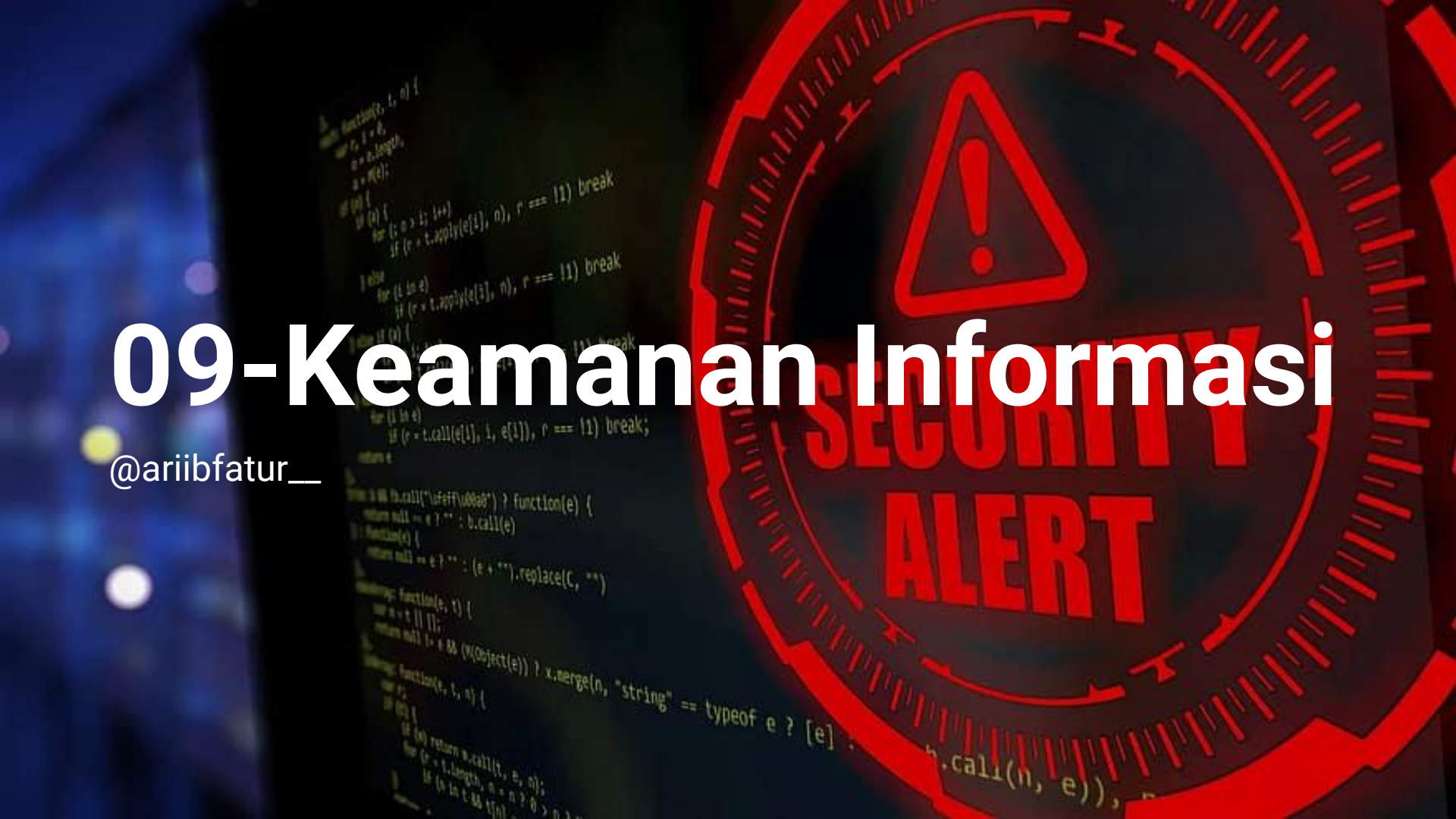


09-Keamanan Informasi

@ariibfatur__

Outline

- Aspek keamanan sistem informasi
- Konsep keamanan sistem informasi
- Bentuk ancaman keamanan sistem informasi
- Jenis-jenis serangan dan cara mengatasi pada sistem informasi

Tujuan Keamanan Sistem Informasi

1. Kerahasian.
2. Ketersediaan.
3. Integritas.

1 Kerahasian.

- Setiap organisasi berusaha melindungi data dan informasinya dari pengungkapan kepada pihak-pihak yang tidak berwenang.
- Sistem informasi yang perlu mendapatkan prioritas kerahasian yang tinggi

2 Ketersediaan

- Ketersediaan dimaksudkan untuk selalu siap menyediakan data dan informasi bagi mereka yang berwenang untuk menggunakannya.
- Tujuan ini penting khususnya bagi sistem yang berorientasi informasi seperti SIM, DSS dan sistem pakar (ES).

3 Integritas

- Semua sistem dan subsistem yang dibangun harus mampu memberikan gambaran yang lengkap dan akurat dari sistem fisik yang diwakilinya.

Aspek Keamanan Sistem Informasi

- Didalam keamanan sistem informasi melingkupi empat aspek, yaitu : **privacy, integrity, authentication, dan availability.**
- Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan electronic commerce, yaitu **access control dan nonrepudiation.**
- Tambahan Aspek **Authority**

Aspek Keamanan Sistem Informasi

1. Privacy
2. Integrity
3. Authentication
4. Availability
5. Access control
6. Nonrepudiation
7. Authority

1 Privacy

- Aspek **privacy atau confidentiality** adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.
- **Privacy** lebih kearah data-data yang sifatnya privat
- **Confidentiality** biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah servis) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

1 Privacy

Privacy

- Contoh hal yang berhubungan dengan privacy adalah e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator.

1 Privacy

Contoh Confidential

- Data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya).
- Daftar pelanggan dari sebuah Internet Service Provider (ISP).
- Konfirmasi akun LINE dengan scan barcode yang ada di Smartphone ketika membuka akun LINE melalui PC.

2 Integrity

- **Integrity** menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi.
- **Contoh** : Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin.

2 Integrity

- **Contoh**: ketika seorang nasabah akan memasukan uang ke dalam rekening, nasabah akan mengisi blanko
- Hak Teller untuk menambah jumlah saldo merupakan contoh integrity karena hanya Teller yang berwenang untuk menambah jumlah saldo sesuai yang disetorkan nasabah.

3 Authentication

- **Authentication** berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli.

1. **Membuktikan keaslian dokumen**, dapat dilakukan dengan teknologi watermarking dan digital signature.

3 Authentication

2. **Access control**, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi.
   - Pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya : password, biometric (ciri-ciri khas orang.
   - Ada tiga hal yang dapat ditanyakan kepada orang untuk menguji siapa dia:
     1) *What you have* (misalnya kartu ATM)
     2) *What you know* (misalnya PIN atau password)
     3) *What you are* (misalnya sidik jari, biometric)

3 Authentication

- **Contoh**: adanya sign in, login, dan sign up dihampir semua akun media sosial bahwa untuk memastikan bahwa yang mengakses adalah pemilik akun tersebut.

4 Availability

- Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan.
- Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.
- Contoh hambatan adalah serangan yang sering disebut dengan "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.

4 Availability

- **Contoh**: bank membutuhkan akses informasi ketika menyusun laporan akhir tahun, dan sistem harus mampu menjamin data yang diinginkan dapat terpenuhi seperti dana masuk, dana keluar, dana tersimpan, pinjaman, dan lain – lain.

5 Access control

- **Access control** berhubungan dengan cara pengaturan akses kepada informasi.
- Hal ini biasanya berhubungan dengan klasifikasi data (public, private, confidential, top secret) & user (guest, admin, top manager, dsb.), mekanisme authentication dan juga privacy.
- Access control seringkali dilakukan dengan menggunakan kombinasi user id/password atau dengan menggunakan mekanisme lain (seperti kartu, biometrics).

5 Access control

- **Contoh**: penggunaan PIN ketika melakukan transaksi menggunakan ATM. Penggunaan access control dapat membantu mengamankan data yang bersifat rahasia.

6 Nonrepudiation

- Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.
- **Contoh** : seseorang yang mengirimkan email untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan email tersebut.
- Aspek ini sangat penting dalam hal electronic commerce. Penggunaan digital signature, certifiates, dan teknologi kriptografi secara umum dapat menjaga aspek ini.
- Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari digital signature itu jelas legal.

6 Nonrepudiation

- **Contoh**: seseorang mengirimkan email untuk memesan/membeli barang tidak dapat disangkal bahwa orang tersebut pernah malakukan transaksi.

7 Aspek Authority

- Informasi yang berada dalam sistem hanya dapat diubah oleh yang diberi hak akses untuk mengubah, sedangkan pengunjung hanya diberi hak akses untuk menampilkan informasi.
- **Contoh**: dalam sebuah website hanya admin yang dapat mengatur isi dan tampilan website dan pengunjung hanya dapat menampilkan informasi yang disajikan oleh admin web dan juga memberi komentar.

Bentuk ancaman keamanan sistem informasi

1. Interruption
2. Interception
3. Modification
4. Fabrication

1 Interruption

- Perangkat sistem menjadi rusak atau tidak tersedia.
- Serangan ditujukan kepada ketersediaan (availability) dari sistem.
- **Contoh** serangan adalah "denial of service attack".

2 Interception

- Pihak yang tidak berwenang berhasil mengakses asset atau informasi.
- Contoh dari serangan ini adalah penyadapan (wiretapping).

3 Modification

- Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset.
- Contoh dari serangan ini antara lain adalah mengubah isi dari website dengan pesan-pesan yang merugikan pemilik website.

4 Fabrication

- Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem.
- Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

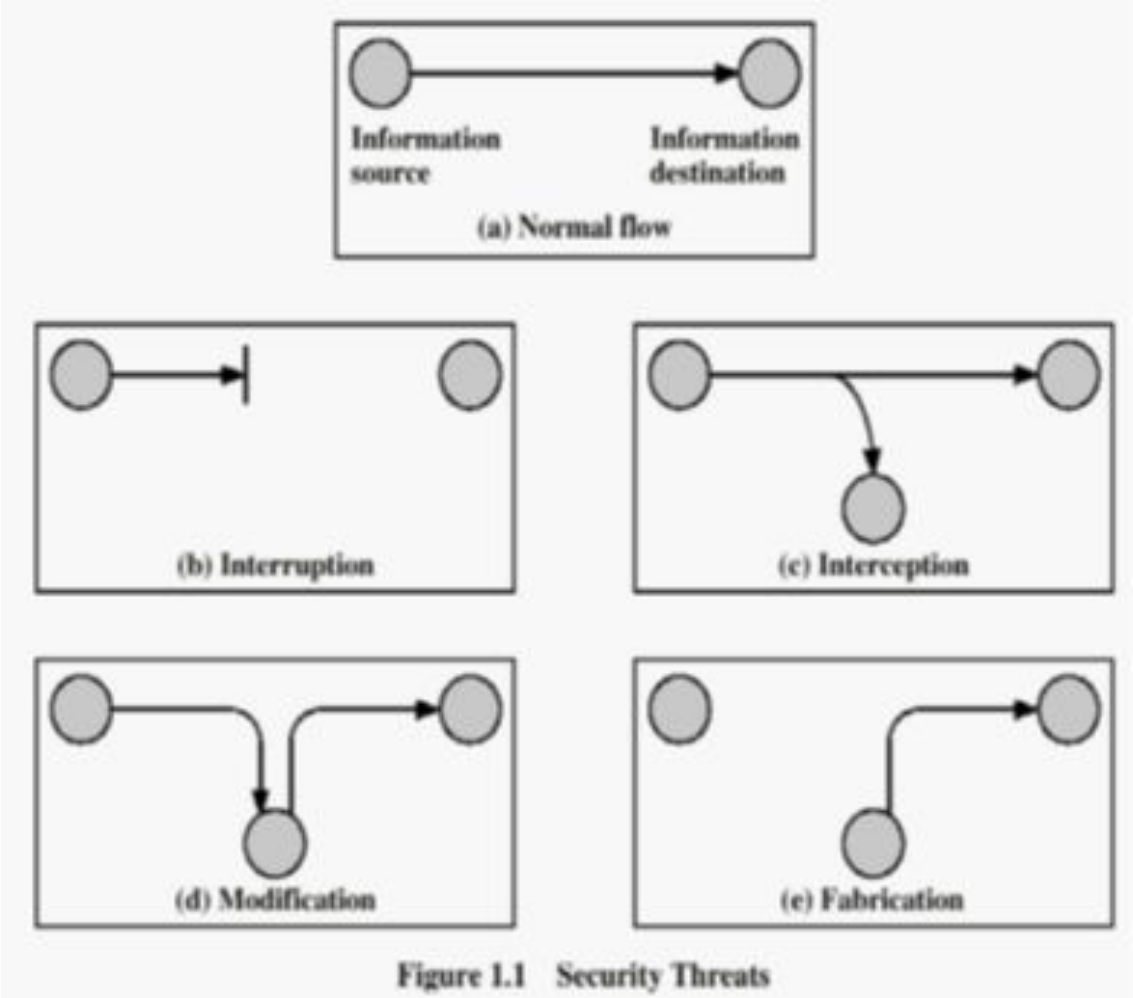


Figure 1.1 Security Threats

Pencegahan/ Mitigasi Serangan Pada Sistem Informasi

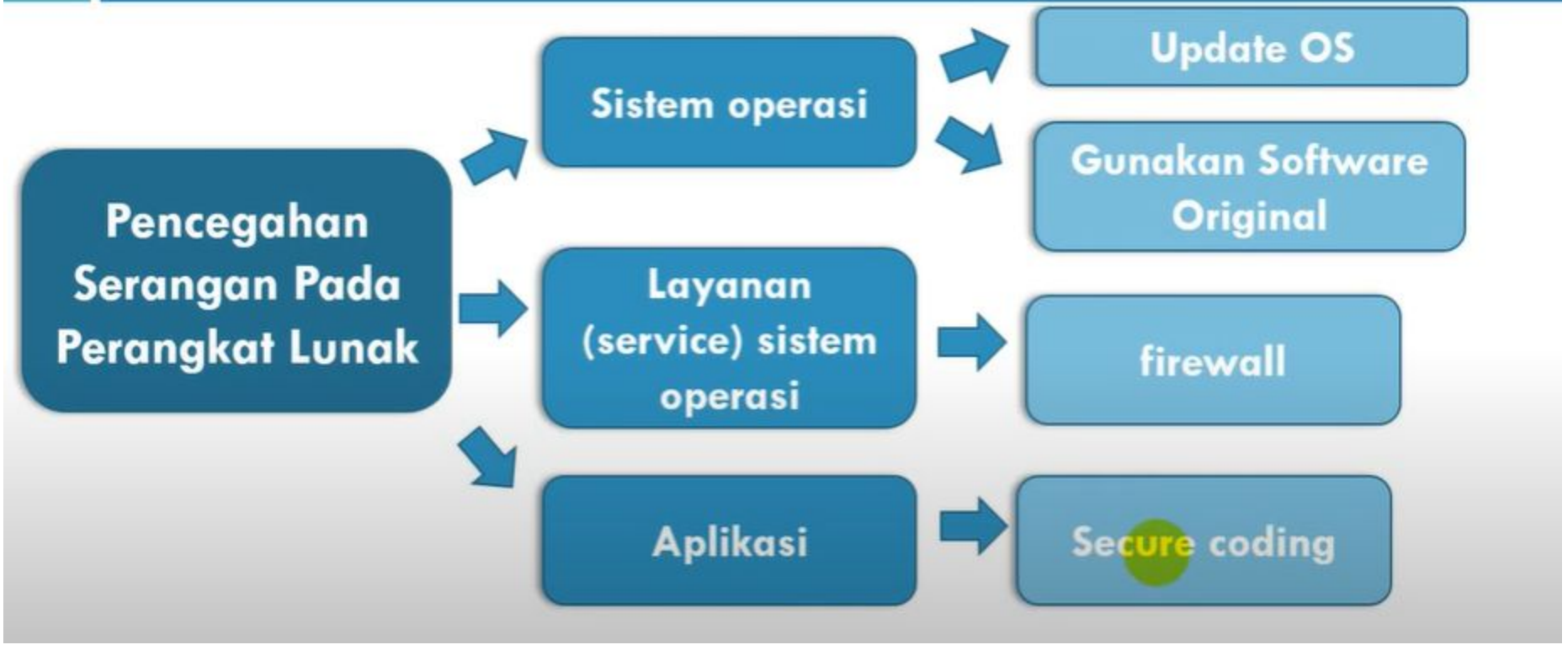
1. Pencegahan Serangan Pada Perangkat Keras
2. Pencegahan Serangan Pada Perangkat Lunak
3. Pencegahan Serangan pada jaringan komputer
4. Pencegahan serangan pada basis data
5. Pencegahan serangan pada pengguna sistem informasi.

1 Pencegahan Serangan Pada Perangkat Keras

Memberikan pengamanan fisik di ruang server/ data center:

1. Pengamanan fisik mulai dari akses kontrol terhadap ruang data center
2. akses kontrol terhadap server rack
3. akses kontrol terhadap fisik server.

2 Pencegahan Serangan Pada Perangkat Lunak



3 Pencegahan Serangan Pada jaringan komputer

1. Desain jaringan komputer yang benar
2. Pemasangan aplikasi monitoring jaringan yang memiliki fitur Intrusion Detection Ssytem / Intrusion Prevention System
3. Autentikasi pengguna menggunakan sistem captive portal.

4 Pencegahan Serangan Pada basis data

1. Pembatasan penggunaan kode SQL sebagai input pada sistem informasi
2. Mengubah karakter spesial kedalam format HTML kemudian pengecekan dilakukan menggunakan regular *expression* dan *exceptions*.

5 Pencegahan Serangan Pada pengguna sistem informasi

1. Edukasi
2. Standard Operational Procedure baku

KUIS

1. Sebutkan dan Jelaskan Tujuan keamanan sistem informasi
2. Sebutkan dan Jelaskan Aspek keamanan sistem informasi
3. Sebutkan dan Jelaskan Bentuk ancaman keamanan sistem informasi
4. Sebutkan dan Jelaskan Pencegahan/ Mitigasi Serangan Pada Sistem Informasi
5. Sebutkan dan berikan contoh kasus bobolnya sistem keamanan informasi yang terjadi di Indonesia? Termasuk kedalam serangan apa?

Referensi

- https://student.blog.dinus.ac.id/fachrizanoor/2017/10/15/aspek-aspek-keamanan-informasi/
- https://glints.com/id/lowongan/kupas-information-security/#.X8oszrMRXIU
- https://www.dosenpendidikan.co.id/keamanan-komputer/
- https://teks.co.id/sistem-keamanan-komputer/
- Johan Ericka Wahyu Prakasa.2020. Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi. Jurnal Ilmiah Teknologi Informasi Asia. Vol.14, No.2, Tahun 2020.

sumber :

Keamanan Sistem Informasi || Materi 10 - YouTube