunikasi antara dua pihak. (Bab 2)

Manajemen Risiko (Risk Management)
Proses sistematis untuk mengidentifikasi, menganalisis, mengevaluasi, dan menangani risiko. (Bab 7)

Matriks Risiko (Risk Matrix)
Alat visual untuk memetakan risiko berdasarkan tingkat kemungkinan (likelihood) dan dampak (impact). (Bab 7)

N

NIST Cybersecurity Framework
Framework sukarela berbasis risiko untuk mengelola keamanan siber, dikembangkan oleh National Institute of Standards and Technology. (Bab 3)

Non-Repudiasi (Non-Repudiation)
Kemampuan untuk mencegah seseorang menyangkal telah melakukan suatu tindakan, seperti mengirim pesan. (Bab 4)

O

OWASP Top 10
Daftar 10 risiko keamanan aplikasi web paling kritis yang diterbitkan oleh Open Web Application Security Project. (Bab 11)

P

Parameterized Query (Prepared Statement)
Teknik pemrograman untuk mencegah SQL Injection dengan memisahkan kode SQL dari data input pengguna. (Bab 11)

Password Policy
Kebijakan yang mengatur pembuatan, penggunaan, dan perlindungan kata sandi. (Bab 9)

PDCA (Plan-Do-Check-Act)
Siklus manajemen berkelanjutan yang digunakan dalam ISO 27001. (Bab 3)

Phishing
Serangan social engineering yang menggunakan email palsu untuk mengelabui korban agar memberikan informasi sensitif. (Bab 2)

PKI (Public Key Infrastructure)
Infrastruktur yang diperlukan untuk membuat, mengelola, mendistribusikan, menggunakan, menyimpan, dan mencabut sertifikat digital. (Bab 6)

Plaintext
Pesan asli yang dapat dibaca sebelum dienkripsi. (Bab 4)

R

Ransomware
Jenis malware yang mengenkripsi data korban dan meminta tebusan untuk mengembalikan akses. (Bab 2)

Risk Treatment (Perlakuan Risiko)
Langkah-langkah untuk menangani risiko: mitigasi, transfer, hindari, atau terima. (Bab 7)

S

Secure Coding
Praktik menulis kode program dengan mempertimbangkan aspek keamanan untuk mencegah kerentanan. (Bab 11)

Segmentasi Jaringan
Praktik membagi jaringan besar menjadi sub-jaringan yang lebih kecil untuk membatasi pergerakan penyerang. (Bab 10)

Sertifikat Digital (Digital Certificate)
Dokumen elektronik yang mengikat kunci publik dengan identitas pemiliknya, diterbitkan oleh CA. (Bab 6)

Simetris (Kriptografi)
Metode kriptografi yang menggunakan satu kunci yang sama untuk enkripsi dan dekripsi. Contoh: AES. (Bab 4)

Social Engineering
Serangan yang memanipulasi psikologi manusia untuk mendapatkan akses atau informasi. (Bab 2)

SQL Injection
Jenis serangan injection yang menargetkan database dengan menyisipkan perintah SQL berbahaya. (Bab 11)

SSL/TLS
Protokol kriptografi untuk komunikasi aman di internet, fondasi dari HTTPS. (Bab 6, Bab 10)

Standar (Standard)
Dokumen yang menetapkan persyaratan wajib, spesifik, dan terukur untuk implementasi keamanan. (Bab 9)

SysSP (System-Specific Security Policy)
Kebijakan teknis yang sangat spesifik untuk suatu sistem, aplikasi, atau perangkat tertentu. (Bab 9)

U

UU ITE (Undang-Undang Informasi dan Transaksi Elektronik)
Payung hukum utama untuk aktivitas digital di Indonesia, mengatur akses ilegal, penyadapan, dan konten ilegal. (Bab 12)

UU PDP (Undang-Undang Pelindungan Data Pribadi)
Undang-undang yang mengatur perlindungan data pribadi warga negara Indonesia. (Bab 12)

V

VPN (Virtual Private Network)
Teknologi yang menciptakan koneksi aman dan terenkripsi melalui jaringan publik. (Bab 10)

W

Whistleblowing
Tindakan membocorkan informasi tentang pelanggaran atau kejahatan di dalam organisasi kepada publik atau otoritas. (Bab 12)

Z

Zero Trust Architecture
Model keamanan dengan prinsip "never trust, always verify", tidak mengandalkan perimeter jaringan. (Bab 10)

INDEKS

F

H

I

J

K

M

N

O

P

R

S

T

LAMPIRAN

LAMPIRAN A: CONTOH STUDI KASUS LENGKAP

Studi Kasus 1: Kebocoran Data Pelanggan E-commerce

Kronologi Lengkap:
Pada bulan Oktober 2024, perusahaan e-commerce fiktif "BeliMurah" mengalami insiden keamanan yang mengakibatkan kebocoran data sekitar 2 juta pelanggan. Insiden ini diketahui ketika seorang pengguna forum dark web menawarkan database berisi nama lengkap, alamat email, nomor telepon, alamat pengiriman, dan hash kata sandi pelanggan BeliMurah.

Investigasi awal mengungkapkan bahwa serangan bermula dari celah keamanan pada API (Application Programming Interface) yang digunakan untuk aplikasi mobile BeliMurah. API tersebut tidak memiliki mekanisme rate-limiting yang memadai, sehingga penyerang dapat melakukan scraping data secara otomatis dengan menggunakan teknik credential stuffing (menggunakan kombinasi email dan kata sandi yang bocor dari situs lain).

Setelah berhasil mendapatkan akses sebagai pengguna terdaftar, penyerang menemukan kerentanan IDOR (Insecure Direct Object References) pada endpoint API yang memungkinkannya mengakses data pelanggan lain hanya dengan mengubah parameter ID pengguna di URL.

Kronologi Waktu:
- **H-30:** Seorang periset keamanan melaporkan celah API melalui email dukungan BeliMurah, namun tidak mendapat respons.
- **H-7:** Penyerang mulai mengexploitasi celah secara sistematis.
- **H-1:** Data berhasil dikumpulkan dan mulai dijual di dark web.
- **H+0:** Seorang jurnalis teknologi menghubungi BeliMurah untuk meminta konfirmasi.
- **H+2:** BeliMurah mengeluarkan siaran pers dan meminta seluruh pelanggan mengganti kata sandi.

Dampak:
- **Finansial:** Potensi denda dari regulator (UU PDP) hingga miliaran rupiah.
- **Reputasi:** Kepercayaan pelanggan menurun, tagar #BoikotBeliMurah sempat menjadi trending topic di media sosial.
- **Operasional:** Tim IT harus bekerja lembur untuk menambal celah dan mengaudit seluruh sistem.

- **Hukum:** Beberapa pelanggan menggugat secara class action.

Pertanyaan Analisis:
1. Dari perspektif CIA Triad, pilar mana saja yang dilanggar? Jelaskan.
2. Kerentanan OWASP apa saja yang dieksploitasi dalam kasus ini?
3. Langkah-langkah preventif apa yang seharusnya dilakukan BeliMurah untuk mencegah insiden ini?
4. Berdasarkan UU PDP, kewajiban apa yang harus dipenuhi BeliMurah pasca insiden ini?

Studi Kasus 2: Serangan Ransomware pada Rumah Sakit

Kronologi Lengkap:
Rumah Sakit "SehatSentosa" adalah rumah sakit tipe B dengan 200 tempat tidur dan melayani rata-rata 500 pasien per hari. Pada suatu Senin pagi, seluruh sistem informasi rumah sakit tiba-tiba tidak dapat diakses. Di layar komputer muncul pesan:

"Semua file Anda telah dienkripsi. Untuk mendapatkan kunci dekripsi, hubungi kami di [alamat email dark web] dan bayar 50 Bitcoin (sekitar Rp 50 miliar). Anda memiliki waktu 72 jam sebelum kunci dihancurkan."

Investigasi menemukan bahwa serangan bermula dari email phishing yang diklik oleh seorang staf administrasi pada Jumat sore. Email tersebut berpura-pura menjadi undangan seminar kesehatan dari Kementerian Kesehatan. Lampiran berupa dokumen Word yang jika dibuka akan menjalankan makro berbahaya yang mengunduh ransomware.

Karena jaringan rumah sakit tidak tersegmentasi dengan baik, ransomware menyebar dengan cepat dari komputer staf administrasi ke server rekam medis, server laboratorium, dan sistem radiologi. Backup yang ada ternyata juga ikut terenkripsi karena media backup terhubung secara permanen ke jaringan.

Dampak:
- **Pelayanan Pasien:** Seluruh jadwal operasi ditunda. Pasien gawat darurat harus dirujuk ke rumah sakit lain. Rekam medis tidak bisa diakses, sehingga dokter kesulitan mengetahui riwayat penyakit pasien.
- **Finansial:** Rumah sakit akhirnya membayar tebusan sebesar 30 Bitcoin (setelah negosiasi). Biaya pemulihan sistem mencapai miliaran rupiah.
- **Hukum:** Rumah sakit dilaporkan ke Kemenkes dan kepolisian karena diduga lalai melindungi data pasien.

Pertanyaan Analisis:

1. Identifikasi vektor serangan (attack vector) dalam kasus ini.
2. Kontrol keamanan apa yang gagal (baik preventif, detektif, maupun korektif)?
3. Bagaimana seharusnya strategi backup yang baik untuk mencegah backup ikut terenkripsi?
4. Analisis aspek hukum dan etika dari keputusan rumah sakit membayar tebusan.

LAMPIRAN B: TEMPLATE DOKUMEN

Template B.1: Matriks Analisis Risiko

No	Aset	Deskripsi Aset	Nilai Aset (1-3)	Ancaman	Kerentanan	Likelihood (1-3)	Impact (1-3)	Tingkat Risiko (L×I)	Prioritas (R/S/T)	Opsi Perlakuan	Kontrol yang Diusulkan
1											
2											
3											
4											
5											

Petunjuk Pengisian:

- **Nilai Aset:** 1 = Rendah, 2 = Sedang, 3 = Tinggi (berdasarkan kepentingan bagi organisasi)
- **Likelihood (Kemungkinan):** 1 = Rendah, 2 = Sedang, 3 = Tinggi
- **Impact (Dampak):** 1 = Rendah, 2 = Sedang, 3 = Tinggi
- **Prioritas:** R = Rendah (1-2), S = Sedang (3-4), T = Tinggi (6-9)
- **Opsi Perlakuan:** Mitigasi, Transfer, Hindari, Terima

Template B.2: Format Kebijakan Keamanan (ISSP)

Logo Perusahaan

[NAMA PERUSAHAAN]

KEBIJAKAN [JUDUL KEBIJAKAN]

Nomor Dokumen	: [KODE/XXX/YYYY]
Versi	: [1.0]
Tanggal Efektif	: [DD/MM/YYYY]
Tanggal Revisi	: [DD/MM/YYYY]
Disediakan oleh	: [Jabatan]
Disetujui oleh	: [Jabatan]

---

1. TUJUAN

[Tuliskan tujuan kebijakan ini dibuat. Jelaskan mengapa kebijakan ini penting bagi organisasi dan apa yang ingin dicapai.]

Contoh: Kebijakan ini bertujuan untuk memastikan bahwa seluruh penggunaan aset teknologi informasi perusahaan dilakukan secara aman, etis, dan sesuai dengan peraturan yang berlaku.

---

2. RUANG LINGKUP

[jelaskan kepada siapa kebijakan ini berlaku dan pada sistem apa saja.]

Contoh: Kebijakan ini berlaku bagi seluruh karyawan tetap, karyawan kontrak, konsultan, dan pihak ketiga yang memiliki akses ke sistem informasi PT Maju Jaya.

---

3. DEFINISI

[Definisikan istilah-istilah kunci yang digunakan dalam kebijakan untuk menghindari ambiguitas.]

Istilah	Definisi

---

4. PERNYATAAN KEBIJAKAN

[Bagian ini berisi aturan-aturan spesifik yang harus dipatuhi. Gunakan bahasa yang jelas, tegas, dan tidak ambigu.]

4.1 [Sub-bab 1]

- [Aturan 1]
- [Aturan 2]

4.2 [Sub-bab 2]

- [Aturan 1]
- [Aturan 2]

---

5. PENEGAKAN DAN SANKSI

[Jelaskan konsekuensi jika kebijakan dilanggar.]

Contoh: Pelanggaran terhadap kebijakan ini akan dikenakan sanksi disipliner sesuai dengan Peraturan Perusahaan, mulai dari teguran tertulis, pemutusan akses, hingga pemutusan hubungan kerja.

---

6. TANGGUNG JAWAB

[Siapa yang bertanggung jawab atas implementasi, sosialisasi, dan penegakan kebijakan?]

Pihak	Tanggung Jawab

---

7. INFORMASI TERKAIT

[Dokumen lain yang terkait dengan kebijakan ini, jika ada.]

- [Nama Dokumen 1]
- [Nama Dokumen 2]

---

8. RIWAYAT REVISI

Versi	Tanggal	Deskripsi Perubahan	Oleh
1.0		Versi awal	

PERSETUJUAN

Dibuat oleh,	Diperiksa oleh,	Disetujui oleh,
[Nama]	**[Nama]**	**[Nama]**
[Jabatan]	**[Jabatan]**	**[Jabatan]**
Tanggal:	**Tanggal:**	**Tanggal:**

Template B.3: Format Laporan Analisis Studi Kasus

HALAMAN JUDUL

LAPORAN ANALISIS STUDI KASUS
[Judul Studi Kasus]

Mata Kuliah : Keamanan Sistem Informasi
Dosen Pengampu : Ir. H.A. Mooduto, M.Kom.

Disusun oleh:
Nama : _____
NIM : _____
Kelas : _____

JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK NEGERI PADANG
TAHUN 2026

BAB I: RINGKASAN KASUS

[Tuliskan ringkasan kasus yang dianalisis. Siapa pelaku, siapa korban, kronologi singkat, dan bagaimana kasus ini diketahui publik.]

BAB II: IDENTIFIKASI MASALAH

[Identifikasi masalah-masalah keamanan yang muncul dalam kasus ini dari berbagai perspektif.]

2.1 Identifikasi Aset yang Terdampak

- [Aset 1]
- [Aset 2]

2.2 Identifikasi Ancaman dan Kerentanan

- [Ancaman dan kerentanan yang dieksploitasi]

2.3 Analisis CIA Triad

- [Pilar CIA mana yang dilanggar dan bagaimana]

2.4 Analisis Kerentanan OWASP (jika relevan)

- [Kerentanan OWASP yang sesuai]

BAB III: ANALISIS DAMPAK

[Jelaskan dampak yang ditimbulkan oleh insiden tersebut.]

3.1 Dampak Finansial

- [Estimasi kerugian finansial]

3.2 Dampak Reputasi

- [Pengaruh terhadap kepercayaan pelanggan/masyarakat]

3.3 Dampak Operasional

- [Gangguan terhadap operasional organisasi]

3.4 Dampak Hukum

- [Potensi pelanggaran regulasi (UU ITE, UU PDP)]

BAB IV: REKOMENDASI

[Berikan rekomendasi perbaikan yang spesifik dan aplikatif.]

4.1 Rekomendasi Jangka Pendek

- [Tindakan yang harus segera dilakukan]

4.2 Rekomendasi Jangka Panjang

- [Perbaikan sistemik yang perlu diterapkan]

4.3 Rekomendasi Kontrol Keamanan

- [Kontrol administratif, teknis, dan fisik yang relevan]

BAB V: KESIMPULAN

[Kesimpulan singkat tentang pembelajaran dari kasus ini.]

DAFTAR PUSTAKA

[Sumber referensi yang digunakan, termasuk tautan berita asli jika ada.]

LAMPIRAN C: KUNCI JAWABAN LATIHAN SOAL (TERBATAS)

Bab 1: Prinsip Dasar Keamanan Informasi

Soal 1: Jelaskan dengan kata-kata Anda sendiri perbedaan antara kerahasiaan dan integritas.

Jawaban:
Kerahasiaan (Confidentiality) berkaitan dengan siapa yang boleh mengakses informasi. Informasi rahasia hanya boleh dilihat oleh pihak yang berwenang. Integritas (Integrity) berkaitan dengan keakuratan dan keutuhan informasi. Informasi harus dijaga agar tidak diubah oleh pihak tidak berwenang.

Contoh: Sebuah email yang berisi password. Kerahasiaan dilanggar jika orang lain membaca email tersebut. Integritas dilanggar jika orang lain mengubah isi email (misal: mengganti password yang dikirim).

Soal 3: Mengapa menjaga keseimbangan antara ketiga pilar CIA itu penting? Berikan contoh.

Jawaban:
Keseimbangan penting karena terlalu fokus pada satu pilar dapat merugikan pilar lain. Contoh: Sebuah bank ingin meningkatkan keamanan dengan menerapkan enkripsi yang sangat kuat dan proses verifikasi berlapis untuk setiap transaksi. Ini baik untuk kerahasiaan dan integritas. Namun, jika prosesnya terlalu lambat dan rumit, nasabah bisa frustrasi dan ketersediaan layanan terganggu. Sebaliknya, jika bank terlalu fokus pada ketersediaan (ingin transaksi secepat mungkin), mereka mungkin mengorbankan keamanan dan berisiko terjadi pencurian data.

Bab 2: Ancaman, Kerentanan, dan Serangan

Soal 1: Jelaskan perbedaan antara ancaman, kerentanan, dan serangan. Berikan analogi.

Jawaban:

- **Ancaman:** Potensi bahaya. *Analogi:* Seekor anjing galak di jalan.

- **Kerentanan:** Kelemahan yang bisa dimanfaatkan. *Analogi:* Pagar rumah yang berlubang.
- **Serangan:** Tindakan nyata memanfaatkan kelemahan. *Analogi:* Anjing galak masuk melalui lubang pagar dan menggigit.

Bab 4: Dasar-Dasar Kriptografi

Soal 2: Mengapa protokol HTTPS menggunakan kombinasi kriptografi simetris dan asimetris, bukan hanya salah satunya saja?

Jawaban:
HTTPS menggunakan kombinasi (kriptografi hibrida) karena:

- **Kriptografi asimetris** (RSA, dll) lambat tetapi aman untuk pertukaran kunci. Digunakan pada awal koneksi untuk bertukar kunci sesi (session key) secara aman.
- **Kriptografi simetris** (AES, dll) cepat dan efisien untuk mengenkripsi data dalam jumlah besar. Digunakan setelah kunci sesi didapatkan untuk mengenkripsi seluruh komunikasi selama sesi berlangsung.

Jika hanya menggunakan asimetris, koneksi akan lambat. Jika hanya menggunakan simetris, tidak ada cara aman untuk bertukar kunci di awal.

Soal 3: Jika Anda diminta memilih algoritma untuk mengenkripsi hard disk eksternal berkapasitas 1 TB, apakah Anda akan memilih AES atau RSA?

Jawaban:
Saya akan memilih **AES** (kriptografi simetris). Alasannya:

- AES dirancang untuk enkripsi data dalam jumlah besar dan sangat cepat. Hard disk 1 TB membutuhkan enkripsi yang efisien.
- RSA sangat lambat dan tidak dirancang untuk enkripsi data massal. RSA biasanya digunakan untuk mengenkripsi kunci simetris yang kecil, bukan data langsung.

Bab 7: Analisis Risiko Keamanan Informasi

Soal 2: Sebuah perusahaan memiliki risiko kebakaran di ruangan server. Dampaknya dinilai Tinggi (3), tetapi kemungkinannya Rendah (1). Berapa nilai risikonya? Masuk kategori apa? Opsi perlakuan risiko apa yang paling mungkin dipilih?

Jawaban:

- Nilai Risiko = Likelihood × Impact = 1 × 3 = **3**.
- Kategori: **Sedang** (berdasarkan matriks 3×3, nilai 3 masuk kategori sedang).
- Opsi perlakuan yang paling mungkin: **Mitigasi**. Meskipun kemungkinan rendah, dampaknya sangat tinggi. Perusahaan akan mengambil langkah-langkah mitigasi seperti memasang detektor asap, sistem pemadam kebakaran otomatis, dan melakukan backup data ke lokasi yang aman. Risiko tidak bisa ditransfer sepenuhnya (asuransi bisa membantu, tetapi data yang hilang tidak bisa diganti), dan tidak bisa dihindari (server harus tetap ada). Menerima risiko juga terlalu berisiko karena dampaknya tinggi.

Bab 11: Keamanan Aplikasi

Soal 1: Jelaskan apa itu SQL Injection dan bagaimana cara mencegahnya.

Jawaban:
SQL Injection adalah serangan di mana penyerang menyisipkan perintah SQL berbahaya melalui input pengguna (misal: form login, kotak pencarian) yang kemudian dieksekusi oleh database. Ini terjadi karena aplikasi menggabungkan input pengguna langsung ke dalam query SQL tanpa validasi atau sanitasi.

Cara mencegah:

1. **Gunakan Parameterized Query (Prepared Statement):** Ini adalah pertahanan utama. Kode SQL dipisahkan dari data input, sehingga input hanya diperlakukan sebagai data, bukan bagian dari perintah SQL.
2. **Validasi Input:** Validasi semua input di sisi server. Pastikan input sesuai dengan format yang diharapkan (misal: email harus mengandung '@').
3. **Prinsip Least Privilege:** Akun database yang digunakan aplikasi sebaiknya tidak memiliki hak administratif (seperti DROP TABLE). Beri hak seminimal mungkin (SELECT, INSERT, UPDATE saja).

4. **Escaping Input:** Jika tidak bisa menggunakan parameterized query (pada sistem lama), lakukan escaping terhadap karakter berbahaya seperti tanda kutip tunggal ('). Namun, ini kurang aman dibanding parameterized query.

Bab 12: Aspek Hukum, Etika, dan Kepatuhan

Soal 3: Seorang teman Anda menemukan celah keamanan di situs web kampus. Ia ingin mencoba masuk "iseng-iseng" untuk membuktikan bahwa celah itu benar-benar bisa dieksploitasi. Nasihat apa yang akan Anda berikan?

Jawaban:
Saya akan menasihati teman saya untuk **TIDAK melakukannya** dan menjelaskan alasannya:

1. **Aspek Hukum:** Mencoba masuk ke sistem orang lain tanpa izin adalah tindakan yang dilarang oleh **Pasal 30 UU ITE** (Akses Ilegal). Meskipun motifnya hanya "iseng" dan tidak merusak, secara hukum tetap bisa dipidana dengan ancaman penjara hingga 6 tahun.
2. **Aspek Etika:** Praktik yang benar adalah **responsible disclosure**. Teman saya seharusnya melaporkan temuan celah tersebut kepada administrator atau tim IT kampus melalui saluran resmi (email, helpdesk), memberikan detail yang cukup, dan memberikan waktu yang cukup untuk memperbaikinya.
3. **Risiko:** Tidak ada jaminan bahwa tindakan "iseng" itu tidak akan merusak data atau sistem. Bisa saja ada efek samping yang tidak terduga.

Alternatif etis: Jika teman saya tertarik dengan pengujian keamanan, ia bisa meminta izin tertulis dari pihak kampus untuk melakukan pengujian resmi (dengan ruang lingkup terbatas) atau bergabung dengan program bug bounty jika kampus memilikinya.

LAMPIRAN D: CONTOH SOAL UJIAN

Contoh Soal Ujian Tengah Semester (UTS)

Mata Kuliah : Keamanan Sistem Informasi
Waktu : 90 Menit
Sifat : Buka buku terbatas (catatan diperbolehkan)

Bagian A: Soal Teori (40%)

Jawablah pertanyaan berikut dengan singkat dan jelas.

1. Jelaskan tiga pilar CIA Triad dan berikan contoh pelanggaran untuk masing-masing pilar dalam konteks sebuah bank. (Skor 15)
2. Apa perbedaan antara ancaman (threat), kerentanan (vulnerability), dan risiko (risk)? Berikan analogi sederhana. (Skor 10)
3. Sebutkan dan jelaskan secara singkat 3 dari 5 fungsi inti dalam NIST Cybersecurity Framework. (Skor 15)

Bagian B: Studi Kasus (60%)

Baca studi kasus berikut dengan saksama, kemudian jawab pertanyaan-pertanyaan di bawahnya.

Studi Kasus: Serangan Ransomware pada "KopiNusantara"

"KopiNusantara" adalah sebuah UKM yang menjual biji kopi secara online melalui website dan marketplace. Perusahaan ini memiliki 15 karyawan. Suatu pagi, seluruh komputer di kantor menampilkan pesan yang sama:

"Semua file Anda telah dienkripsi. Termasuk database pelanggan, data keuangan, dan semua dokumen. Kirim 5 Bitcoin ke alamat ini dalam 48 jam untuk mendapatkan kunci dekripsi."

Tim IT "KopiNusantara" yang hanya terdiri dari satu orang mencoba mengatasi, tetapi tidak berhasil. Ternyata, backup yang mereka lakukan setiap minggu juga ikut terenkripsi karena hard disk backup selalu terpasang di server.

Setelah diselidiki, serangan bermula dari email yang diklik oleh salah satu staf administrasi. Email itu berpura-pura menjadi konfirmasi pesanan dari pelanggan, tetapi lampirannya berisi malware.

Pertanyaan:

1. **Identifikasi (Skor 20)**
   - Identifikasi aset-aset kritis yang terdampak dalam kasus ini.
   - Identifikasi ancaman, kerentanan, dan serangan yang terjadi.
   - Analisis pilar CIA Triad mana saja yang dilanggar. Jelaskan.
2. **Analisis (Skor 20)**
   - Jika Anda adalah konsultan keamanan, kontrol preventif apa yang seharusnya sudah diterapkan untuk mencegah serangan ini? Berikan minimal 3 kontrol (sebutkan jenisnya: administratif, teknis, atau fisik).
   - Kontrol detektif apa yang bisa membantu mendeteksi serangan lebih dini?
3. **Rekomendasi (Skor 20)**
   - Rancanglah strategi backup yang baik untuk "KopiNusantara" agar kejadian serupa tidak terulang. Jelaskan aturan 3-2-1 backup.
   - Apa yang harus dilakukan "KopiNusantara" setelah insiden ini? Berikan langkah-langkah konkret.

Contoh Soal Ujian Akhir Semester (UAS)

Mata Kuliah : Keamanan Sistem Informasi
Waktu : 90 Menit
Sifat : Buka buku terbatas (catatan diperbolehkan)

Bagian A: Soal Teori (40%)

Jawablah pertanyaan berikut dengan singkat dan jelas.

1. Jelaskan perbedaan antara IDS dan IPS. Kapan sebaiknya organisasi menggunakan IPS dibandingkan IDS? (Skor 10)
2. Sebutkan dan jelaskan 3 kerentanan utama dalam OWASP Top 10 yang paling sering dieksploitasi pada aplikasi web. Berikan contoh singkat untuk masing-masing. (Skor 15)
3. Jelaskan hak-hak pemilik data pribadi berdasarkan UU PDP. (Skor 15)

Bagian B: Studi Kasus (60%)

Baca studi kasus berikut dengan saksama, kemudian jawab pertanyaan-pertanyaan di bawahnya.

Studi Kasus: Integrasi Sistem Informasi "SmartHealth"

"SmartHealth" adalah sebuah perusahaan rintisan (startup) di bidang kesehatan digital. Mereka baru saja meluncurkan aplikasi mobile yang memungkinkan pengguna menyimpan rekam medis pribadi, berkonsultasi dengan dokter secara online, dan membeli obat. Aplikasi ini menyimpan data sensitif seperti:

- Nama lengkap, tanggal lahir, alamat
- Riwayat penyakit, alergi obat
- Hasil laboratorium
- Data pembayaran (kartu kredit)

Perusahaan ini berkembang pesat dan dalam 6 bulan telah memiliki 500.000 pengguna aktif. Saat ini, aplikasi berjalan di server cloud dengan arsitektur sederhana: satu server aplikasi dan satu server database. Tim pengembang (10 orang) sangat fokus pada kecepatan rilis fitur baru, sehingga keamanan sering menjadi prioritas kedua. Belum ada kebijakan keamanan tertulis, dan karyawan menggunakan kata sandi sederhana untuk akses ke sistem internal.

Pertanyaan:

1. **Analisis Risiko (Skor 20)**
   - Identifikasi minimal 5 aset kritis yang dimiliki "SmartHealth".
   - Untuk setiap aset, identifikasi satu ancaman dan satu kerentanan yang mungkin ada.
   - Lakukan penilaian risiko kualitatif dengan skala Likelihood dan Impact 1-3. Buat matriks risiko sederhana dan tentukan prioritas risiko (Rendah, Sedang, Tinggi) untuk setidaknya 3 risiko utama.
2. **Keamanan Aplikasi dan Jaringan (Skor 20)**
   - Berdasarkan OWASP Top 10, kerentanan apa yang paling mungkin ada pada aplikasi "SmartHealth" mengingat fokus pengembangan yang terburu-buru? Jelaskan.
   - Rekomendasikan arsitektur jaringan yang lebih aman untuk "SmartHealth" (aplikasi di cloud). Apakah perlu DMZ? Bagaimana dengan segmentasi? Jelaskan secara singkat.

3. **Kebijakan, Hukum, dan Etika (Skor 20)**
   - Sebagai konsultan keamanan, Anda diminta menyusun draf kebijakan singkat. Sebutkan 3 kebijakan (ISSP) yang paling mendesak untuk segera dibuat oleh "SmartHealth" dan jelaskan mengapa.
   - Berdasarkan UU PDP, kewajiban apa saja yang harus segera dipenuhi oleh "SmartHealth" terkait data pengguna yang mereka kelola?
   - Jika seorang pengembang di "SmartHealth" menemukan bahwa data pengguna dijual secara diam-diam oleh manajemen kepada pihak ketiga tanpa persetujuan, apa dilema etika yang dihadapinya? Apa yang sebaiknya ia lakukan?

--- Selamat Mengerjakan ---

LAMPIRAN E: PANDUAN TUGAS KELOMPOK DAN PRESENTASI

Tujuan Tugas Kelompok

Tugas kelompok bertujuan untuk mengembangkan kemampuan mahasiswa dalam:

1. Bekerja sama dalam tim.
2. Melakukan riset mendalam tentang topik keamanan informasi terkini.
3. Mengkomunikasikan temuan secara efektif melalui presentasi.
4. Mengembangkan kemampuan berpikir kritis dan analitis.

Topik Tugas Kelompok (Pilih Salah Satu)

1. **Analisis Implementasi ISO 27001 di Sebuah Perusahaan (Studi Kasus)**
   - Pilih perusahaan yang sudah tersertifikasi ISO 27001 (cari studi kasus online).
   - Analisis manfaat, tantangan, dan proses yang dilalui.
2. **Studi Perbandingan: Keamanan Aplikasi Mobile vs Aplikasi Web**
   - Identifikasi perbedaan kerentanan pada aplikasi mobile dan web.
   - Berikan rekomendasi praktik aman untuk pengembangan aplikasi mobile.
3. **Analisis Kebocoran Data Besar (Big Data Breach) di Indonesia**
   - Pilih satu kasus kebocoran data besar di Indonesia (Tokopedia, BPJS, dll).
   - Analisis penyebab, dampak, dan pelajaran yang bisa diambil.
4. **Penerapan Zero Trust Architecture untuk UKM**
   - Jelaskan konsep Zero Trust secara sederhana.
   - Rancang bagaimana UKM dapat mulai menerapkan prinsip Zero Trust dengan biaya terjangkau.
5. **Analisis Regulasi: Perbandingan UU PDP Indonesia dan GDPR Eropa**
   - Bandingkan persamaan dan perbedaan utama.
   - Implikasi bagi perusahaan Indonesia yang ingin berekspansi ke Eropa.

Format Laporan Kelompok

1. **Halaman Judul**
2. **Lembar Pengesahan** (ditandatangani semua anggota)
3. **Kata Pengantar**
4. **Daftar Isi**
5. **Bab I: Pendahuluan**
   - Latar Belakang
   - Rumusan Masalah
   - Tujuan Penulisan

6. **Bab II: Pembahasan**
   (Berisi analisis mendalam sesuai topik)
7. **Bab III: Kesimpulan dan Rekomendasi**
8. **Daftar Pustaka**
9. **Lampiran** (jika ada)

Rubrik Penilaian Presentasi

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Kualitas Materi	30%	Materi sangat relevan, mendalam, dan didukung data/sumber terpercaya	Materi relevan dan cukup mendalam	Materi relevan tetapi dangkal	Materi tidak relevan atau salah
Penyampaian	25%	Penyampaian jelas, percaya diri, kontak mata baik, suara terdengar	Penyampaian cukup jelas	Penyampaian kurang jelas, banyak membaca slide	Penyampaian tidak jelas, gugup
Visualisasi (Slide)	20%	Slide menarik, tidak terlalu padat, mendukung presentasi	Slide cukup baik	Slide terlalu padat atau terlalu sederhana	Slide berantakan, sulit dibaca
Penguasaan Materi	15%	Menguasai materi, mampu menjawab pertanyaan dengan baik	Cukup menguasai, mampu menjawab sebagian pertanyaan	Kurang menguasai, kesulitan menjawab pertanyaan	Tidak menguasai materi
Manajemen Waktu	10%	Waktu tepat (sesuai durasi)	Waktu kurang/lebih sedikit	Waktu kurang/lebih jauh	Waktu sangat tidak sesuai

LAMPIRAN F: DAFTAR ISTILAH DAN SINGKATAN

Singkatan	Kepanjangan	Bab
AES	Advanced Encryption Standard	4
AUP	Acceptable Use Policy	9
CA	Certificate Authority	6
CIA	Confidentiality, Integrity, Availability	1
CPMK	Capaian Pembelajaran Mata Kuliah	RPS
CPL	Capaian Pembelajaran Lulusan	RPS
CRL	Certificate Revocation List	6
DDoS	Distributed Denial of Service	2
DES	Data Encryption Standard	4
DMZ	Demilitarized Zone	10
EDR	Endpoint Detection and Response	10
EISP	Enterprise Information Security Policy	9
GDPR	General Data Protection Regulation	12
HTTPS	Hypertext Transfer Protocol Secure	4, 6
IAM	Identity and Access Management	10
IDOR	Insecure Direct Object References	11
IDS	Intrusion Detection System	10
IoT	Internet of Things	12
IPS	Intrusion Prevention System	10
IPSec	Internet Protocol Security	10
ISMS	Information Security Management System	3
ISO	International Organization for Standardization	3
ISSP	Issue-Specific Security Policy	9

Singkatan	Kepanjangan	Bab
MD5	Message Digest 5	5
MFA	Multi-Factor Authentication	8
NGFW	Next-Generation Firewall	10
NIST	National Institute of Standards and Technology	3
OCSP	Online Certificate Status Protocol	6
OWASP	Open Web Application Security Project	11
PDCA	Plan-Do-Check-Act	3
PKI	Public Key Infrastructure	6
RA	Registration Authority	6
RSA	Rivest-Shamir-Adleman	4
SHA	Secure Hash Algorithm	5
SMKI	Sistem Manajemen Keamanan Informasi	3
SQL	Structured Query Language	11
SSH	Secure Shell	10
SSL	Secure Sockets Layer	6, 10
SysSP	System-Specific Security Policy	9
TLS	Transport Layer Security	6, 10
UU ITE	Undang-Undang Informasi dan Transaksi Elektronik	12
UU PDP	Undang-Undang Pelindungan Data Pribadi	12
VPN	Virtual Private Network	10
WAF	Web Application Firewall	7
XSS	Cross-Site Scripting	11
ZTA	Zero Trust Architecture	10

JURUSAN TEKNOLOGI INFORMASI
RENCANA PEMBELAJARAN SEMESTER (RPS)
MATA KULIAH KEAMANAN SISTEM INFORMASI (PRAKTIKUM)
Program Studi D3-Manajemen Informatika Politeknik Negeri Padang

---

1. Identitas Mata Kuliah

Komponen	Keterangan
Program Studi	D3-Manajemen Informatika
Nama Mata Kuliah	Keamanan Sistem Informasi (Praktikum)
Kode Mata Kuliah	ISY3210
Semester	4
SKS	1 SKS
Nama Dosen Pengampu	1. Ir. H. A. Mooduto, M.Kom. 2. Ideva Gaputra, S.Kom., M.Kom.

---

2. Deskripsi Singkat Mata Kuliah

Mata kuliah praktikum ini merupakan pelengkap dari mata kuliah teori Keamanan Sistem Informasi yang memberikan pengalaman langsung kepada mahasiswa dalam mengimplementasikan berbagai konsep dan teknik keamanan informasi. Mahasiswa akan melakukan praktik konfigurasi perangkat keamanan, implementasi kriptografi, analisis kerentanan, simulasi serangan dan pertahanan, serta penyusunan kebijakan keamanan. Praktikum dilaksanakan di laboratorium komputer dengan panduan modul dan pendampingan instruktur. Setiap pertemuan dirancang untuk mengembangkan keterampilan teknis yang relevan dengan kebutuhan industri dan sesuai dengan KKNI Level 5.

3. Capaian Pembelajaran Lulusan (CPL) yang Dibebankan

Mata kuliah Keamanan Sistem Informasi (Praktikum) berkontribusi terhadap pencapaian dua CPL Program Studi:

Kode CPL	Deskripsi Capaian Pembelajaran Lulusan
CPL-2	Mampu menguasai konsep teoretis bidang manajemen informatika secara umum dan khusus untuk menyelesaikan masalah secara prosedural sesuai dengan lingkup pekerjaannya.
CPL-6	Mampu mengelola dan memelihara infrastruktur teknologi informasi (jaringan, server, sistem cloud) serta menerapkan prinsip keamanan informasi untuk mendukung keberlangsungan operasional organisasi.

4. Capaian Pembelajaran Mata Kuliah (CPMK)

Setelah menyelesaikan mata kuliah praktikum ini, mahasiswa mampu:

Kode CPMK	Deskripsi Capaian Pembelajaran Mata Kuliah
CPMK 1	Mengimplementasikan teknik kriptografi untuk pengamanan data dan komunikasi.
CPMK 2	Melakukan analisis risiko keamanan dan menyusun dokumen kebijakan keamanan sederhana.
CPMK 3	Mengkonfigurasi perangkat keamanan jaringan (firewall, IDS, VPN) dan menganalisis keamanannya.
CPMK 4	Melakukan pengujian keamanan aplikasi web dan mengidentifikasi kerentanan berdasarkan OWASP Top 10.

5. Kemampuan yang Diharapkan (Sub-CPMK)

CPMK	Kode Sub-CPMK	Deskripsi Kemampuan Akhir (Sub-CPMK)
CPMK 1	Sub-CPMK 1.1	Menggunakan tools kriptografi (OpenSSL, GnuPG) untuk mengenkripsi dan mendekripsi file
	Sub-CPMK 1.2	Membuat dan memverifikasi digital signature menggunakan OpenSSL
	Sub-CPMK 1.3	Mengimplementasikan hash untuk verifikasi integritas file
CPMK 2	Sub-CPMK 2.1	Melakukan identifikasi aset dan analisis risiko menggunakan metode kualitatif
	Sub-CPMK 2.2	Menyusun kebijakan keamanan (Acceptable Use Policy, Password Policy)
CPMK 3	Sub-CPMK 3.1	Mengkonfigurasi firewall (iptables) dengan aturan yang sesuai
	Sub-CPMK 3.2	Menginstal dan mengkonfigurasi IDS (Snort) untuk mendeteksi serangan
	Sub-CPMK 3.3	Mengkonfigurasi VPN server dan client menggunakan OpenVPN
	Sub-CPMK 3.4	Menganalisis keamanan jaringan menggunakan tools seperti Wireshark dan Nmap
CPMK 4	Sub-CPMK 4.1	Melakukan vulnerability scanning menggunakan tools (Nessus, OWASP ZAP)
	Sub-CPMK 4.2	Mengidentifikasi kerentanan OWASP Top 10 pada aplikasi web
	Sub-CPMK 4.3	Membuat laporan hasil pengujian keamanan dan rekomendasi perbaikan

6. Tabel Korelasi CPL – CPMK dengan Bobot Kontribusi

CPMK	CPL-2 (50%)	CPL-6 (50%)	Total Kontribusi
CPMK 1	√ (12.5%)	√ (12.5%)	25%
CPMK 2	√ (12.5%)	√ (12.5%)	25%
CPMK 3	√ (12.5%)	√ (12.5%)	25%
CPMK 4	√ (12.5%)	√ (12.5%)	25%
Total	**50%**	**50%**	**100%**

Keterangan:

- Simbol √ menunjukkan kontribusi langsung CPMK terhadap CPL
- Angka dalam persen menunjukkan bobot kontribusi setiap CPMK terhadap masing-masing CPL
- Total kontribusi mata kuliah terhadap CPL-2 = 50%, terhadap CPL-6 = 50%

---

7. Tabel Korelasi CPL - Sub-CPMK

Sub-CPMK	CPL-2	CPL-6
Sub-CPMK 1.1	√	√
Sub-CPMK 1.2	√	√
Sub-CPMK 1.3	√	√
Sub-CPMK 2.1	√	√

Sub-CPMK	CPL-2	CPL-6
Sub-CPMK 2.2	√	√
Sub-CPMK 3.1	√	√
Sub-CPMK 3.2	√	√
Sub-CPMK 3.3	√	√
Sub-CPMK 3.4	√	√
Sub-CPMK 4.1	√	√
Sub-CPMK 4.2	√	√
Sub-CPMK 4.3	√	√

---

8. Daftar Referensi

1. Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.
2. Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.
3. Easttom, C. (2021). *Computer Security Fundamentals* (5th ed.). Pearson.
4. OWASP Foundation. (2021). *OWASP Top Ten - 2021*. The Open Web Application Security Project.
5. Messier, R. (2021). *Network Security with OpenSSL*. O'Reilly Media.
6. Oracle. (2022). *MySQL Security Guide*. Oracle Corporation.
7. Snort Project. (2023). *Snort User Manual*. Cisco Systems.
8. OpenVPN. (2023). *OpenVPN Documentation*. OpenVPN Inc.

---

9. Bahan Kajian (Praktikum)

1. **Kriptografi Terapan**: Enkripsi/dekripsi file dengan OpenSSL/GnuPG, pembuatan key pair, digital signature, hash.
2. **Analisis Risiko**: Identifikasi aset, penilaian risiko, matriks risiko.
3. **Kebijakan Keamanan**: Penyusunan dokumen kebijakan (AUP, Password Policy).
4. **Keamanan Jaringan**: Konfigurasi firewall iptables, instalasi dan konfigurasi Snort IDS, konfigurasi OpenVPN, analisis traffic dengan Wireshark, scanning dengan Nmap.
5. **Keamanan Aplikasi**: Vulnerability scanning dengan Nessus/OWASP ZAP, identifikasi kerentanan OWASP Top 10.
6. **Pelaporan**: Penyusunan laporan hasil pengujian keamanan.

---

10. Tabel Rencana Pembelajaran per Pertemuan

Pertemuan Ke-	Kemampuan Akhir (Sub-CPMK)	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%) Penilaian	CPL yang Dikaitkan
1	[1.1] Menggunakan tools kriptografi (OpenSSL) untuk enkripsi/dekripsi file	Pengenalan OpenSSL, enkripsi simetris (AES) dan asimetris (RSA)	Demonstrasi, praktik mandiri, workshop	• Menginstal OpenSSL • Melakukan enkripsi dan dekripsi file menggunakan AES • Membuat key pair RSA dan melakukan enkripsi/dekripsi	170	**Kriteria**: Keberhasilan enkripsi/dekripsi, ketepatan penggunaan perintah **Indikator**: Semua file berhasil dienkripsi dan didekripsi, perintah sesuai	2%	CPL-2, CPL-6
2	[1.2] Membuat dan memverifikasi digital signature	Digital signature dengan	Demonstrasi, praktik	• Menghitung hash file (SHA-256) • Membuat digital	170	**Kriteria**: Keberhasilan pembuatan dan	2%	CPL-2, CPL-6

Pertemuan Ke-	Kemampuan Akhir (Sub-CPMK)	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%) Penilaian	CPL yang Dikaitkan
		OpenSSL, fungsi hash		signature • Memverifikasi signature		verifikasi signature **Indikator**: Signature berhasil dibuat dan diverifikasi, hash konsisten		
3	[1.3] Mengimplementasikan hash untuk verifikasi integritas	Hash file, verifikasi integritas, studi kasus	Praktik, studi kasus	• Menghitung hash file sebelum dan sesudah modifikasi • Membandingkan hash untuk deteksi perubahan	170	**Kriteria**: Ketepatan perhitungan hash, kemampuan deteksi perubahan **Indikator**: Hash berubah setelah modifikasi, laporan analisis	2.5%	CPL-2, CPL-6
4	[2.1] Melakukan identifikasi aset dan analisis risiko	Identifikasi aset, penilaian risiko, matriks risiko	Simulasi, studi kasus, diskusi	• Mengidentifikasi aset organisasi fiktif • Menilai likelihood dan impact • Membuat matriks risiko	170	**Kriteria**: Kelengkapan identifikasi, ketepatan penilaian **Indikator**: 10+ aset teridentifikasi, matriks risiko jelas	2%	CPL-2, CPL-6

Pertemuan Ke-	Kemampuan Akhir (Sub-CPMK)	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%) Penilaian	CPL yang Dikaitkan
5	[2.2] Menyusun kebijakan keamanan	Struktur kebijakan, Acceptable Use Policy, Password Policy	Workshop, penyusunan dokumen	• Menyusun draf kebijakan AUP • Menyusun kebijakan password	170	**Kriteria**: Kelengkapan struktur, kejelasan bahasa, kesesuaian standar **Indikator**: Kebijakan lengkap (tujuan, ruang lingkup, sanksi)	2%	CPL-2, CPL-6
6	[3.1] Mengkonfigurasi firewall (iptables)	Dasar iptables, aturan filtering, NAT	Demonstrasi, praktik	• Mengkonfigurasi aturan dasar iptables • Memblokir port tertentu • Mengatur forwarding	170	**Kriteria**: Keberhasilan konfigurasi, aturan bekerja sesuai **Indikator**: Port yang diblokir tidak dapat diakses, aturan persist	2%	CPL-2, CPL-6
7	[3.2] Menginstal dan mengkonfigurasi IDS (Snort)	Instalasi Snort, konfigurasi rules, deteksi serangan	Demonstrasi, praktik	• Menginstal Snort • Mengkonfigurasi rules sederhana • Menguji deteksi serangan (ping, port scan)	170	**Kriteria**: Instalasi berhasil, deteksi serangan tepat **Indikator**: Snort berjalan, alert muncul saat	2.5%	CPL-2, CPL-6

Pertemuan Ke-	Kemampuan Akhir (Sub-CPMK)	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%) Penilaian	CPL yang Dikaitkan
						serangan		
8	**UJIAN TENGAH SEMESTER**	Praktikum mencakup pertemuan 1-7	Ujian praktik	• Menyelesaikan tugas praktik individu (enkripsi, firewall, Snort)	170	**Kriteria**: Ketepatan dan kecepatan penyelesaian **Indikator**: Semua tugas selesai dengan benar	30%	CPL-2, CPL-6
9	[3.3] Mengkonfigurasi VPN (OpenVPN)	Konsep VPN, instalasi OpenVPN, konfigurasi server-client	Demonstrasi, praktik	• Menginstal OpenVPN server • Membuat sertifikat • Mengkonfigurasi client dan koneksi	170	**Kriteria**: Koneksi VPN berhasil, enkripsi aktif **Indikator**: Client dapat terhubung, traffic terenkripsi	2%	CPL-2, CPL-6
10	[3.4] Menganalisis keamanan jaringan dengan Wireshark dan Nmap	Packet analysis dengan Wireshark, scanning dengan Nmap	Demonstrasi, praktik	• Menggunakan Wireshark untuk menganalisis traffic • Melakukan port scanning dengan Nmap • Mengidentifikasi port terbuka dan layanan	170	**Kriteria**: Kemampuan analisis traffic, ketepatan identifikasi **Indikator**: Menjelaskan isi packet, mengidentifikasi layanan	2.5%	CPL-2, CPL-6

Pertemuan Ke-	Kemampuan Akhir (Sub-CPMK)	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%) Penilaian	CPL yang Dikaitkan
11	[4.1] Melakukan vulnerability scanning dengan Nessus	Instalasi Nessus, konfigurasi scan, analisis hasil	Demonstrasi, praktik	• Menginstal Nessus • Melakukan basic network scan • Menganalisis laporan kerentanan	170	**Kriteria**: Scan berhasil, analisis laporan tepat **Indikator**: Menjelaskan temuan dan tingkat keparahan	2%	CPL-2, CPL-6
12	[4.1] Melakukan vulnerability scanning dengan OWASP ZAP	OWASP ZAP untuk aplikasi web, spider, active scan	Demonstrasi, praktik	• Mengkonfigurasi OWASP ZAP • Melakukan spidering dan active scan • Menganalisis hasil	170	**Kriteria**: Scan berhasil, identifikasi kerentanan tepat **Indikator**: Menjelaskan temuan dan rekomendasi	2%	CPL-2, CPL-6
13	[4.2] Mengidentifikasi kerentanan OWASP Top 10 pada aplikasi web	OWASP Top 10, contoh kerentanan (SQLi, XSS)	Praktik, studi kasus	• Menguji aplikasi web rentan (DVWA) • Mengidentifikasi SQL injection, XSS • Mencatat langkah-langkah	170	**Kriteria**: Keberhasilan identifikasi kerentanan **Indikator**: Menemukan minimal 3 jenis kerentanan	2%	CPL-2, CPL-6
14	[4.3] Membuat laporan hasil	Struktur laporan,	Workshop, penyusunan	• Menyusun laporan dari hasil	170	**Kriteria**: Kelengkapan	2%	CPL-2, CPL-6

Pertemuan Ke-	Kemampuan Akhir (Sub-CPMK)	Topik Bahasan	Metode Pembelajaran	Pengalaman Belajar Mahasiswa	Waktu (menit)	Kriteria & Indikator Penilaian	Bobot (%) Penilaian	CPL yang Dikaitkan
	pengujian keamanan	rekomendasi perbaikan	laporan	scanning dan identifikasi • Memberikan rekomendasi perbaikan		laporan, kejelasan rekomendasi **Indikator**: Laporan mencakup metodologi, temuan, rekomendasi		
15	Review dan integrasi semua praktikum	Simulasi proyek keamanan terintegrasi	Proyek kelompok, presentasi	• Mengerjakan proyek keamanan (studi kasus) • Mempresentasikan hasil	170	**Kriteria**: Kualitas proyek, presentasi, kerja tim **Indikator**: Proyek lengkap, presentasi jelas	2%	CPL-2, CPL-6
16	**UJIAN AKHIR SEMESTER**	Praktikum mencakup pertemuan 9-15	Ujian praktik	• Menyelesaikan tugas praktik komprehensif (VPN, scanning, laporan)	170	**Kriteria**: Ketepatan dan kelengkapan **Indikator**: Semua tugas selesai dengan benar	30%	CPL-2, CPL-6

Total Bobot Penilaian: Tugas per pertemuan (14 pertemuan × 2% atau 2.5%) = **30%** + Partisipasi = **10%** + UTS = **30%** + UAS = **30%** → **Total = 100%**

RUBRIK PENILAIAN RENCANA PEMBELAJARAN SEMESTER (RPS)
MATA KULIAH KEAMANAN SISTEM INFORMASI (ISY3210) – 2 SKS TEORI
Program Studi D3-Manajemen Informatika Politeknik Negeri Padang

---

A. RUBRIK UMUM TUGAS PER PERTEMUAN

Rubrik ini digunakan sebagai acuan penilaian untuk setiap tugas pada pertemuan 1-7 dan 9-15. Setiap tugas memiliki bobot 2% atau 2.5% dengan rentang nilai 0-100. Nilai akhir tugas = (Skor total / 100) × Bobot tugas.

Kriteria	Bobot Kriteria	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Ketepatan Analisis	40%	Analisis sangat tepat, komprehensif, mendalam, mengaitkan dengan konsep dan studi kasus relevan, serta menunjukkan pemahaman tingkat tinggi	Analisis tepat dan cukup mendalam dengan sebagian besar konsep terkait, namun kurang eksplorasi	Analisis cukup tepat namun kurang mendalam, beberapa konsep tidak terkait atau kurang relevan	Analisis tidak tepat, dangkal, atau tidak sesuai dengan konsep
Kelengkapan	30%	Semua elemen tugas diselesaikan dengan lengkap, terstruktur, dan memenuhi semua instruksi	Sebagian besar elemen tugas diselesaikan dengan cukup lengkap, memenuhi sebagian besar instruksi	Beberapa elemen tugas tidak diselesaikan atau kurang lengkap, instruksi tidak sepenuhnya diikuti	Banyak elemen tugas tidak diselesaikan, instruksi diabaikan
Sistematika dan Bahasa	30%	Penyajian sangat sistematis, bahasa jelas, formal, mudah dipahami, dan bebas dari kesalahan tata bahasa	Penyajian sistematis, bahasa cukup jelas dan formal dengan sedikit kesalahan tata bahasa	Penyajian kurang sistematis, bahasa kurang jelas, terdapat beberapa kesalahan tata bahasa	Penyajian tidak sistematis, bahasa tidak jelas, banyak kesalahan tata bahasa

---

B. RUBRIK KHUSUS PER PERTEMUAN

Pertemuan 1: Sub-CPMK 1.1 – Prinsip CIA Triad (Bobot 2%)

Tugas: Analisis studi kasus kebocoran data dan identifikasi pelanggaran CIA

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Identifikasi Pelanggaran CIA	Kemampuan mengidentifikasi aspek kerahasiaan, integritas, dan ketersediaan dalam kasus	Mengidentifikasi dengan tepat ketiga aspek CIA, disertai bukti dan penjelasan mendalam	Mengidentifikasi ketiga aspek dengan tepat namun kurang detail	Hanya mengidentifikasi 1-2 aspek dengan benar	Tidak dapat mengidentifikasi atau salah identifikasi
Analisis Dampak	Kemampuan menganalisis dampak pelanggaran terhadap organisasi dan pengguna	Analisis dampak komprehensif mencakup aspek finansial, reputasi, operasional, dan hukum	Analisis dampak mencakup 2-3 aspek dengan cukup baik	Analisis dampak hanya mencakup 1 aspek secara sederhana	Tidak ada analisis dampak atau tidak relevan
Rekomendasi Dasar	Kemampuan memberikan rekomendasi perbaikan sederhana	Memberikan 3+ rekomendasi yang relevan, spesifik, dan dapat ditindaklanjuti	Memberikan 2 rekomendasi yang cukup relevan	Memberikan 1 rekomendasi yang kurang spesifik	Tidak memberikan rekomendasi

Pertemuan 2: Sub-CPMK 1.2 – Ancaman dan Kerentanan (Bobot 2%)

Tugas: Analisis kasus serangan siber dan pembuatan peta ancaman

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Identifikasi Ancaman	Kemampuan mengidentifikasi jenis ancaman dan modus serangan	Mengidentifikasi 5+ ancaman dengan deskripsi modus operandi yang detail dan akurat	Mengidentifikasi 3-4 ancaman dengan deskripsi cukup jelas	Mengidentifikasi 1-2 ancaman dengan deskripsi minimal	Tidak dapat mengidentifikasi ancaman
Peta Ancaman	Kualitas pembuatan peta ancaman (threat map)	Peta ancaman komprehensif mencakup vektor serangan, aset terdampak, tingkat risiko, dan mitigasi awal	Peta ancaman cukup lengkap mencakup sebagian besar elemen	Peta ancaman sederhana dengan beberapa elemen	Peta ancaman tidak lengkap atau tidak sesuai
Keterkaitan dengan Organisasi	Kemampuan mengaitkan ancaman dengan konteks organisasi tertentu	Menjelaskan secara mendalam bagaimana ancaman berdampak pada organisasi spesifik (UKM, rumah sakit, bank)	Menjelaskan dampak secara umum tanpa konteks spesifik	Kurang mampu mengaitkan dengan konteks organisasi	Tidak ada kaitan dengan konteks organisasi

Pertemuan 3: Sub-CPMK 1.3 – Standar Keamanan Informasi (Bobot 2.5%)

Tugas: Analisis perbandingan ISO 27001 dan NIST Cybersecurity Framework

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Pemahaman Struktur Standar	Kemampuan menjelaskan struktur ISO 27001 (14 domain) dan NIST (5 functions)	Menjelaskan secara rinci dan akurat kedua standar beserta komponennya	Menjelaskan dengan cukup baik namun ada sedikit kekurangan	Menjelaskan secara umum tanpa detail	Tidak dapat menjelaskan atau salah
Analisis Perbandingan	Kualitas perbandingan antara kedua standar	Perbandingan komprehensif mencakup 5+ aspek (pendekatan, fokus, implementasi, sertifikasi, dll) dengan analisis mendalam	Perbandingan mencakup 3-4 aspek dengan analisis cukup	Perbandingan sederhana 1-2 aspek dengan analisis dasar	Perbandingan tidak lengkap atau tidak relevan
Rekomendasi Penggunaan	Kemampuan merekomendasikan standar yang sesuai untuk organisasi tertentu	Memberikan rekomendasi tepat disertai justifikasi kuat berdasarkan karakteristik organisasi	Memberikan rekomendasi dengan justifikasi cukup	Rekomendasi kurang tepat atau tanpa justifikasi	Tidak memberikan rekomendasi

Pertemuan 4: Sub-CPMK 2.1 – Kriptografi Simetris dan Asimetris (Bobot 2%)

Tugas: Analisis penerapan kriptografi dalam e-commerce, email, dan perbankan

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Pemahaman Konsep	Kemampuan menjelaskan perbedaan kriptografi simetris dan asimetris	Menjelaskan dengan sangat jelas perbedaan, kelebihan, kekurangan, dan contoh algoritma masing-masing	Menjelaskan dengan cukup jelas namun kurang detail	Penjelasan kurang jelas atau ada kesalahan konsep	Tidak memahami perbedaan
Analisis Skenario	Kemampuan menganalisis skenario penggunaan dalam aplikasi nyata	Menganalisis 3 skenario (e-commerce, email, perbankan) dengan tepat, menjelaskan algoritma yang digunakan dan alasannya	Menganalisis 2 skenario dengan cukup tepat	Menganalisis 1 skenario dengan sederhana	Tidak dapat menganalisis
Evaluasi Keamanan	Kemampuan mengevaluasi keamanan implementasi	Mengevaluasi kelebihan dan kelemahan implementasi kriptografi dalam setiap skenario disertai rekomendasi perbaikan	Mengevaluasi secara umum tanpa rekomendasi spesifik	Evaluasi dangkal atau tidak tepat	Tidak ada evaluasi

Pertemuan 5: Sub-CPMK 2.2 – Hash dan Digital Signature (Bobot 2%)

Tugas: Analisis penggunaan hash untuk verifikasi integritas dan digital signature pada dokumen elektronik

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Pemahaman Hash	Kemampuan menjelaskan fungsi hash dan aplikasinya	Menjelaskan sifat-sifat hash (one-way, collision resistance), contoh algoritma, dan aplikasi verifikasi integritas dengan sangat jelas	Menjelaskan dengan cukup baik namun kurang detail	Penjelasan kurang lengkap atau ada kesalahan	Tidak memahami konsep hash
Pemahaman Digital Signature	Kemampuan menjelaskan digital signature dan cara kerjanya	Menjelaskan proses pembuatan dan verifikasi digital signature, peran hash, dan contoh implementasi dengan sangat jelas	Menjelaskan dengan cukup baik	Penjelasan kurang lengkap	Tidak memahami digital signature
Analisis Kasus	Kemampuan menganalisis kasus penggunaan dalam dokumen elektronik	Menganalisis 2+ kasus (kontrak digital, dokumen pemerintah, software distribution) dengan detail dan tepat	Menganalisis 1 kasus dengan cukup baik	Analisis dangkal	Tidak ada analisis

Pertemuan 6: Sub-CPMK 2.3 – Infrastruktur Kunci Publik (PKI) (Bobot 2%)

Tugas: Analisis implementasi SSL/TLS pada website dan evaluasi sertifikat digital

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Pemahaman PKI	Kemampuan menjelaskan komponen PKI (CA, RA, sertifikat)	Menjelaskan dengan sangat jelas hierarki trust, peran masing-masing komponen, dan proses penerbitan sertifikat	Menjelaskan dengan cukup baik	Penjelasan kurang lengkap	Tidak memahami PKI
Analisis Sertifikat	Kemampuan menganalisis informasi sertifikat SSL pada website	Menganalisis minimal 3 website, mengidentifikasi issuer, masa berlaku, algoritma, dan mengevaluasi keamanannya	Menganalisis 2 website dengan cukup baik	Menganalisis 1 website dengan sederhana	Tidak dapat menganalisis
Evaluasi Keamanan	Kemampuan mengevaluasi keamanan implementasi SSL/TLS	Mengevaluasi potensi kerentanan (misal: sertifikat self-signed, usang, cipher lemah) dan memberikan rekomendasi perbaikan	Mengevaluasi secara umum tanpa rekomendasi	Evaluasi dangkal	Tidak ada evaluasi

Pertemuan 7: Sub-CPMK 3.1 – Analisis Risiko Keamanan (Bobot 2.5%)

Tugas: Melakukan analisis risiko untuk organisasi fiktif (UKM/rumah sakit) dan membuat matriks risiko

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Identifikasi Aset	Kemampuan mengidentifikasi aset informasi organisasi	Mengidentifikasi 10+ aset dengan klasifikasi nilai dan kepentingan yang tepat	Mengidentifikasi 7-9 aset dengan cukup lengkap	Mengidentifikasi 4-6 aset dengan penjelasan minimal	<4 aset atau tidak relevan
Penilaian Risiko	Ketepatan menilai likelihood dan impact	Menilai risiko dengan akurat menggunakan skala yang konsisten, disertai justifikasi kuat	Menilai dengan cukup akurat namun justifikasi kurang	Penilaian kurang konsisten atau tanpa justifikasi	Penilaian tidak akurat
Matriks Risiko	Kualitas visualisasi dan prioritas risiko	Matriks risiko sangat jelas, menunjukkan prioritas (tinggi, sedang, rendah) dengan tepat, dan dilengkapi analisis	Matriks cukup jelas dengan prioritas yang tepat	Matriks sederhana dengan beberapa elemen	Matriks tidak lengkap atau salah

Pertemuan 9: Sub-CPMK 3.2 – Perancangan Kontrol Keamanan (Bobot 2%)

Tugas: Merancang kontrol keamanan untuk mitigasi risiko yang telah diidentifikasi

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Relevansi Kontrol	Kesesuaian kontrol dengan risiko	Semua kontrol yang dirancang sangat relevan dan efektif untuk mitigasi risiko spesifik	Sebagian besar kontrol relevan	Beberapa kontrol kurang relevan	Kontrol tidak relevan
Kelengkapan Aspek	Cakupan kontrol administratif, teknis, dan fisik	Mencakup ketiga aspek dengan detail implementasi yang jelas	Mencakup dua aspek dengan cukup detail	Mencakup satu aspek dengan detail minimal	Tidak mencakup aspek yang diperlukan
Feasibility	Kemungkinan implementasi kontrol	Semua kontrol feasible dengan pertimbangan biaya, sumber daya, dan kompleksitas yang realistis	Sebagian besar kontrol feasible	Beberapa kontrol tidak feasible	Kontrol tidak feasible

Pertemuan 10: Sub-CPMK 3.3 – Penyusunan Kebijakan Keamanan (Bobot 2.5%)

Tugas: Menyusun kebijakan keamanan sederhana (Acceptable Use Policy atau Password Policy)

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Kelengkapan Struktur	Kesesuaian dengan template kebijakan	Kebijakan lengkap dengan: tujuan, ruang lingkup, definisi, kebijakan, sanksi, dan review	Memiliki sebagian besar elemen	Hanya memiliki beberapa elemen	Struktur tidak lengkap
Kejelasan Bahasa	Kejelasan dan ketepatan bahasa	Bahasa sangat jelas, tidak ambigu, konsisten, dan profesional	Bahasa cukup jelas dengan sedikit ambiguitas	Bahasa kurang jelas atau ambigu	Bahasa tidak jelas
Kesesuaian Standar	Mengacu pada standar keamanan	Kebijakan sangat sesuai dengan ISO 27001 atau NIST, mengacu pada klausul spesifik	Cukup sesuai dengan prinsip umum	Kurang sesuai	Tidak sesuai

Pertemuan 11: Sub-CPMK 4.1 – Analisis Keamanan Jaringan (Firewall, IDS/IPS) (Bobot 2%)

Tugas: Menganalisis konfigurasi firewall pada skenario jaringan tertentu

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Pemahaman Firewall	Kemampuan menjelaskan fungsi dan jenis firewall	Menjelaskan dengan sangat jelas packet filtering, stateful inspection, application firewall, dan contoh implementasi	Menjelaskan dengan cukup baik	Penjelasan kurang lengkap	Tidak memahami
Analisis Konfigurasi	Kemampuan menganalisis aturan firewall	Menganalisis aturan firewall (allow/deny) pada skenario, mengidentifikasi kelemahan, dan merekomendasikan perbaikan	Menganalisis dengan cukup baik namun kurang rekomendasi	Analisis dangkal	Tidak dapat menganalisis
Pemahaman IDS/IPS	Kemampuan menjelaskan perbedaan IDS dan IPS	Menjelaskan dengan sangat jelas deteksi vs pencegahan, signature-based vs anomaly-based	Menjelaskan dengan cukup baik	Penjelasan kurang	Tidak memahami

Pertemuan 12: Sub-CPMK 4.1 – Lanjutan Analisis Keamanan Jaringan (Arsitektur Jaringan Aman) (Bobot 2%)

Tugas: Menganalisis desain arsitektur jaringan organisasi

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Analisis Arsitektur	Kemampuan menganalisis kelemahan arsitektur	Mengidentifikasi 5+ kelemahan arsitektur (misal: kurang segmentasi, DMZ tidak tepat, single point of failure) dengan analisis mendalam	Mengidentifikasi 3-4 kelemahan dengan cukup baik	Mengidentifikasi 1-2 kelemahan	Tidak ada identifikasi
Pemahaman Zero Trust	Kemampuan menjelaskan konsep Zero Trust	Menjelaskan dengan sangat jelas prinsip "never trust, always verify", micro-segmentation, dan implementasinya	Menjelaskan dengan cukup baik	Penjelasan kurang	Tidak memahami
Rekomendasi Perbaikan	Kualitas rekomendasi perbaikan	Memberikan rekomendasi spesifik, detail, dan feasible untuk setiap kelemahan	Rekomendasi cukup spesifik	Rekomendasi umum	Tidak ada rekomendasi

Pertemuan 13: Sub-CPMK 4.2 – Kerentanan Keamanan Aplikasi (OWASP Top 10) (Bobot 2%)

Tugas: Menganalisis kerentanan pada aplikasi web fiktif berdasarkan OWASP Top 10

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Identifikasi Kerentanan	Kemampuan mengidentifikasi kerentanan OWASP	Mengidentifikasi 5+ kerentanan dari OWASP Top 10 dengan deskripsi tepat dan contoh skenario	Mengidentifikasi 3-4 kerentanan dengan cukup baik	Mengidentifikasi 1-2 kerentanan	Tidak dapat mengidentifikasi
Pemahaman Dampak	Kemampuan menjelaskan dampak kerentanan	Menjelaskan dampak terhadap kerahasiaan, integritas, ketersediaan, serta potensi eksploitasi dengan sangat jelas	Menjelaskan dampak secara umum	Penjelasan dangkal	Tidak ada penjelasan
Rekomendasi Perbaikan	Kualitas rekomendasi perbaikan	Memberikan rekomendasi perbaikan yang spesifik (misal: input validation, parameterized queries) dan sesuai standar secure coding	Rekomendasi cukup spesifik	Rekomendasi umum	Tidak ada rekomendasi

Pertemuan 14: Sub-CPMK 4.3 – Aspek Hukum dan Etika (UU ITE, UU PDP) (Bobot 2%)

Tugas: Analisis kasus pelanggaran UU ITE dan cyber crime

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Pemahaman Regulasi	Kemampuan menjelaskan UU ITE dan UU PDP	Menjelaskan dengan sangat jelas pasal-pasal terkait cyber crime, perlindungan data pribadi, dan sanksi	Menjelaskan dengan cukup baik	Penjelasan kurang lengkap	Tidak memahami
Analisis Kasus Hukum	Kemampuan menganalisis kasus hukum	Menganalisis 2+ kasus dengan mengidentifikasi pasal yang dilanggar, modus, dan putusan (jika ada)	Menganalisis 1 kasus dengan cukup baik	Analisis dangkal	Tidak ada analisis
Etika Profesional	Kemampuan mengevaluasi dilema etika	Mengevaluasi dilema etika (whistleblowing, ethical hacking) dengan argumen kuat dan perspektif multiple	Mengevaluasi dengan cukup baik	Evaluasi sederhana	Tidak ada evaluasi

Pertemuan 15: Sub-CPMK 4.3 – Lanjutan Aspek Hukum dan Kepatuhan (Bobot 2%)

Tugas: Presentasi kelompok tentang tren keamanan terkini dan implikasi kepatuhan

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Kualitas Presentasi	Kejelasan, sistematika, dan komunikasi	Presentasi sangat jelas, sistematis, komunikatif, menggunakan media yang menarik, dan waktu tepat	Presentasi cukup jelas dan sistematis	Presentasi kurang sistematis atau sulit dipahami	Presentasi tidak terstruktur
Kedalaman Analisis Tren	Kemampuan menganalisis tren keamanan (AI security, IoT, cloud)	Analisis mendalam tentang tren, dampak, tantangan, dan peluang, disertai contoh nyata	Analisis cukup baik dengan beberapa contoh	Analisis dangkal	Tidak ada analisis
Implikasi Kepatuhan	Kemampuan menjelaskan implikasi kepatuhan terhadap regulasi	Menjelaskan dengan sangat jelas bagaimana tren mempengaruhi kepatuhan terhadap UU/standar, dan rekomendasi adaptasi	Menjelaskan dengan cukup baik	Penjelasan kurang	Tidak ada penjelasan

C. RUBRIK PARTISIPASI (Bobot 10%)

Penilaian partisipasi dilakukan setiap pertemuan dan diakumulasi pada akhir semester.

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Keaktifan Bertanya/Menjawab	40%	Aktif bertanya/menjawab dengan pertanyaan mendalam minimal 2x per pertemuan	Aktif 1x per pertemuan	Jarang bertanya/menjawab (1-2x selama semester)	Tidak pernah berpartisipasi
Kualitas Kontribusi	30%	Kontribusi konstruktif, mengaitkan konsep, memperkaya diskusi, dan relevan	Kontribusi relevan dan tepat	Kontribusi sederhana, mengulang pendapat	Kontribusi tidak relevan atau mengganggu
Kehadiran dan Ketepatan Waktu	30%	Hadir tepat waktu di semua 16 pertemuan	Hadir tepat waktu di ≥14 pertemuan	Hadir di 12-13 pertemuan, beberapa terlambat	Hadir <12 pertemuan

D. RUBRIK UJIAN TENGAH SEMESTER (UTS) – Bobot 30%

UTS terdiri dari soal teori (40%) dan studi kasus (60%). Total nilai UTS = (Nilai teori × 40%) + (Nilai studi kasus × 60%).

Komponen Teori (40% dari nilai UTS)

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Ketepatan Jawaban	50%	Semua jawaban tepat dengan penjelasan akurat dan lengkap	Sebagian besar jawaban tepat dengan sedikit kesalahan	Beberapa jawaban tepat, beberapa salah	Banyak jawaban salah atau tidak dijawab
Pemahaman Konsep	50%	Menunjukkan pemahaman mendalam, mampu mengaitkan antar konsep	Menunjukkan pemahaman cukup baik	Pemahaman dasar, kurang mengaitkan	Tidak memahami konsep

Komponen Studi Kasus (60% dari nilai UTS)

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Analisis Kasus	40%	Analisis sangat tepat, komprehensif, mengidentifikasi semua isu kunci	Analisis tepat, mengidentifikasi sebagian besar isu	Analisis cukup tepat, beberapa isu terlewat	Analisis dangkal atau salah
Penerapan Konsep	30%	Menerapkan konsep yang relevan dengan sangat tepat dan kreatif	Menerapkan konsep dengan tepat	Kurang tepat dalam penerapan	Tidak menerapkan konsep
Solusi dan Rekomendasi	30%	Memberikan solusi yang spesifik, feasible, dan inovatif	Solusi cukup spesifik dan feasible	Solusi umum dan kurang feasible	Solusi tidak relevan

E. RUBRIK UJIAN AKHIR SEMESTER (UAS) – Bobot 30%

UAS terdiri dari soal teori (40%) dan studi kasus (60%). Total nilai UAS = (Nilai teori × 40%) + (Nilai studi kasus × 60%).

Komponen Teori (40% dari nilai UAS)

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Ketepatan Jawaban	50%	Semua jawaban tepat dengan penjelasan akurat dan lengkap	Sebagian besar jawaban tepat	Beberapa jawaban tepat	Banyak jawaban salah
Pemahaman Konsep	50%	Menunjukkan pemahaman mendalam, mampu mengaitkan antar konsep	Pemahaman cukup baik	Pemahaman dasar	Tidak memahami

Komponen Studi Kasus (60% dari nilai UAS)

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Analisis Kasus	40%	Analisis sangat tepat, komprehensif, mengidentifikasi semua isu kunci	Analisis tepat, mengidentifikasi sebagian besar isu	Analisis cukup tepat, beberapa isu terlewat	Analisis dangkal atau salah
Penerapan Konsep	30%	Menerapkan konsep dengan sangat tepat dan kreatif	Menerapkan konsep dengan tepat	Kurang tepat dalam penerapan	Tidak menerapkan konsep
Solusi dan Rekomendasi	30%	Solusi spesifik, feasible, inovatif, dan mempertimbangkan aspek hukum/etika	Solusi cukup spesifik dan feasible	Solusi umum	Solusi tidak relevan

F. REKAPITULASI PENILAIAN

Komponen	Bobot	Nilai Maksimal
Tugas Pertemuan 1	2%	100
Tugas Pertemuan 2	2%	100
Tugas Pertemuan 3	2.5%	100
Tugas Pertemuan 4	2%	100
Tugas Pertemuan 5	2%	100
Tugas Pertemuan 6	2%	100
Tugas Pertemuan 7	2.5%	100
Tugas Pertemuan 9	2%	100
Tugas Pertemuan 10	2.5%	100
Tugas Pertemuan 11	2%	100
Tugas Pertemuan 12	2%	100
Tugas Pertemuan 13	2%	100
Tugas Pertemuan 14	2%	100
Tugas Pertemuan 15	2%	100

Komponen	Bobot	Nilai Maksimal
Subtotal Tugas	**30%**	
Partisipasi	10%	100
UTS	30%	100
UAS	30%	100
Total	**100%**	

Nilai Akhir = (Rata-rata nilai tugas × 30%) + (Nilai partisipasi × 10%) + (Nilai UTS × 30%) + (Nilai UAS × 30%)

G. KONVERSI NILAI AKHIR KE HURUF

Rentang Nilai	Nilai Huruf	Indeks Prestasi
85.00 – 100.00	A	4.00
80.00 – 84.99	A-	3.75
75.00 – 79.99	B+	3.50
70.00 – 74.99	B	3.00
65.00 – 69.99	B-	2.75
60.00 – 64.99	C+	2.50

Rentang Nilai	Nilai Huruf	Indeks Prestasi
55.00 – 59.99	C	2.00
50.00 – 54.99	D	1.00
0.00 – 49.99	E	0.00

Ditetapkan di: Padang
Tanggal: 23 Februari 2026
Dosen Pengampu,

Ir. H. A. Mooduto, M.Kom.
NIP. 196605101994031003