

Database Security

Levels of database security

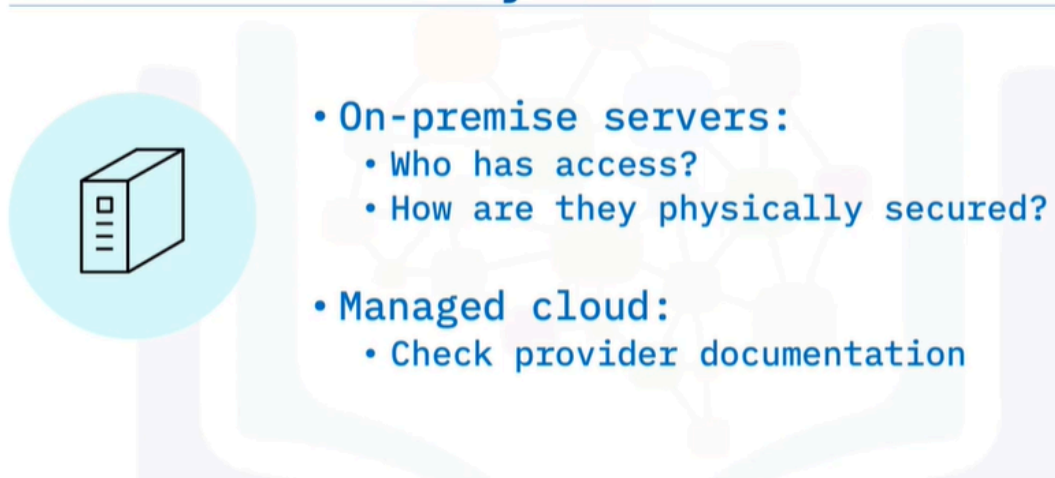


Levels of database security



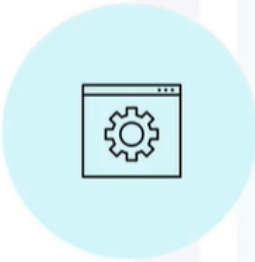
- Ensuring the security of the data stored in your systems is an essential part of the database management role. It involves identifying the potential risks to your data and mitigating those risks by applying security measures and controls at all levels of a system. Even though the actual implementation of the measures at some levels may not be your direct responsibility, it is imperative that you evaluate that they are adequate for the data you store or access there.

Server security



- Firstly, you need to make sure that the actual servers in your system are physically secure. For on-premise servers, you should assess who has access to server location and the security measures in place. If you are using a managed cloud environment, your provider will be responsible for the security at this level.

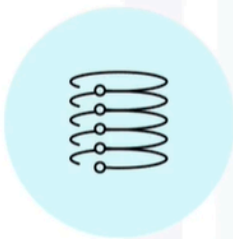
Operating system configuration



- Regular patching
- System hardening
- Access monitoring

- Next, you should consider the operating system hosting your database. You should ensure that it is regularly patched with the latest tested updates, that it is hardened using a known configuration to reduce vulnerabilities, and that it is continuously monitored for any unauthorized access.

RDBMS configuration

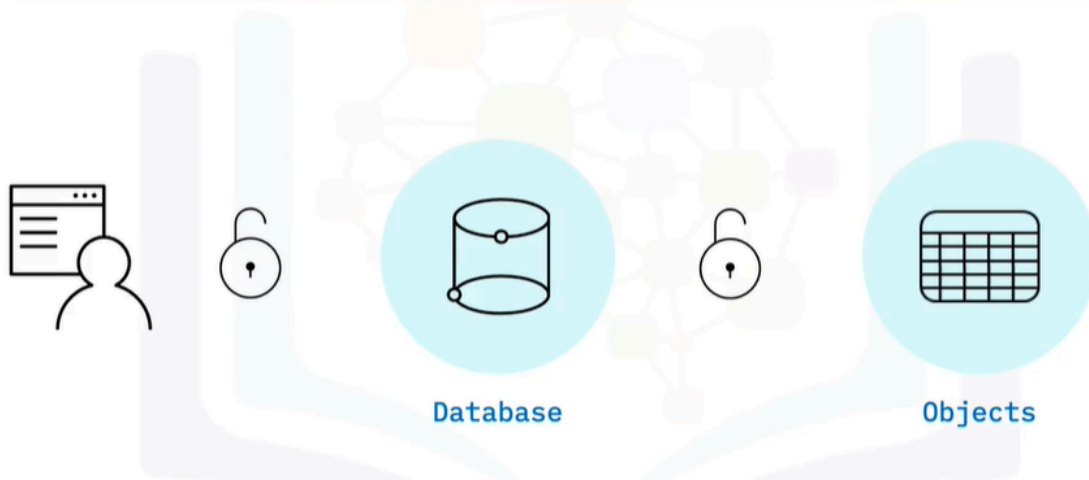


- Regular patching
- Review and use system-specific security features
- Reduce the number of administrators

- You should take similar measures on your RDBMS to those for your operating system. You should regularly apply the latest tested updates, you should review and use all security features and configuration options available in the

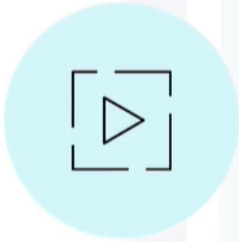
system, and you should ensure that only a small set of trusted users have administrative privileges.

Accessing databases and objects



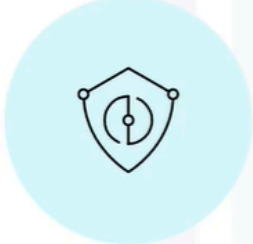
- Users and client applications need to be permitted to access a server or database and the objects in it. Firstly, users need to be authenticated on the server or database to enable them to access it. And then they need to be granted permissions on individual objects, or groups of objects, in the database to interact with them.

Authentication



- Similar to:
 - PIN for cell phone
 - Password for computer
 - Verifies that the user is who they claim to be:
 - For example, by validating username and password
 - External authentication methods
 - PAM
 - Windows login IDs
 - LDAP
 - Kerberos
- Database authentication is similar to the authentication you use when using a PIN or fingerprint to access your cell phone or a password to access your computer. It is a process of verifying that the user is who they claim to be, for example, by validating credentials such as username and password. Some database systems enable you to use operating system or other credentials to authenticate against a database. For example, you can use external authentication methods, such as pluggable authentication module (PAM), Windows login IDs, lightweight directory access protocol (LDAP) or Kerberos.

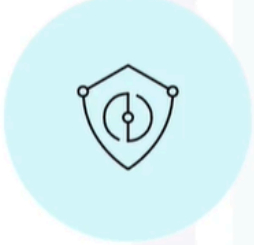
Authorization



- Authorized to access:
 - Objects
 - Data
- Grant privileges to:
 - Users
 - Groups
 - Roles

- Even when a user is authenticated on a database, they still need to be authorized to access the objects and data in that database. You authorize users by giving them permissions, or privileges, to access objects and data. Because groups of users often need the same access privileges, in most RDBMSs you can grant privileges to a group of users who undertake a specific role in that database.

Privileges



product_id	product	category_id
1	Rich coffee	100
2	Smooth coffee	100
3	Breakfast tea	101
4	Earl grey tea	101
5	Assam tea	101

Privileges



product_id	product	category_id
1	Rich coffee	100
2	Smooth coffee	100
3	Breakfast tea	101
4	Earl grey tea	101
5	Assam tea	101
6	Darjeeling	101

Privileges



product_id	product	category_id
1	Rich coffee	100
2	Smooth coffee	100
3	Breakfast tea	101
4	Lady grey tea	101
5	Assam tea	101
6	Darjeeling	101

Privileges

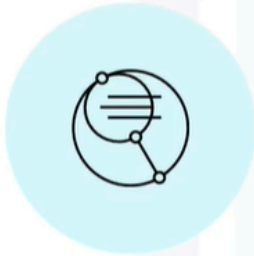


product_id	product	category_id	cost
1	Rich coffee	100	
3	Breakfast tea	101	
4	Lady grey tea	101	
5	Assam tea	101	
6	Darjeeling	101	

Principle of least privilege

- Assigning privileges will vary depending on the object you are working with. For example, on a table you can allow users to select, insert, update, or delete data, or to alter the structure of the table.
- In some RDBMSs, you can narrow this down even further to assign privileges on a columnar basis. You should always use the principle of least privilege, that is, only allow users to access the least amount of data that they need to succeed in their tasks.

Auditing

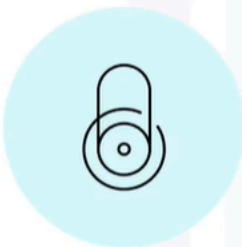


- **Monitor:**
 - Who accesses what objects
 - What actions they perform
- **Audit:**
 - Actual access against security plan

- In addition to restricting users to only access the information and objects that their role requires, you should also consider monitoring and auditing database activity. You should track which users access a server or database and the actions that they perform.

Analyzing this information against your security plan can alert you to gaps in it.

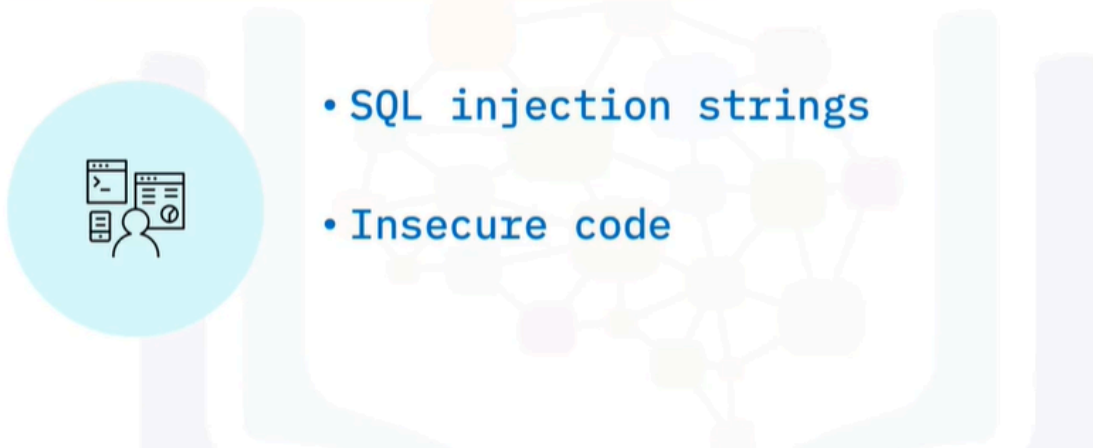
Encryption



- **Adds another layer of security:**
 - Intruders need to decrypt
- **Industry & regional regulations:**
 - Algorithms
 - Key management
- **Performance impact**

- As well as securing your systems and data and auditing access to it, you could consider using encryption to add another layer to your security system. Then if an intruder does manage to access the data, they also have to decrypt the data to make any use of it. Certain industry regulations and regions legislate the use of specific levels of encryption for sensitive data. It is important to check such regulations for algorithm and key management requirements when planning your database security. Do remember though, that encrypting and decrypting data can be a time and resource intensive operation, so you will need to consider the impact this will have on your operations and whether you need to upgrade your hardware accordingly.

Application security



- Even the most secure combination of operating system and RDBMS can be compromised by lax application security such as SQL injection strings and insecure code. Therefore, it is important that you test and monitor the security of any applications interacting with your data and databases.

Summary

In this video, you learned that:

- You need to consider the security of the server and operating system, as well as the database and data
 - Users need to be authenticated on the server or database to access it
 - Users need to be authorized to access the objects and data in the database
 - You should use the principle of least privilege
 - You should monitor and audit database activity
 - Encryption can strengthen your data security
 - Data security includes securing your applications
-