Identifikasi Risiko IT

Assoc.Prof. Dr. Muhammad Said Hasibuan,S.Kom.,M.Kom
Fakultas Ilmu Komputer IIB Darmajaya
2025

Identifikasi Risiko IT

- Risiko IT adalah potensi ancaman terhadap aset TI yang dapat menyebabkan kerugian finansial, reputasi, atau operasional.
- Contoh: Serangan siber, kegagalan sistem, kesalahan manusia, atau bencana alam.

Klasifikasi Risiko IT

1. **Risiko Keamanan (Security Risk)**
   Serangan malware, hacking, phishing, data breach.
2. **Risiko Operasional (Operational Risk)**
   Kesalahan manusia, sistem down, kegagalan perangkat keras.
3. **Risiko Kepatuhan (Compliance Risk)**
   Pelanggaran regulasi seperti GDPR, ISO 27001.
4. **Risiko Strategis (Strategic Risk)**
   Ketidaksesuaian strategi TI dengan tujuan bisnis.
5. **Risiko Finansial (Financial Risk)**
   Kerugian akibat downtime, denda kepatuhan, pencurian data.

Malware

Malware, singkatan dari “malicious software”, adalah program komputer yang dibuat dengan tujuan jahat. Malware dirancang untuk merusak, mengubah, atau mencuri data dari komputer atau jaringan. Ada berbagai jenis malware, termasuk virus, worm, Trojan, ransomware, spyware, dan adware

Hacking

Phishing

Phising adalah tindakan kejahatan pengelabuan dengan tujuan mendapatkan informasi berupa data pribadi, data akun, atau data finansial seperti rekening dan kartu kredit

Data Breach

Data Breach (Pelanggaran Data) adalah suatu insiden pada informasi sensitif yang bisa diakses oleh pihak yang tidak bertanggung jawab dengan cara yang disengaja.

Metode Identifikasi Risiko IT

1. **Analisis Dokumen** (Review kebijakan, prosedur, dan sistem IT yang ada)
2. **Wawancara & Kuesioner** (Melibatkan stakeholder untuk mengidentifikasi potensi risiko)
3. **Observasi Langsung** (Meninjau infrastruktur TI secara langsung)
4. **Penilaian Ancaman & Kerentanan** (Menggunakan framework seperti NIST, ISO 27001)
5. **Analisis Historis** (Menggunakan data insiden masa lalu untuk mengidentifikasi pola risiko)

Contoh Tools untuk Identifikasi Risiko IT

- **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- **INDEKS KAMI** (Keamanan Informasi)
- **FAIR** (Factor Analysis of Information Risk)
- **NIST Risk Management Framework**
- **ISO/IEC 27005** (Standar Manajemen Risiko Keamanan Informasi)
- **COBIT** (Control Objectives for Information and Related Technologies)

Studi Kasus

Kasus: Serangan Ransomware pada Perusahaan X

- Kronologi serangan
- Dampak yang ditimbulkan
- Langkah-langkah identifikasi dan mitigasi risiko yang dilakukan

Strategi Mitigasi Risiko IT

1. **Pencegahan** (Implementasi kebijakan keamanan, enkripsi data, pelatihan karyawan)
2. **Deteksi** (Monitoring sistem, SIEM, IDS/IPS)
3. **Respon** (Rencana pemulihan bencana, backup berkala)
4. **Pemulihan** (Disaster Recovery Plan, Business Continuity Plan)

Kesimpulan

- Identifikasi risiko IT adalah langkah awal dalam manajemen risiko TI.
- Berbagai metode dapat digunakan untuk mengidentifikasi risiko secara efektif.
- Mitigasi risiko memerlukan kombinasi strategi teknologi dan kebijakan organisasi.
- Kesadaran dan pelatihan pengguna sangat penting dalam mencegah risiko IT.

Terima Kasih