Database Security

1 Database Management System

DBMS Roles

- Concurrency
- Security
- Data integrity
- Administration procedures
  - Change management
  - Performance monitoring/tuning
  - Backup and recovery
- Automated rollbacks, restarts and recovery
- Logging/auditing of activity

DBMS consists of

1. The data
2. The engine
   - Allows data to be
     - Locked
     - Accessed
     - Modified
3. The schema
   - Defines the database's logical structure

2 NoSQL Databases

Created lazily - none of the commands have actually performed any operations on the server until the first document is included into them

3 Database Security Overview

Primary concepts

- Authentication - who are you?
- Authorization - what are you allowed to do?
- Encryption - protecting the data
- Auditing - what did you do?

Other important concepts

- Redaction - disguise sensitive data on returned results
- Masking - creating similar but inauthentic version of the data for training/testing
- Firewall - threat patterns, approved whitelisted commands, blacklist (harmful) commands, monitor for data leakage, evaluate IP address/time/location
- Integrity - data should be accurate and tolerant to physical problems

4 Database security background

- Vast majority of records breached are from database leaks
  - Not surprising that hackers are going after databases, they contain transactional information, financial details, emails ...
- Relatively small portion of security budget is spent on data centre security.

5 Excessive and unused privileges

- Privilege control mechanisms for job roles have often not been well defined or maintained
- People join the company, leave the company, change roles, their privileges often grow and aren't scaled back to be inline with their job requirements
- Probably the greatest chance of impact in organisations

6 Privilege Abuse

- People who have legitimate use of data, but choose to abuse it
- Employees often feel entitled to take data with them
  - They feel they were part of creating this data, therefore they will take it with them

7 SQL Injection

- Inserting or injecting unauthorised malicious database statements somewhere in the application or database that gets executed by the database itself
- Typing SQL commands to the database
- Can be fixed with prepared statements

8 Malware

- Organisations are quickly conpromised and then their data does out of the door within minutes or hours
- Common strategy:
  - Spear phishing
  - Malware
  - Credentials stolen
  - Data being stolen

9 Weak audit trail

- We get a much clearer picture of what's going on with more detail and resolution
- Most organisations don't record the details that you need to deal with the aftermath of these situations

10 Storage media exposure

- After spear phishing and malware, it's often the database backups that are actually leaked in the end
- Often something that's completely unprotected from an attack
- Shows up in the details of a variety of security breaches

11 Database Vulnerability Exploitation

- Companies rarely patch their servers

12 Unmanaged sensitive data

- You can easily end up with some of your sensitive data being used in testing environments, or R&D environments and not being managed properly

13 DoS

- Attackers overload server resources
- Flooding database with queries that cause server to crash

14 Limited expertise

- Majority of organisations experienced staff related breaches when policies weren't well understood
- Small businesses don't even have a position for educating their staff about security

15 Obscure Queries

- Hide your real query in a more complex query - harder for the system to identify the real query

16 Inference Attacks

- Data mining technique
  - Analyze data in order to illegitimately gain knowledge of subject or database
  - Sensitive information can be leaked if hacker can infer real value with high confidence
- Occur when someone is allowed to execute queries that they're authorized for, but by executing those queries they are able to gain access to information for which they are not authorized

17 Approach to database security

1. Discovery and assessment
   - You can't protect against problems if you don't know they exist
   - Quickly identify sensitive data and assessing vulnerabilities/misconfigurations
2. User rights management
   - Make sure you have thorough process to review and eliminate excessive user rights
3. Monitoring and blocking
   - Have procedures in place to monitor activity and block attempted policy violations
4. Auditing (creating a trail)
5. Protecting the data
   - Storage encryption, tamper-proof audit trail
6. Non-technical security
   - Raise awareness and cultivate experienced security professionals