Securing Information Systems

Assoc.Prof.Dr.Muhammad Said Hasibuan
Fakultas Ilmu Komputer IIB Darmajaya
2025

Definisi

- Definisi Sistem Informasi
- Mengapa Keamanan Sistem Informasi Penting?
- Dampak Serangan Siber terhadap Organisasi

Definisi

- Sistem informasi adalah kombinasi dari teknologi, manusia, dan proses yang bekerja bersama untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan informasi.
- Contoh: Sistem ERP, sistem e-learning, sistem keuangan digital.

Mengapa Keamanan Sistem Informasi Penting?

- Sistem informasi menyimpan aset digital penting seperti data pribadi, transaksi keuangan, atau informasi strategis perusahaan.
- Jika tidak diamankan, sistem ini menjadi rentan terhadap ancaman seperti pencurian data, manipulasi, atau penghancuran.

Dampak Serangan Siber terhadap Organisasi:

- **Finansial**: Kerugian langsung (uang dicuri) atau tidak langsung (biaya pemulihan, denda hukum).
- **Reputasi**: Kehilangan kepercayaan pelanggan, investor, dan publik.
- **Legal & Compliance**: Potensi pelanggaran hukum atau regulasi data (misal: GDPR, UU PDP di Indonesia).
- **Operasional**: Gangguan layanan, downtime, dan kehilangan produktivitas.

Threat Landscape

- Jenis Ancaman: Malware, Phishing, Ransomware
- Aktor Ancaman: Hacker, Insider, APT (Advanced Persistent Threat)
- Statistik Serangan Siber Global

Jenis-Jenis Ancaman Siber:

- **Malware (Malicious Software):** Perangkat lunak berbahaya seperti virus, worm, trojan, dan ransomware.
  → *Contoh:* WannaCry (2017) mengunci data dan meminta tebusan.
- **Phishing:** Upaya penipuan dengan menyamar sebagai entitas tepercaya untuk mencuri informasi (biasanya lewat email).
  → *Contoh:* Email palsu dari “bank” yang meminta username dan password.
- **Ransomware:** Mengunci atau mengenkripsi data korban dan meminta pembayaran tebusan.
- **Denial of Service (DoS/DDoS):** Menyerang sistem agar tidak bisa diakses oleh pengguna yang sah.

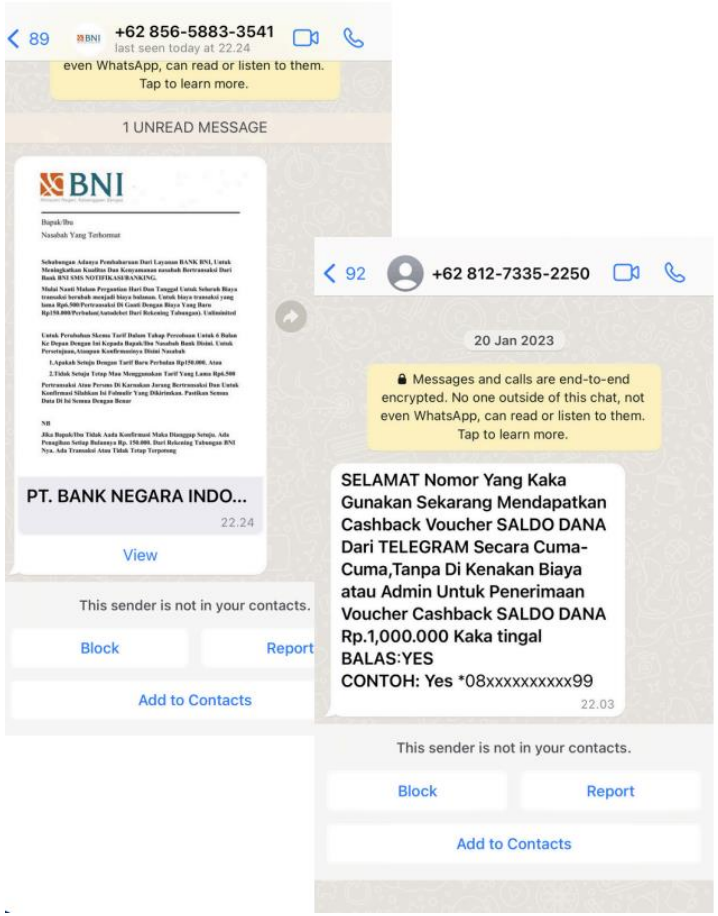
Aktor Ancaman (Threat Actors):

- **Hacker/Cracker:** Individu atau kelompok yang menyerang sistem karena motif finansial, politik, atau rekreasi.
- **Insider Threats:** Karyawan atau pihak internal yang menyalahgunakan akses sistem (bisa disengaja atau tidak).
- **Script Kiddies:** Penyerang amatir yang menggunakan alat siap pakai tanpa memahami secara teknis.
- **Nation-State Actors:** Agen negara yang melakukan spionase atau sabotase digital (cyberwarfare).
- **Hacktivists:** Kelompok yang menyerang untuk menyampaikan pesan politik/sosial (contoh: Anonymous).

Aktor Ancaman (Threat Actors):

- **Hacker/Cracker:** Individu atau kelompok yang menyerang sistem karena motif finansial, politik, atau rekreasi.
- **Insider Threats:** Karyawan atau pihak internal yang menyalahgunakan akses sistem (bisa disengaja atau tidak).
- **Script Kiddies:** Penyerang amatir yang menggunakan alat siap pakai tanpa memahami secara teknis.
- **Nation-State Actors:** Agen negara yang melakukan spionase atau sabotase digital (cyberwarfare).
- **Hacktivists:** Kelompok yang menyerang untuk menyampaikan pesan politik/sosial (contoh: Anonymous).

Threat Landscape



phishing

upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan

Target Pencurian

- data pribadi (nama, usia, alamat, KTP)
- data akun (username dan password)
- data finansial (informasi kartu kredit, akun m-banking).

Threat Landscape

phishing pada umumnya menggunakan teknik social engineering

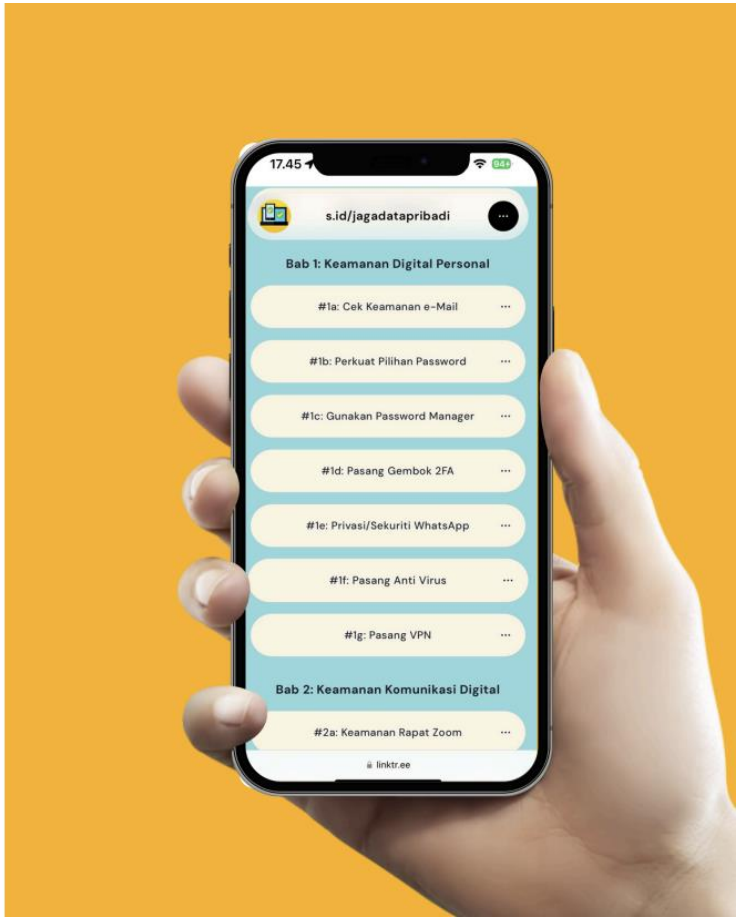
teknik manipulasi psikologis yang digunakan untuk menipu seseorang agar memberikan informasi sensitif atau melakukan tindakan yang tidak aman, misalnya memberikan password, kode OTP, atau data penting lainnya

memanfaatkan sifat manusia, bukan kelemahan teknis, untuk mencapai tujuan serangan.

Threat Landscape

Periksa Keamanan Digitalmu di:

privasi.id



Security Goals (CIA Triad)

- **Confidentiality**: Menjaga kerahasiaan informasi
- **Integrity**: Menjaga keakuratan dan konsistensi data
- **Availability**: Menjaga agar sistem tersedia saat dibutuhkan

Security Goals (CIA Triad)

- 🕵️ **Confidentiality (Kerahasiaan)**
- Menjamin bahwa hanya pihak yang berwenang yang dapat mengakses informasi.
- Menghindari kebocoran data pribadi, dokumen rahasia, dan informasi sensitif.
- **Teknologi pendukung:**
  - Enkripsi (AES, RSA)
  - Autentikasi (password, biometrik)
  - Access control list (ACL)
- ✅ *Contoh:* Sistem HRD membatasi akses data gaji hanya untuk manajer dan staf terkait.

Security Goals (CIA Triad)

- **Integrity (Integritas)**
- Menjaga keakuratan dan konsistensi data selama siklus hidupnya.
- Mencegah modifikasi data secara tidak sah, baik sengaja maupun tidak disengaja.
- **Teknologi pendukung:**
  - Hashing (SHA-256)
  - Digital signatures
  - Version control & checksums
- ✅ *Contoh:* File log transaksi harus tetap utuh dari sumber hingga audit.

Security Goals (CIA Triad)

- **Availability (Ketersediaan)**
- Memastikan sistem dan informasi selalu dapat diakses saat dibutuhkan oleh pengguna yang sah.
- Menghindari downtime yang mengganggu layanan bisnis.
- **Teknologi pendukung:**
  - Backup & disaster recovery
  - Load balancing
  - Redundant systems
- ✅ *Contoh:* Website e-commerce harus tetap online saat promo besar-besaran.

Security Policies & Governance

- Peran Kebijakan Keamanan
- Framework Keamanan (ISO 27001, NIST)
- Peran Manajemen Risiko

Peran Kebijakan Keamanan

- **Security Policy** adalah dokumen formal yang menetapkan aturan dan pedoman terkait perlindungan informasi dan aset digital dalam organisasi.
- **Governance** adalah mekanisme pengelolaan keamanan secara strategis, mencakup perencanaan, pelaksanaan, pemantauan, dan pengawasan terhadap keamanan informasi di seluruh organisasi.
- 🎯 **Tujuan Utama:**
- Melindungi kerahasiaan, integritas, dan ketersediaan informasi.
- Menjaga kepatuhan terhadap regulasi dan standar internasional (ISO 27001, NIST).
- Menyelaraskan keamanan TI dengan strategi dan tujuan bisnis.

Technical Safeguards

- Firewall, Antivirus, IDS/IPS
- Enkripsi (Data at Rest & in Transit)
- Autentikasi dan Otorisasi (MFA, RBAC)

Human Factors & Social Engineering

- Faktor Kelemahan Manusia
- Contoh: Email Phishing, Baiting
- Strategi Mitigasi: Pelatihan dan Awareness

Cybersecurity Architecture

- Defense in Depth (Layered Security)
- Zero Trust Architecture
- Model Perimeter vs. Post-Perimeter

Zero Trust Architecture (ZTA)

- **Prinsip utama:** *"Never trust, always verify"* — setiap akses harus diverifikasi secara ketat, meskipun berasal dari dalam jaringan.
- Berbasis pada asumsi bahwa ancaman **sudah ada di dalam jaringan.**
- Elemen kunci ZTA:
  - Identitas dan akses berbasis kontekstual (device, lokasi, waktu)
  - Autentikasi berlapis (MFA)
  - Mikrosegmentasi jaringan
  - Logging dan monitoring real-time
- ✅ *Contoh:* Seorang pegawai tidak otomatis dapat mengakses sistem keuangan hanya karena berada di kantor pusat.

Incident Response & Recovery

- Tahapan Respons Insiden: Detect, Contain, Eradicate, Recover
- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)

Case Study

- Studi Kasus: Serangan terhadap Target / Equifax / SolarWinds
- Analisis Penyebab & Dampaknya
- Pelajaran yang Dapat Diambil

Trends in Securing Information Systems

- Penggunaan AI/ML dalam Cybersecurity
- Cloud Security & Challenges
- Regulation: GDPR, PDP Law, HIPAA, dll.

Trends in Securing Information Systems

- Tantangan Menerapkan Keamanan di Dunia Nyata
- Diskusi Kasus di Indonesia
- Q&A

Closing Slide

- Ringkasan Materi
- Saran Referensi Tambahan
- Quote: *"Security is not a product, but a process." – Bruce Schneier*

Terima Kasih