Database Security

Zartasha Baloch

Agenda

- Data and Database Administration
- What is Database Security?
- Database Security Threats
- How Can You Secure Your Database Server?

Data administration and database administration

- Data Administrator (DA) and Database Administrator (DBA) are responsible for managing and controlling activities associated with corporate data and corporate database, respectively.

- DA is more concerned with early stages of lifecycle and DBA is more concerned with later stages.

Data administration

- Management and control of data resource, including:
  - Database planning
  - Development and maintenance of standards, policies, and procedures
  - Conceptual and Logical database design

Data administration tasks

- Selecting appropriate productivity tools
- Assisting in the development of the corporate IT/IS and business strategies
- Undertaking feasibility studies and planning for database development
- Developing a corporate data model
- Determining the organization's data requirements
- Setting data collection standards and establishing data formats
- Estimating volumes of data and likely growth
- Determining patterns and frequencies of data usage
- Determining data access requirements and safeguards for both legal and corporate requirements
- Undertaking logical database design
- Liaising with database administration staff and application developers to ensure applications meet all stated requirements
- Educating users on data standards and legal responsibilities
- Keeping up to date with IT/IS and business developments
- Ensuring documentation is complete, including the corporate data model, standards, policies, procedures, and controls on end-users
- Managing the data dictionary
- Liaising with end-users and database administration staff to determine new requirements and to resolve data access or performance problems
- Developing a security policy

Database administration

- Management and control of physical realization of a database system, including:
  - Physical database design and implementation
  - Setting security and integrity controls
  - Monitoring system performance
  - Reorganizing the database

Database administration tasks

Evaluating and selecting DBMS products

Undertaking physical database design

Implementing a physical database design using a target DBMS

Defining security and integrity constraints

Liaising with database system developers

Developing test strategies

Training users

Responsible for 'signing off' the implemented database system

Monitoring system performance and tuning the database, as appropriate

Performing backups routinely

Ensuring recovery mechanisms and procedures are in place

Ensuring documentation is complete, including in-house produced material

Keeping up to date with software and hardware developments and costs, and installing updates as necessary

Comparison of data and database administration

Data administration	Database administration
Involved in strategic IS planning	Evaluates new DBMSs
Determines long-term goals	Executes plans to achieve goals
Determines standards, policies, and procedures	Enforces standards, policies, and procedures
Determines data requirements	Implements data requirements
Develops logical database design	Develops physical database design
Develops and maintains corporate data model	Implements physical database design
Coordinates database development	Monitors and controls database use
Managerial orientation	Technical orientation
DBMS independent	DBMS dependent

What is Database Security?

Database security includes a variety of measures used to secure database management systems from malicious cyber-attacks and illegitimate use.

Database security programs are designed to protect not only the data within the database, but also the data management system itself, and every application that accesses it, from misuse, damage, and intrusion.

Database security encompasses tools, processes, and methodologies which establish security inside a database environment.

Database Security Threats

- Many software vulnerabilities, misconfigurations, or patterns of misuse or carelessness could result in breaches. Here are a number of the most known causes and types of database security cyber threats.
- Insider Threats
- An insider threat is a security risk from one of the following three sources, each of which has privileged means of entry to the database:
  - A malicious insider with ill-intent
  - A negligent person within the organization who exposes the database to attack through careless actions
  - An outsider who obtains credentials through social engineering or other methods, or gains access to the database's credentials
- An insider threat is one of the most typical causes of database security breaches and it often occurs because a lot of employees have been granted privileged user access.

Database Security Threats

- Human Error
- Weak passwords, password sharing, accidental erasure or corruption of data, and other undesirable user behaviors are still the cause of almost half of data breaches reported.
- Exploitation of Database Software Vulnerabilities
- Attackers constantly attempt to isolate and target vulnerabilities in software, and database management software is a highly valuable target.
- New vulnerabilities are discovered daily, and all open-source database management platforms and commercial database software vendors issue security patches regularly. However, if you don't use these patches quickly, your database might be exposed to attack.
- Even if you do apply patches on time, there is always the risk of zero-day attacks, when attackers discover a vulnerability, but it has not yet been discovered and patched by the database vendor.

Database Security Threats

- SQL/NoSQL Injection Attacks
- A database-specific threat involves the use of arbitrary non-SQL and SQL attack strings into database queries. Typically, these are queries created as an extension of web application forms or received via HTTP requests.
- Any database system is vulnerable to these attacks, if developers do not adhere to secure coding practices, and if the organization does not carry out regular vulnerability testing.

- Buffer Overflow Attacks
- Buffer overflow takes place when a process tries to write a large amount of data to a fixed-length block of memory, more than it is permitted to hold.
- Attackers might use the excess data, kept in adjacent memory addresses, as the starting point from which to launch attacks.

Database Security Threats

- Denial of Service (DoS/DDoS) Attacks
- In a denial of service (DoS) attack, the cybercriminal overwhelms the target service—in this instance the database server—using a large amount of fake requests. The result is that the server cannot carry out genuine requests from actual users, and often crashes or becomes unstable.
- In a distributed denial of service attack (DDoS), fake traffic is generated by many computers, participating in a botnet controlled by the attacker. This generates very large traffic volumes, which are difficult to stop without a highly scalable defensive architecture. Cloud-based DDoS protection services can scale up dynamically to address very large DDoS attacks.
- Malware
- Malware is software written to take advantage of vulnerabilities or to cause harm to a database. Malware could arrive through any endpoint device connected to the database's network. Malware protection is important on any endpoint, but especially so on database servers, because of their high value and sensitivity.

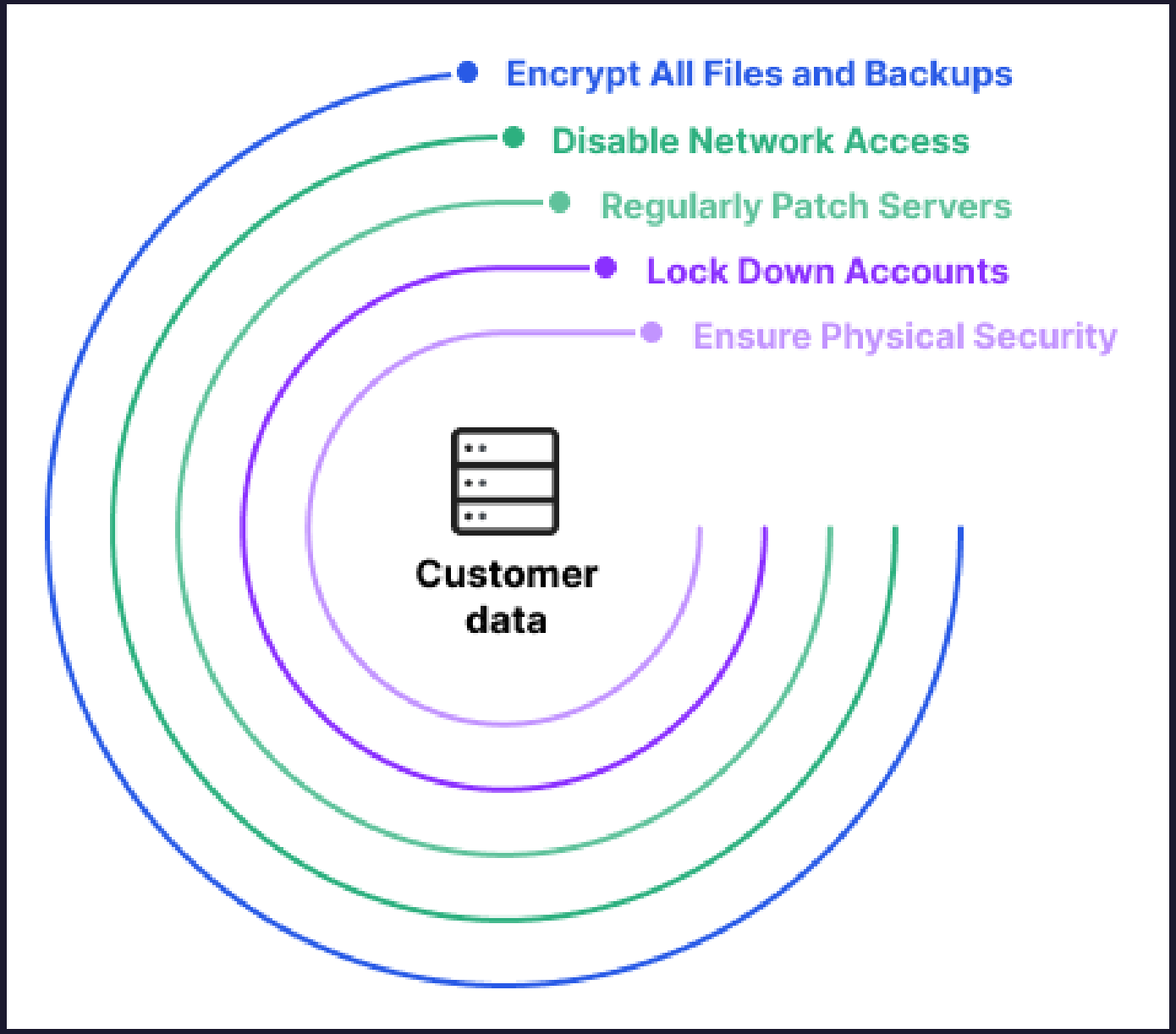
Database Security Threats

- An Evolving IT Environment
- The evolving IT environment is making databases more susceptible to threats. Here are trends that can lead to new types of attacks on databases, or may require new defensive measures:
- **Growing data volumes**—storage, data capture, and processing is growing exponentially across almost all organizations. Any data security practices, or tools must be highly scalable to address distant and near-future requirements.
- **Distributed infrastructure**—network environments are increasing in complexity, especially as businesses transfer workloads to hybrid cloud or multi-cloud architectures, making the deployment, management, and choice of security solutions more difficult.
- **Increasingly tight regulatory requirements**—the worldwide regulatory compliance landscape is growing in complexity, so following all mandates are becoming more challenging.
- **Cybersecurity skills shortage**—there is a global shortage of skilled cybersecurity professionals, and organizations are finding it difficult to fill security roles. This can make it more difficult to defend critical infrastructure, including databases.


How Can You Secure
Your Database Server?

A database server is a physical or virtual machine running the database.

Securing a database server, also known as “hardening”, is a process that includes physical security, network security, and secure operating system configuration.



Securing Database Server

- Ensure Physical Database Security
- Refrain from sharing a server for web applications and database applications, if your database contains sensitive data. Although it could be cheaper, and easier, to host your site and database together on a hosting provider, you are placing the security of your data in someone else's hands.
- If you do rely on a web hosting service to manage your database, you should ensure that it is a company with a strong security track record. It is best to stay clear of free hosting services due to the possible lack of security.
- If you manage your database in an on-premise data center, keep in mind that your data center is also prone to attacks from outsiders or insider threats. Ensure you have physical security measures, including locks, cameras, and security personnel in your physical facility. Any access to physical servers must be logged and only granted to authorized individuals.
- In addition, do not leave database backups in locations that are publicly accessible, such as temporary partitions, web folders, or unsecured cloud storage buckets.

Securing Database Server

- Lock Down Accounts and Privileges
- Let's consider the Oracle database server. After the database is installed, the Oracle database configuration assistant (DBCA) automatically expires and locks most of the default database user accounts.
- If you install an Oracle database manually, this doesn't happen, and default privileged accounts won't be expired or locked. Their password stays the same as their username, by default. An attacker will try to use these credentials first to connect to the database.
- It is critical to ensure that every privileged account on a database server is configured with a strong, unique password. If accounts are not needed, they should be expired and locked.
- For the remaining accounts, access must be limited to the absolute minimum required. Each account should only have access to the tables and operations (for example, SELECT or INSERT) required by the user. Avoid creating user accounts with access to every table in the database.

Securing Database Server

- Regularly Patch Database servers
- Ensure that patches remain current. Effective database patch management is a crucial security practice because attackers are actively seeking out new security flaws in databases, and new viruses and malware appear on a daily basis.
- A timely deployment of up-to-date versions of database service packs, critical security hotfixes, and cumulative updates will improve the stability of database performance.

Securing Database Server

- Disable Public Network Access
- Organizations store their applications in databases. In most real-world scenarios, the end-user doesn't require direct access to the database. Thus, you should block all public network access to database servers unless you are a hosting provider. Ideally, an organization should set up gateway servers (VPN or SSH tunnels) for remote administrators.

Securing Database Server

- Encrypt All Files and Backups
- Irrespective of how solid your defenses are, there is always a possibility that a hacker may infiltrate your system. Yet, attackers are not the only threat to the security of your database. Your employees may also pose a risk to your business. There is always the possibility that a malicious or careless insider will gain access to a file they don't have permission to access.
- Encrypting your data makes it unreadable to both attackers and employees. Without an encryption key, they cannot access it, this provides a last line of defense against unwelcome intrusions. Encrypt all-important application files, data files, and backups so that unauthorized users cannot read your critical data.

Securing Database Server

- Authorization
  - The granting of a right or privilege that enables a subject to have legitimate access to a database system or a database system's object.
- Authentication
  - A mechanism that determines whether a user is, who he or she claims to be.
- View
  - A view is a *virtual table* that does not necessarily exist in the database but can be produced upon request by a particular user, at the time of request.
- Backup
  - Process of periodically taking a copy of the database and log file (and possibly programs) onto offline storage media.
- Journaling
  - Process of keeping and maintaining a log file (or journal) of all changes made to database to enable recovery to be undertaken effectively in the event of failure.