DASAR KEAMANAN JARINGAN

Created by :
Vian Ardiyansyah Saputro
Revised by :
Ning Ratwastuti
Kevin Trikusuma Dewo
Tim Pengajar Jarkom

MENGAPA SECURITY ?

- **Internet pada awalnya dirancang untuk konektivitas**
  - ✓ Dianggap sangat dipercaya / Trust Assumed
  - ✓ Kita melakukan lebih banyak dengan internet saat ini
  - ✓ Protokol keamanan ditambahkan di atas TCP / IP
- **Aspek mendasar dari informasi harus dilindungi**
  - ✓ Data rahasia
  - ✓ Informasi Pegawai
  - ✓ Model bisnis
  - ✓ Lindungi identitas dan sumber daya
- **Kita tidak bisa menjaga diri kita terisolasi dari Internet**
  - ✓ Sebagian besar komunikasi bisnis dilakukan secara online
  - ✓ Kita menyediakan layanan online
  - ✓ Kita mendapatkan layanan dari organisasi pihak ketiga secara online

APAKAH INTERNET AMAN ?

❖ **JIKA ANDA BERTANYA ...**

- "Apakah Internet aman?“
- "Bisakah Internet diamankan?“
- "Bisakah masyarakat pengguna internet aman?“
- Jawaban yang benar adalah "**TIDAK**“

❖ **TETAPI JIKA ANDA BERTANYA ...**

- "Bisakah layanan / jaringan / transaksi saya diamankan?“
- "Bisakah Internet digunakan dengan aman?“
- "Bisakah saya tetap aman?“
- Jawabannya mungkin "**YA" (TETAPI DENGAN HATI-HATI!)**

TIPE SECURITY

- **KEAMANAN FISIK :**

  Melibatkan langkah-langkah seperti kontrol akses, pengawasan, dan kontrol lingkungan untuk melindungi aset fisik, fasilitas, dan personel.

- **KEAMANAN JARINGAN (NETWORK SECURITY) :**

  Melibatkan perlindungan terhadap infrastruktur jaringan komputer dan data yang ditransmisikan melalui jaringan tersebut.

- **KEAMANAN INFORMASI (INFOSEC) :**

  Berkaitan dengan perlindungan informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah.

SECURITY ITU TENTANG APA ?

❖ PENCEGAHAN :

Tindakan yang diambil untuk mencegah aset Anda rusak (atau dicuri),

❖ DETEKSI :

langkah-langkah yang diambil sehingga Anda dapat mendeteksi kapan, bagaimana, dan oleh siapa suatu aset telah rusak,

❖ REAKSI :

Tindakan yang diambil agar Anda dapat memulihkan asset Anda.

MODEL KEAMANAN INFORMASI

CIA TRIAD

- **CONFIDENTIALITY / KERAHASIAAN**:

  Mencegah penggunaan atau pengungkapan informasi yang tidak sah

- **INTEGRITY / INTEGRITAS** :

  Menjaga keaslian, keakuratan dan kelengkapan informasi.

- **AVAILABILITY / KETERSEDIAAN** :

  Memastikan pengguna yang berwenang memiliki akses yang andal dan tepat waktu ke informasi

CIA TRIAD

Item	Confidentiality	Integrity	Availability
Definisi	Berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut	Informasi tidak boleh diubah tanpa seijin pemilik informasi.	Berhubungan dengan ketersediaan informasi ketika dibutuhkan
Contoh Kasus	Data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security nomor kartu kredit, dsb) tersebar	Email di intercept di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju	Denial of Service Attack (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash
Bentuk Serangan	Usaha penyadapan (dengan program sniffer)	Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain	Contmailbomb, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya

MODEL KEAMANAN INFORMASI

PARKERIAN HEXAD

Model ini dikembangkan oleh Donn B. Parker, memperluas konsep CIA Triad dengan menambahkan tiga elemen lainnya, sehingga membentuk **enam dimensi** yang lebih komprehensif, yaitu :

- **POSSESSION/CONTROL (KEPEMILIKAN/KONTROL)**:

  Fokus pada kepemilikan fisik atau kendali atas informasi.

- **AUTHENTICITY / KEASLIAN** :

  Memastikan bahwa informasi asli dan berasal dari sumber yang valid, tanpa manipulasi atau pemalsuan.

- **UTILITY / KEGUNAAN** :

  Menjamin bahwa informasi berguna dan dapat dimanfaatkan untuk tujuan yang dimaksudkan.

PARKERIAN HEXAD

3 item sudah dijelaskan di CIA Triad, untuk 3 item yang lain adalah sebagai berikut :

Item	Possession or Control	Authenticity	Utility
Penjelasan	• Kontrol atas informasi • Mencegah terjadinya kontak fisik dengan data • Mencegah penyalinan atau penggunan yang tidak sah dari kekayaan intelektual	Keaslian atau kebenaran berkenaan dengan kebenaran atas kepemilikan suatu informasi.	• Utility atau funcionality atau kegunaan, dapat juga disimpulkan bahwa informasi itu harus berguna bagi penerimanya
Contoh	Misalkan seorang pencuri yang mencuri amplop tertutup berisi kartu debit bank dan nomor identifikasi pribadi tersebut. Bahkan jika pencuri tidak membuka amplop itu, wajar untuk korban menjadi khawatir bahwa pencuri bisa melakukannya setiap saat. Situasi yang menggambarkan hilangnya kontrol atau kepemilikan informasi tetapi tidak melibatkan pelanggaran kerahasiaan.	• Ketika kita akan mengakses email kita maka kita akan diminta untuk memasukkan password untuk memastikan bahwa memang kita pemilik dari email account tersebut • Kita diminta memasukkan PIN setiap kali hendak melakukan transaksi di ATM	• Data seseoarang yang dienkripsi datanya oleh pihak bank untuk mencegah data tersebut diakses secara tidak sah atau dimodifikasi oleh pihak yang tidak berwenang, akan tetapi jika pihak bank kehilangan key deskripsinya, maka hal ini akan menyebabkan terjadinya pelanggaran utilitas • Penggunan mata uang dollar untuk transaksi lokal dirasa kurang tepat.

MEKANISME SECURITY

- **ENKRIPSI** :

  Mengubah data menjadi sesuatu yang tidak dapat dipahami oleh penyerang,

- **OTENTIKASI**:

  Memverifikasi identitas yang diklaim pengguna,seperti nama pengguna, kata sandi, dll.

- **OTORISASI**:

  Memeriksa apakah pengguna memiliki hak untukmelakukan tindakan yang diminta.

- **AUDITING**:

  Melacak pengguna mana yang mengakses apa, kapan,dan ke mana. Secara umum, audit tidak memberikan perlindungan, tetapi dapat menjadi alat untuk analisis masalah.

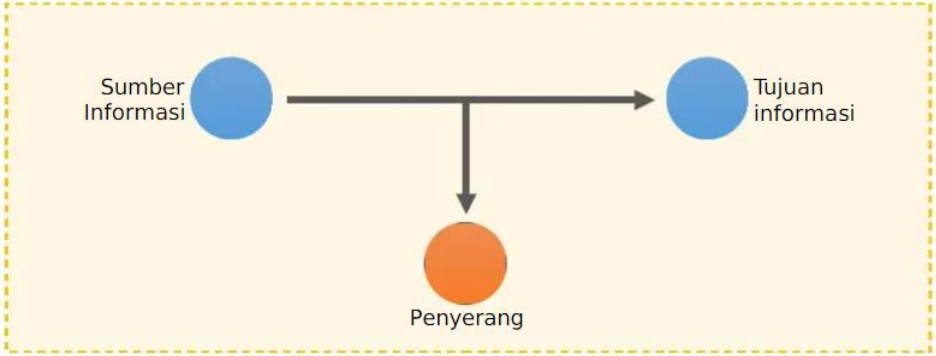
ANCAMAN / SERANGAN KEAMANAN

NORMAL FLOW

INTERRUPTION

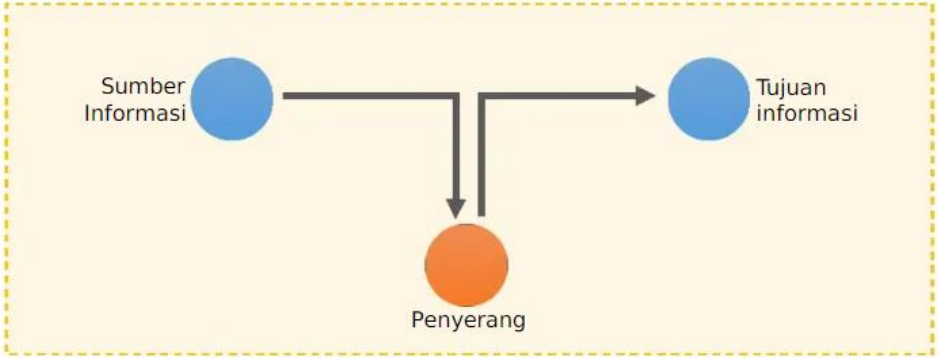
"Layanan atau data menjadi tidak tersedia, tidak dapat digunakan, dihancurkan, dan sebagainya, seperti kehilangan file, penolakan layanan, dll."

INTERCEPTION



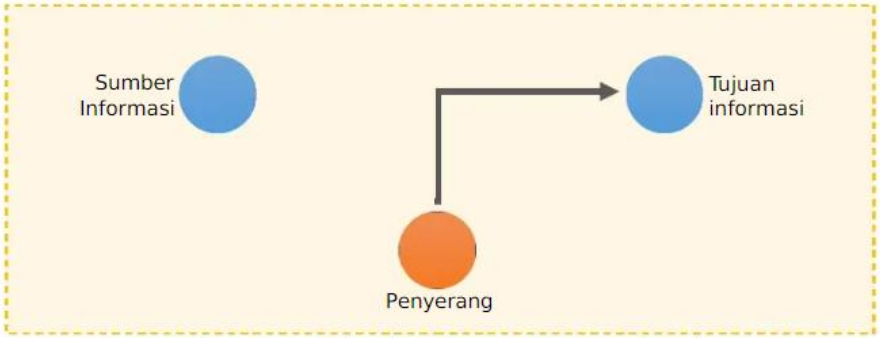
"Pihak ke-3 yang tidak sah telah mendapatkan akses ke objek, seperti mencuri data, mendengar komunikasi orang lain, dll."

MODIFICATION



"perubahan data yang tidak sah atau merusak layanan, seperti perubahan data, modifikasi pesan, dll."

FABRICATION



"Data atau kegiatan tambahan dihasilkan yang biasanya tidak ada, seperti menambahkan kata sandi ke sistem, memutar ulang pesan yang dikirim sebelumnya, dll."

CONTOH ANCAMAN UMUM

❖ **BOTNET**

"Kumpulan perangkat lunak robot, atau 'bot', yang menciptakan pasukan komputer yang terinfeksi (dikenal sebagai 'zombie') yangdikendalikan dari jarak jauh oleh pencetusnya"

❖ **APA YANG BISA DILAKUKANNYA :**

- Kirim email spam dengan virus terlampir.
- Sebarkan semua jenis malware.
- Dapat menggunakan komputer Anda sebagai bagian dari penolakan serangan layanan terhadap sistem lain.

CONTOH ANCAMAN UMUM

❖ **SPAM**

"Spam adalah salah satu metode yang lebih umum untuk mengirim informasi dan mengumpulkannya dari orang-orang yang tidak menaruh curiga.“

❖ **APA YANG BISA DILAKUKANNYA :**

- Mengganggu Anda dengan surat sampah yang tidak diinginkan.
- Buat beban bagi penyedia layanan komunikasi dan bisnis untuk memfilter pesan elektronik.
- Lihat informasi Anda dengan menipu Anda untuk mengikuti tautan atau memasukkan detail dengan penawaran dan promosi yang terlalu bagus.
- Memberikan jalan masuk untuk malware, penipuan (scam, fraud), dan ancaman terhadap privasi Anda.

CONTOH ANCAMAN UMUM

❖ **PHISHING**

"Phishing paling sering digunakan oleh penjahat dunia maya karena mudah dieksekusi dan dapat menghasilkan hasil yang mereka cari dengan sedikit usaha.“

❖ **APA YANG BISA DILAKUKANNYA :**

- Menipu Anda agar memberi mereka informasi dengan meminta Anda memperbarui, memvalidasi, atau mengonfirmasi akun Anda. Seringkali disajikan dengan cara yang tampaknya resmi dan tidak mengintimidasi, untuk mendorong Anda mengambil tindakan.
- Berikan penjahat cyber dengan nama pengguna dan kata sandi Anda sehingga mereka dapat mengakses akun Anda (akun bank online Anda, akun belanja, dll.) Dan mencuri nomor kartu kredit Anda.

CONTOH ANCAMAN UMUM

- **DISTRIBUTED DENIAL-OF-SERVICE (DDOS)**

  "Serangan penolakan layanan (DDoS) yang didistribusikan - atau serangan DDoS - adalah ketika pengguna jahat mendapatkan jaringankomputer zombie untuk menyabot situs web atau server tertentu.“

- **APA YANG BISA DILAKUKANNYA :**
  - Jenis serangan DDoS yang paling umum dan jelas terjadiketika penyerang "membanjiri" jaringan dengan informasi yang tidak berguna.
  - Banjir pesan yang masuk ke sistem target pada dasarnya memaksanya untuk ditutup, sehingga menolak akses ke pengguna yang sah.

CONTOH ANCAMAN UMUM

- **RANSOMWARE**

  "Ransomware adalah jenis malware yang membatasi akses ke komputer Anda atau file Anda dan menampilkan pesan yang menuntut pembayaran agar pembatasan dihapus.“

- **APA YANG BISA DILAKUKANNYA :**

  - **Ransomware Lockscreen :**

    Menampilkan gambar yang mencegahAnda mengakses komputer Anda.

  - **Encryption ransomware :**

    Mengenkripsi file pada hard drive sistem Andadan kadang-kadang pada drive jaringan bersama, drive USB, hard drive eksternal, dan bahkan beberapa drive penyimpanan cloud, mencegah Anda untuk membukanya.

Terima Kasih