# LAPORAN RESMI
# KEMANAN JARINGAN

## Resume Bab 1 Cyber Security Fundamentals


**Dosen :**
**Dr. Ferry Astika Saputra ST, M.Sc**
**Oleh :**
**Septiana Dyah Anissawati**
**D4 LJ Teknik Informatika B**
**3122640031**

**POLITEKNIK ELEKTRONIKA NEGERI SURABAYA**
**TAHUN AJARAN**
**2022/2023**

**Ketergantungan Sistem**

Meskipun internet dapat dilihat sebagai satu desa global besar, itu terdiri dari banyak sistem dan jaringan terpisah.

(Sistem atau jaringan terpisah biasanya dapat bekerja sama menggunakan protokol umum yang menentukan bagaimana sistem atau jaringan yang berbeda saling bertukar informasi. Meskipun baik ketika semuanya berfungsi bersama, ketergantungan ini cenderung memperkenalkan beberapa risiko. Pikirkan tentang efisiensi, keandalan, dan keamanan.)

**Nilai Data dan Informasi**

Pada tingkat dasar, data dan informasi sangat berharga bagi organisasi. Ini dianggap sebagai aset bisnis.

**Data dan Informasi**

- Laporan internal
- Data transaksi
- Informasi pelanggan
- Desain produk atau resep rahasia

**Ancaman Data & Informasi**

- Modifikasi tanpa izin
- Akses tanpa izin
- Kehilangan informasi

**Kebutuhan untuk Menjamin Keamanan Informasi**

Data dan informasi dapat berada dalam berbagai kondisi - diam, digunakan, atau bergerak.

**Data diam (Data at rest)**

- Data yang tidak aktif disimpan secara fisik di dalam database, gudang data, lembar kerja, arsip, pita, cadangan luar situs, dll.

**Data bergerak (Data in motion)**

- Data yang sedang berpindah melalui jaringan atau sementara berada di memori komputer untuk dibaca atau diperbarui.

**Apa saja Tujuan Utama Keamanan?**

Tujuan utama keamanan informasi adalah menjaga kerahasiaan, integritas, dan ketersediaan (CIA) aset dan sistem informasi.

**Kerahasiaan (Confidentiality)**

- Sifat informasi yang tidak dibuat tersedia atau diungkapkan kepada individu, entitas, atau proses yang tidak berwenang

**Integritas (Integrity)**

- Sifat menjaga akurasi dan kelengkapan aset

**Ketersediaan (Availability)**

- Sifat yang dapat diakses dan dapat digunakan sesuai permintaan oleh entitas yang diizinkan tanpa penundaan

**Menggunakan CIA dalam Konteks**

Perusahaan XYZ memiliki webmail untuk karyawan mengakses akun email mereka. Kadang-kadang mereka berbagi laporan dan berkomunikasi dengan pelanggan. Berikut adalah beberapa contoh yang mewakili konteks CIA.

Kerahasiaan **(Confidentiality)**

- Nama pengguna dan kata sandi (atau kredensial pengguna) untuk mengakses webmail harus diketahui hanya oleh pengguna. Konten komunikasi email harus hanya tersedia untuk penerima yang dimaksudkan.

Integritas

- Email yang diterima atau dikirim tidak dimodifikasi dari bentuk aslinya.

Ketersediaan

- Karena komunikasi email sangat penting bagi perusahaan, layanan email ini harus tersedia sepanjang waktu.

**Ancaman, Kerentanan, dan Risiko**

Dimensi lain yang harus kita pahami adalah hubungan Ancaman, Risiko terhadap konteks melindungi aset informasi kita.

**Ancaman (Threat)**

- Ancaman adalah penyebab potensial dampak yang tidak diinginkan terhadap sistem atau organisasi. Ada beberapa kategori ancaman seperti ancaman alam, ancaman manusia, dan ancaman lingkungan. Sumber Ancaman adalah: sengaja atau tidak sengaja.
- Ancaman Alam mengacu pada banjir, gempa bumi, tornado, tanah longsor, longsoran salju, badai petir, dan peristiwa lainnya.
- Ancaman Lingkungan mengacu pada kegagalan daya listrik jangka panjang, polusi, bahan kimia, dan kebocoran cairan.
- Ancaman Manusia adalah peristiwa yang diaktifkan oleh atau disebabkan oleh manusia, seperti tindakan tidak sengaja (pengetikan data yang tidak disengaja) atau tindakan yang disengaja (serangan berbasis jaringan, unggahan perangkat lunak jahat, akses tidak sah ke informasi rahasia).

**Kerentanan (Vulnerability)**

- Kerentanan adalah kelemahan dalam prosedur keamanan sistem, desain, implementasi, atau kontrol internal yang dapat dieksploitasi (dipicu secara tidak sengaja atau dimanfaatkan secara sengaja) dan mengakibatkan pelanggaran keamanan atau pelanggaran kebijakan keamanan sistem.

**Risiko (Risk)**

- Risiko adalah kemungkinan sumber ancaman tertentu mengeksploitasi kerentanan potensial dan dampak yang dihasilkan dari kejadian buruk tersebut pada organisasi.

| Vulnerability | Threat Source | Threat Action |
|---|---|---|
| Kerentanan Kritis dalam perangkat lunak server web telah diidentifikasi tetapi pembaruan perangkat lunak belum diterapkan. | Unauthorized users (i.e. internal employees, hacker, criminals) | Mendapatkan akses yang tidak sah ke informasi (file, informasi sensitif) |
| Kredensial (nama pengguna & kata sandi) karyawan yang telah dihentikan tidak dihapus dari sistem. | Terminated employees | Mengakses sistem perusahaan dan informasi properti. |

**Kontrol Keamanan**

Kontrol adalah tindakan pencegahan yang diterapkan oleh organisasi untuk melindungi aset informasi. Kontrol keamanan mengurangi risiko.

**Kebijakan dan Prosedur**

- Contoh kontrol : kebijakan keamanan siber, prosedur penanganan insiden
- Tujuan : untuk membuat semua orang menyadari pentingnya keamanan, menentukan peran dan tanggung jawab, dan lingkup masalah.

**Teknis**

- Contoh kontrol : firewall, sistem deteksi intrusi, perangkat lunak antivirus
- Tujuan : untuk mencegah dan mendeteksi serangan potensial, mengurangi risiko pelanggaran pada jaringan atau lapisan sistem.

**Fisik**

- Contoh kontrol : CCTV, kunci, ruang kerja aman

- Tujuan : untuk mencegah pencurian aset informasi secara fisik atau akses fisik yang tidak sah.

**Prinsip Keamanan**

Seperti yang kita lihat, ada berbagai jenis kontrol keamanan yang harus diterapkan berdasarkan penilaian risiko kita. Kontrol keamanan harus bekerja sama untuk mencapai tujuan keamanan kita. Dalam hal ini, ada dua prinsip keamanan yang sangat berguna untuk diingat:

**Prinsip Lingkaran Terlemah (Principle of Weakest Link)**

- Prinsip lingkaran terlemah pada dasarnya berarti bahwa penyerang akan mencari cara paling mudah untuk mencapai tujuannya. Misalnya, mungkin lebih mudah menebak kata sandi atau menipu karyawan untuk membagikan kata sandinya daripada mencoba menguraikan sesi jaringan yang dienkripsi.

**Prinsip Hak Akses Terkecil (Principle of Least Privilege)**

- Prinsip hak akses terkecil berarti bahwa entitas (orang, program, atau sistem) hanya dapat mengakses informasi dan sumber daya yang diperlukan untuk kebutuhan bisnisnya. Prinsip ini penting untuk membatasi kerusakan atau dampak dari pelanggaran dan diterapkan pada kontrol keamanan. Misalnya:
- Pengguna di sistem hanya memerlukan hak akses untuk diri mereka sendiri untuk menyelesaikan tugas mereka.
- Jika akun pengguna telah diretas, maka penyerang hanya memiliki akses ke aset informasi yang dapat diakses oleh pengguna tersebut.

Hasil :

# Knowledge Check 1

You will need to achieve a score of 80% or higher to pass the quiz. If you don't pass on your first attempt, you can retake the quiz as needed.

What is the term used to describe the security property that means our information can be read only by people who are allowed to read it?

- ○ Threat
- ◉ Confidentiality
- ○ Availability
- ○ Integrity

What is the term used to describe the security property that means the information can be assessible when needed?

- ○ Confidentiality
- ○ Integrity
- ◉ Availability
- ○ Accuracy

The property of safeguarding the accuracy and completeness of information assets is also known as

- ○ Confidentiality
- ○ Availability
- ◉ Integrity
- ○ Consistency

In reducing the impact of an attack, what can you do to prevent your data being accessed in the event that your computer is stolen?

- ○ implement user accounts with strong passwords
- ◉ encrypt the hard disk
- ○ install anti-virus software and keep it up to date
- ○ install a personal firewall

To an organization, systems that can no longer be patched with security fixes can be considered as a:

- ◉ Vulnerability
- ○ Risk
- ○ Threat
- ○ Loophole

Limiting access to information on the need to know basis is an example of:

- ◉ Principle of the Least Privilege
- ○ Principle of Access Control
- ○ The principle of the weakest link
- ○ Denial of Service

A potential cause of an unwanted impact to an organization is also known as

- ○ Control
- ◉ Threat
- ○ Vulnerability
- ○ Risk

Encrypting emails with sensitive content will achieve which security goal?

- ○ Integrity
- ○ Secrecy
- ○ Availability
- ◉ Confidentiality

The likelihood of a given threat source exploiting an existing vulnerability is also known as

- ◉ Risk
- ○ Exploitation
- ○ Threat
- ○ Vulnerability

An attacker will take advantage of the easiest way to bypass the security controls implemented in an organisation. This is also known as the:

- ○ Principle of the Least Privilege
- ○ Principle of Defense
- ○ Principle of Exploitation
- ◉ The principle of the weakest link

Which of the following can affect the integrity of data and information?

- ○ Unauthorized Shutdown
- ○ Denial of Service
- ○ Phishing
- ◉ Unauthorized Modification

Finish Quiz

**Course Progress**

**Course Navigation**

Module 1: Cyber Security Fundamentals
Knowledge Check 1
Module 2: Cyber Security in the Organization
Module 3: Cyber Security Controls
Module 4: Cyber Security Professionals
Module 5: Cyber Security Ecosystem

Return to Introduction to Cybersecurity Course