MODUL - WEEK.05
DATABASE SECURITY AND ADMINISTRATION

I. DESKRIPSI TEMA

Apply user role and right access to increase security in database system

II. CAPAIAN PEMBELAJARAN MINGGUAN (SUB-CAPAIAN PEMBELAJARAN)

CLO2-SUB-CLO5: Students are able to apply security in database (C3): Backup & Restore Database, Users Administrations & Roles, Data Transformation Services, Grant & Revoke

III. PENUNJANG PRAKTIKUM

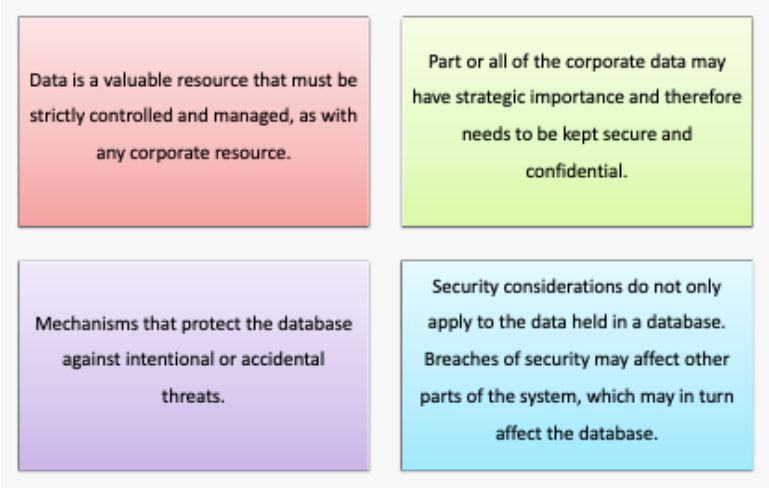
1. Microsoft SQL Server management studio, SQL Server 2019
2. Module Practicum
3. These Module have been adapted from Connolly, T., & Begg, C. (2015). Database Systems: A Practical Approach to Design, Implementation, and Management. 6th edition. Pearson Education. USA. ISBN: 978-1-292-06118-4, **Chapter 20**

IV. LANGKAH-LANGKAH PRAKTIKUM

1. Database Security

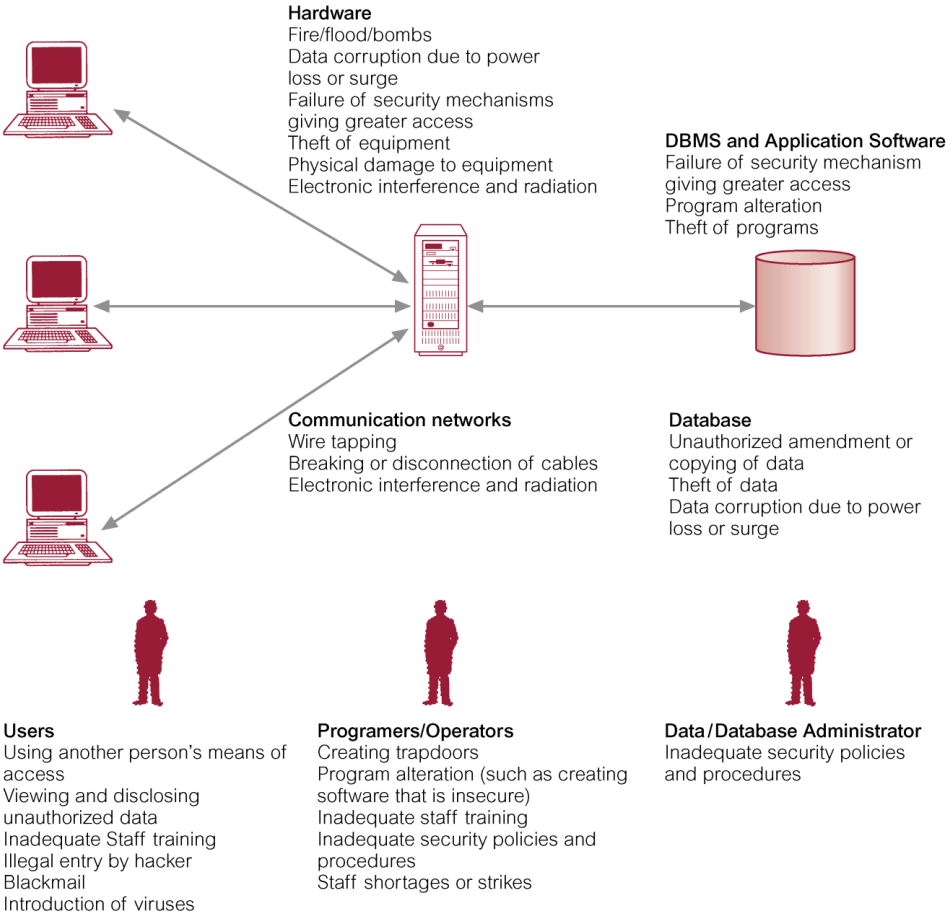
Database Security is the mechanisms that protect the database against intentional or accidental threats. Involves measures to avoid:

a. Theft and fraud
b. Loss of confidentiality (secrecy): refers to the need to maintain secrecy of data (critical data)
c. Loss of privacy: refers to the need to protect data about individuals
d. Loss of integrity: invalid or corrupted data
e. Loss of availability: cannot be accessed

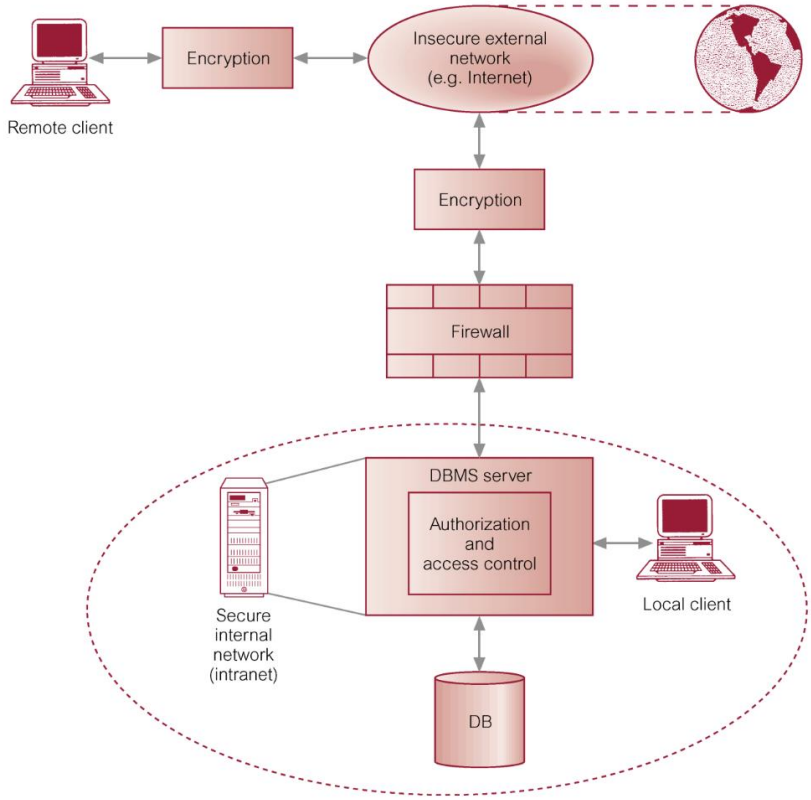


2. **Threat**

   Any situation or event, whether intentional or unintentional, that will adversely affect a system and consequently an organization.



3. Protecting a Computer System



Countermeasures – Computer-Based Controls

Concerned with physical controls to administrative procedures and includes:

1. Authorization
2. Access controls
3. Views
4. Backup and recovery
5. Integrity
6. Encryption
7. RAID technology

4. Access Control: GRANT and REVOKE Command

- **Access Control - Authorization Identifiers and Ownership**
  1. D Authorization identifier is normal SQL identifier used to establish identity of a user. Usually has an associated password.
  2. Used to determine which objects user may reference and what operations may be performed on those objects.
  3. Each object created in SQL has an owner, as defined in AUTHORIZATION clause of schema to which object belongs.
  4. Owner is only person who may know about it.

- **Actions user permitted to carry out on given base table or view:**
  1. **SELECT** **Retrieve data from a table.**
  2. **INSERT** **Insert new rows into a table.**
  3. **UPDATE** **Modify rows of data in a table.**
  4. **DELETE** **Delete rows of data from a table.**
  5. **REFERENCES** **Reference columns of named table in integrity constraints.**
  6. **USAGE** **Use domains, collations, character sets, and translations.**

  - Can restrict INSERT/UPDATE/REFERENCES to named columns.
  - Owner of table must grant other users the necessary privileges using GRANT statement.
  - To create view, user must have SELECT privilege on all tables that make up view and REFERENCES privilege on the named columns.

5. **Grant**

GRANT {PrivilegeList | ALL PRIVILEGES}
ON ObjectName
TO {AuthorizationIdList | PUBLIC}
[WITH GRANT OPTION]

- PrivilegeList consists of one or more of above privileges separated by commas.
- ALL PRIVILEGES grants all privileges to a user.
- PUBLIC allows access to be granted to all present and future authorized users.
- ObjectName can be a base table, view, domain, character set, collation or translation.
- WITH GRANT OPTION allows privileges to be passed on.

6. **Grant Examples**

- Give Manager full privileges to Staff table.

```
GRANT ALL PRIVILEGES
ON Staff
TO Manager WITH GRANT OPTION;
```

- Give users Personnel and Director SELECT and UPDATE on column salary of Staff.

```
GRANT SELECT, UPDATE (salary)
ON Staff
TO Personnel, Director;
```

- Give all users SELECT on Branch table.

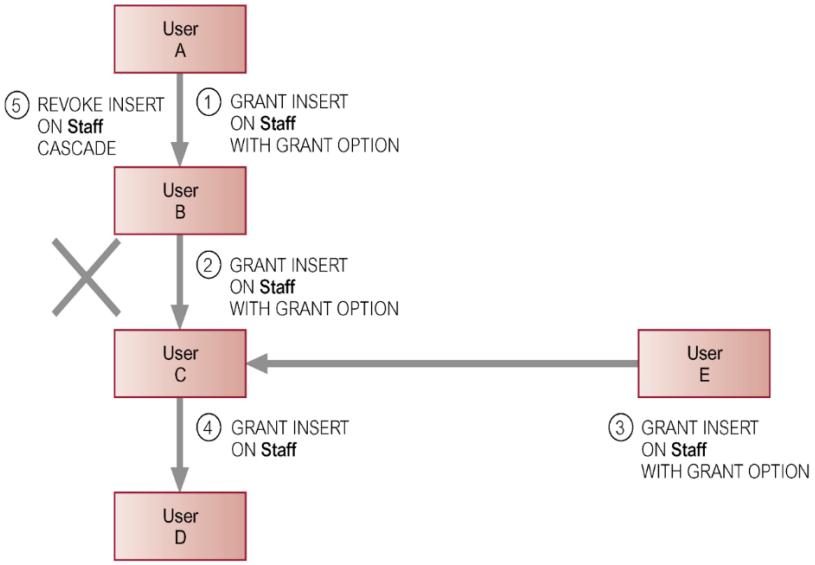
```
GRANT SELECT
ON Branch
TO PUBLIC;
```

7. **Revoke**

REVOKE takes away privileges granted with GRANT.

```
REVOKE [GRANT OPTION FOR]
        {PrivilegeList | ALL PRIVILEGES}
ON ObjectName
FROM {AuthorizationIdList | PUBLIC}
        [RESTRICT | CASCADE]
```

- ALL PRIVILEGES refers to all privileges granted to a user by user revoking privileges.
- GRANT OPTION FOR allows privileges passed on via WITH GRANT OPTION of GRANT to be revoked separately from the privileges themselves.
- REVOKE fails if it results in an abandoned object, such as a view, unless the CASCADE keyword has been specified.
- Privileges granted to this user by other users are not affected.



- Revoke privilege SELECT on Branch table from all users.

```
REVOKE SELECT
ON Branch
FROM PUBLIC;
```

- Revoke all privileges given to Director on Staff table.

```
REVOKE ALL PRIVILEGES
ON Staff
FROM Director;
```

8. **Syntax**

   GRANT

   GRANT { ALL [PRIVILEGES] }
   | permission [(column [,...n])] [,...n]
   [ON [class ::] securable] TO principal [,...n]
   [WITH GRANT OPTION] [AS principal]

9. **REVOKE**

   REVOKE { ALL [PRIVILEGES] }
   | permission [(column [,...n])] [,...n]
   [ON [class ::] securable] FROM principal [,...n]
   [CASCADE] [AS principal]

10. **Assessment**

    a. Lakukan backup database ‘dbPracCase’ secara full backup ke Drive D:\ dengan nama file ‘ContohBackUp1’.
    b. Lakukan restore database dari file ‘ContohBackUp1’ di Drive D:\ menjadi database baru bernama ‘praktikum’.
    c. Buatlah sebuah user bernama ‘user1’ dengan password ‘user1’ dan server roles yang dimiliki adalah ‘public, sysadmin, serveradmin, setupadmin’.
    d. Buatlah sebuah user bernama ‘user2’ dengan password ‘user2’ dengan default database ‘dbPracCase’ dan user mapping ke database ‘dbPracCase’ dan ‘master’.
    e. Berilah hak akses select kepada user2 terhadap tabel MsPatient. (**grant**)
    f. Berilah hak akses insert, update kepada user2 terhadap tabel TransactionDetail. (**grant**)
    g. Berilah semua hak akses kepada user2 terhadap tabel MsDoctor. (**grant**)
    h. Cabutlah hak akses select pada tabel MsPatient dari user2. (**revoke**)
    i. Cabutlah hak akses insert, update pada tabel TransactionDetail dari user2. (**revoke**)
    j. Cabutlah semua hak akses pada tabel MsDoctor dari user2. (**revoke**)

REFERENSI

Connolly, T., & Begg, C. (2015). Database Systems: A Practical Approach to Design, Implementation, and Management. 6th edition. Pearson Education. USA. ISBN: 978-1-292-06118-4, **Chapter 20**