DATABASE SECURITY CHECKLIST

Prepared by HANIM EKEN

https://ie.linkedin.com/in/hanimeken

It is a checklist for database security, which includes various aspects to consider when securing a database:

Authentication:

□ Implement strong authentication mechanisms.
□ Enforce password policies (complexity, expiration, etc.).
□ Use multi-factor authentication (MFA) for additional security.

Authorization and Access Control:

□ Define and enforce access control policies.
□ Assign roles and permissions based on the principle of least privilege.
□ Regularly review and update user access levels.

Encryption:

□ Encrypt data at rest using database-level encryption.
□ Encrypt data in transit using SSL/TLS.
□ Manage and protect encryption keys securely.

Audit Logging:

□ Enable and configure detailed audit logging.
□ Regularly review audit logs for suspicious activities.
□ Ensure logs are stored securely and retained for compliance.

Backup and Recovery:

□ Establish regular backup schedules.
□ Store backups securely, and test restoration processes.
□ Implement a disaster recovery plan.

Database Activity Monitoring:

□ Implement real-time monitoring of database activities.
□ Set up alerts for unusual or suspicious behavior.
□ Respond promptly to alerts and investigate incidents.

Data Masking and Redaction:

□ Apply data masking or redaction for sensitive information.
□ Ensure that only authorized users can access the complete dataset.

https://ie.linkedin.com/in/hanimeken

Vulnerability Management:

□ Regularly scan for vulnerabilities in the database.
□ Develop and implement a patch management process.
□ Address and remediate identified vulnerabilities promptly.

Database Encryption Key Management:

□ Establish a secure key management system.
□ Periodically rotate encryption keys.
□ Monitor and audit key access and usage.

Database Patch Management:

□ Regularly update and patch the database management system.
□ Follow a testing process before applying patches in a production environment.

User Training and Awareness:

□ Provide security training to database administrators and users.
□ Promote awareness of security best practices and potential risks.
□ Conduct periodic security training sessions.

Compliance Requirements:

□ Ensure compliance with relevant industry regulations (e.g., GDPR, HIPAA, PCI DSS).
□ Periodically review and update security measures to meet evolving compliance standards.

HANIM EKEN

https://ie.linkedin.com/in/hanimeken