# Database Security

## Unit 9 [5 LH]

- Issues regarding the right to access information, syste related issues
- system levels: physical hardware, Operating system, DBMS level, Multiple security level and
- categorization of data and users, Loss of integrity, Loss availability, Loss of confidentiality,
- Access control, Inference control, flow control, data encryption.

# The Need for database securi

- Organizational databases tend to concentrate sensitive information in a single log system. Examples include:
  - Corporate financial data
  - Confidential phone records
  - Customer and employee information, such as name, Social Security number,bank account information, and credit card information
  - Proprietary product information
  - Health care information and medical records
- For many businesses and other organizations, it is important to be able to provide customers, partners, and employees with access to this information.
- But such information can be targeted by internal and external threats of misuse o unauthorized change.

# What is Database?

- A **database** is a structured collection of data stored for use by one or more applications.
- In addition to data, a database contains the relationships between data items and groups o data items.
- For example: A simple personnel file might consist of a set of records, one for each employ Each record gives the employee's name, address, date of birth, position, salary, and other d needed by the personnel department. A personnel database includes a personnel file, as ju described.
- A **database management system (DBMS**), which is a suite of programs for constructing a maintaining the database and for offering ad hoc query facilities to multiple users and applications. A **query language** provides a uniform interface to the database for users and applications.
- Database systems provide efficient access to large volumes of data and are vital
- to the operation of many organizations.

# Database Security

- Database security refers to the collective measures used to protect and secure a datab or database management software from illegitimate use and malicious threats and att
- It is a broad term that includes a multitude of processes, tools and methodologies tha ensure security within a database environment.
- Database security covers and enforces security on all aspects and components of databases. This includes:
  - Data stored in database
  - Database server
  - Database management system (DBMS)
  - Other database workflow applications
- Database security is generally planned implemented and maintained by a database administrator and/or other information security professional.

# Best Practices of Database Security

- Because databases are nearly always network-accessible, any security th to any component within or portion of the network infrastructure is also threat to the database, and any attack impacting a user's device or workstation can threaten the database. Thus, database security must ext far beyond the confines of the database alone.
- When evaluating database security in your environment to decide on you team's top priorities, consider each of the following areas:
- **Physical security**:
  - Whether your database server is on-premise or in a cloud data center, it must be located within a secure, climate-controlled environment. (If your database server a cloud data center, your cloud provider will take care of this for you.)

# Best Practices of Database Security

- **Administrative and network access controls**:
  - The practical minimum number of users should have access to the database, and the permissions should be restricted to the minimum levels necessary for them to do the jobs.
    - Likewise, network access should be limited to the minimum level of permissions necessary.
- **End user account/device security**:
  - Always be aware of who is accessing the database and when and how the data is bei used.
  - Data monitoring solutions can alert you if data activities are unusual or appear risky.
  - All user devices connecting to the network housing the database should be physicall secure (in the hands of the right user only) and subject to security controls at all time

# Best Practices of Database Security

- **Encryption**:
  - ALL data—including data in the database, and credential data—should be protected with in-class encryption while at rest and in transit.
  - All encryption keys should be handled in accordance with best-practice guidelines.

- **Database software security:**
  - Always use the latest version of your database management software, and apply all patch soon as they are issued.

- **Application/web server security:**
  - Any application or web server that interacts with the database can be a channel for attack should be subject to ongoing security testing and best practice management.

# Best Practices of Database Security

- **Backup security**:
  - All backups, copies, or images of the database must be subject to same (or equally stringent) security controls as the database itself
- **Auditing**:
  - Record all logins to the database server and operating system, and log all operations performed on sensitive data as well. Database security standard audits should be performed regularly.

# Issues regarding the right to access informati

- Information access is the freedom or ability to identify, obtain and make use of data or information effectively.
- Freedom of information is a fundamental human right
- Right to access information depends upon the information policy and access control mechanisms of a organization.
- Information access covers many issues including **copyright**, **open source**, **privacy**, and **security**

# Security Related Issues

- Databases are a key target for cybercriminals due to the ofte valuable nature of sensitive information locked away inside.
- Whether the data is financial or holds intellectual property a corporate secrets, hackers worldwide can profit from breach a businesses' servers and plundering databases.
- The top ten vulnerabilities often found in database-driven systems, whether during the creation phase, through the integration of applications or when updating and patching, a

# Security Related Issues

- Deployment Failures
- Broken Databases
- Data Leaks
- Stolen Database backups
- A lack of segregation
- SQL Injection
- Database Insonsistencies

# Deployment Failure

- The most common cause of database vulnerabilities is a lack of due
  at the moment they are deployed.
- Although any given database is tested for functionality and to make
  sure it is doing what the databases is designed to do, very few check
  are made to check the database is not doing things it should not be
  doing.

# Broken Databases

- Malicious programs are able to infect vulnerable computers within minutes of deployment, taking down thousands of databases in minutes.

# Data Leaks

- Databases may be considered a "back end" part of the office and se
  from Internet-based threats (and so data doesn't have to be encrypt
  but this is not the case.
- Databases also contain a networking interface, and so hackers are a
  to capture this type of traffic to exploit it.
- To avoid such a pitfall, administrators should use SSL- or TLS-encryp
  communication platforms

# Stolen Database Backups

- External attackers who infiltrate systems to steal data are one threat but what about those inside the corporation?
- Insiders are also likely to steal archives — including database backup — whether for money, profit or revenge.
- This is a common problem for the modern enterprise, and businesses should consider encrypting archives to mitigate the insider-risk.

# A lack of segregation

- The separation of administrator and user powers, a well as the segregation of duties, can make it more difficult for fraud or theft undertaken by internal st
- In addition, limiting the power of user accounts ma give a hacker a harder time in taking complete con of a database.

# SQL Injection

- A popular method for hackers to take, SQL injections remain a critica problem in the protection of enterprise databases.
- Applications are attacked by injections, and the database administra is left to clean up the mess caused by unclean variables and maliciou code which is inserted into strings, later passed to an instance of SQ server for parsing and execution.
- The best ways to protect against these threats are to protect web-fa databases with firewalls and to test input variables for SQL injection during development.

# Database Inconsistencies

- The common thread which brings all of these vulnerabilities together is a lack of consistency, which is an administrative rath than database technology problem.
- System administrators and database developers need to develo consistent practice in looking after their databases, staying awa of threats and making sure that vulnerabilities are taken care of
- This isn't an easy task, but documentation and automation to tr and make changes can ensure that the information contained i enterprise networks is kept secure.