INTEGRITY, CONFIDENTIALITY, DAN AVALIABILITY PRIVACY

ETIKA PROFESI

Materi Review

- UU ITE
- Sertifikasi, Administrasi, *Maintenance, Management*, Audit
- *Integrity, confidentiality*, dan *avaliability Privacy*

UU ITE

- ✓ Mahasiswa memahami hal-hal yang diatur dalam UU ITE dan bentuk-bentuk pelanggaran UU ITE
  - Mahasiswa mampu menjelaskan kembali hal-hal yang diatur dalam UU ITE dan bentuk-bentuk pelanggaran UU ITE
  - Mahasiswa mampu melakukan analisa kasus pelanggaran UU ITE

UU Hak Cipta

- Mahasiswa memahami hal-hal yang diatur dalam UU Hak Cipta dan prosedur pengajuan HaKI
  - Mahasiswa dapat menjelaskan apa saja yang diatur dalam UU Hak Cipta dan bagaimana prosedur dalam pengajuan HaKI

Sertifikasi, Administrasi, *Maintenance*, *Management*, Audit

- Mahasiswa memahami sertifikasi internasional di bidang IT
  - Mahasiswa mampu menjelaskan macam-macam dan lingkup dari sertifikasi internasional di bidang IT

Confidentiality, Integrity, dan *Avaliability (CIA) Ethics*

- Mahasiswa memahami maksud dan jenis ancaman yang timbul dari *Confidentiality, Integrity*, dan *Availability* Pada Keamanan Informasi
  - Mahasiswa mampu menjelaskan maksud dan jenis ancaman yang timbul dari *Confidentiality, Integrity*, dan *Availability* Pada Keamanan Informasi

Confidentiality, Integrity, dan *Avaliability (CIA) Ethics*

Confidentiality

C*onfidentiality* merupakan aspek yang menjamin kerahasiaan data atau informasi. ***Kerahasiaan ini dapat diimplementasikan dengan berbagai cara, seperti misalnya menggunakan teknologi kriptografi dengan melakukan proses enkripsi (penyandian) pada transmisi data, pengolahan data (aplikasi dan database), dan penyimpanan data (storage).*** Akses terhadap informasi juga harus dilakukan dengan melalui mekanisme otorisasi (*authorization*) yang ketat. Sebagai contoh dari confidentiality adalah daftar pelanggan dari sebuah *Internet Service Provider* (ISP). Jadi, data dari daftar pelanggan tersebut seperti **nama, alamat, nomor telephone dan data lainnya** harus dilindungi agar tidak tersebar pada pihak yang tidak seharusnya mendapatkan informasi tersebut.

Ancaman yang muncul terhadap aspek *Confidentiality*

1. *Password strength* (lemahnya *password* yang digunakan, sehingga mudah ditebak ataupun di-*bruteforce*)
2. *Malware* (masuknya virus yang dapat membuat *backdoor* ke sistem ataupun mengumpulkan informasi *pengguna*)
3. *Social Engineering* (lemahnya *security awareness* pengguna dimana mudah sekali untuk 'dibohongi' oleh *attacker,* yang biasanya adalah orang yang sudah dikenalnya).

Cara mengatasi

Cara yang umum digunakan untuk menjamin tercapainya aspek c*onfidentiality* adalah dengan menerapkan enkripsi. Enkripsi merupakan sebuah teknik untuk mengubah file/data/informasi dari bentuk yang dapat dimengerti (*plaintext*) menjadi bentuk yang tidak dapat dimengerti (*ciphertext*), sehingga membuat *attacker* sulit untuk mendapatkan informasi yang mereka butuhkan. Enkripsi harus dilakukan pada level media penyimpanan dan transmisi data.

Confidentiality, Integrity, dan *Avaliability (CIA) Ethics*

Integrity

Integrity merupakan aspek yang menjamin bahwa data tidak boleh berubah tanpa ijin pihak yang berwenang (*authorized*). Bisa juga disebut menjaga keutuhan sesuatu yang sudah ditetapkan sebelumnya. Secara teknis ada beberapa cara untuk menjamin aspek *integrity* ini, seperi misalnya dengan menggunakan *message authentication code , hash function, digital signature*.

Ancaman yang muncul terhadap aspek *Integrity*

1. Menerapkan *strong encryption* pada media penyimpanan dan transmisi data.
2. Menerapkan *strong authentication* dan *validation* pada setiap akses file/akun login/action yang diterapkan. Authentication dan validation dilakukan untuk menjamin legalitas dari akses yang dilakukan.
3. Menerapkan *access control* yang ketat ke sistem, yaitu setiap akun yang ada harus dibatasi hak aksesnya. Misal tidak semua memiliki hak akses untuk mengedit, lainnya hanya bisa melihat saja.

Contoh kasus

Contoh mudah dan umum dari rusaknya *integrity* terkait keamanan informasi adalah pada proses pengiriman *email*. Alice mengirimkan email ke Bob. Namun ketika email dikirim, di tengah jalan Eve meng-*intercept* email tersebut dan mengganti isi emailnya kemudian baru diteruskan ke Bob. Bob akan mengira bahwa email tersebut benar dari Alice padahal isinya telah terlebih dahulu dirubah oleh Eve. Hal tersebut menunjukkan aspek *integrity* dari email yang dikirim oleh Alice telah hilang/rusak.

Confidentiality, Integrity, dan *Avaliability (CIA) Ethics*

Avaliability

Availability merupakan aspek yang menjamin bahwa data tersedia ketika dibutuhkan. Jadi, pada prinsipnya ketersediaan data dan informasi yang menyangkut kebutuhan suatu kegiatan merupakan suatu keharusan untuk menjalankan kegiatan tersebut. Jika *avaliabillity* data atau informasi yang dibutuhkan untuk menjalankan suatu proses kegiatan tidak dapat dipenuhi, maka proses kegiatan tersebut tidak akan terjadi atau terlaksana.

Ancaman yang muncul terhadap aspek *Avaliability*

1. *Disaster recovery plan* (memiliki cadangan baik tempat dan *resource*, apabila terjadi bencana pada sistem)
2. *Redundant hardware* (misal memiliki banyak *power supply*)
3. RAID (salah satu cara untuk menanggulangi *disk failure*)
4. *Data backup* (rutin melakukan backup data)

Contoh kasus

Untuk contoh dari rusaknya aspek *availability* sistem baru-baru ini adalah steam, *platform* distribusi *game* digital terbesar di dunia, tidak bisa diakses atau mengalami *server down* oleh serangan *Distributed Denial of Service (DDoS)*. Padahal pada waktu tersebut *steam* sedang dibanjiri pengunjung karena sedang mengadakan *winter sale*.

Confidentiality, Integrity, dan *Avaliability (CIA) Ethics*

Privacy

Pada dasarnya, *privacy* ini sama dengan *confidentiality*. Namun, jika *confidentiality* biasanya berhubungan dengan data-data perusahaan atau organisasi, sedangkan *privacy* lebih ke arah data-data yang bersifat pribadi. Contoh hal yang berhubungan dengan *privacy* adalah **e-mail** seorang pemakai tidak boleh dibaca oleh administrator . Hal ini untuk menjamin *privacy* dari isi e-mail tersebut, sehingga tidak bisa disalah gunakan oleh pihak lain.

Term & Condition Penggunaan Teknologi Informasi

Term & Condition Penggunaan Teknologi Informasi adalah aturan-aturan dan kondisi yang harus ditaati pada penggunaan teknologi informasi. Hal tersebut mencakup integrity, privacy, availability dan privacy dari informasi yang terdapat dan dibutuhkan di dalamnya.