Database Security Roadmap

A Best Practices Guide from Pivot Point Security

PivotPoint SECURITY SIMPLIFIED

www.pivotpointsecurity.com

Secure the Data

Evaluate User Rights (present impact)
- What database users have access to sensitive data?

Evaluate DB Object Grant Strategy (future impact)
- Are privileges granted directly to users which may result in unintended privileges in the future?

Evaluate DBA Segregation of Duties
- Do DBA account privileges adhere to the principle of least privilege?

Evaluate Data Encryption
- Is data stored in plain text or is it encrypted?
- What kind of encryption is used?
- Where are the keys stored and how are they secured?

Evaluate Resource Controls
- Are user resource controls in place (user disk & cpu quotas)?

Evaluate Stored Procedure/Function access and visibility
- Is sensitive stored procedure code encrypted?
- Is read or execute access to powerful stored procedures protected from inappropriate users?

Evaluate Access Controls – Password Policies
- Is a strong password policy enforced?
- Are proper limits on login failures enforced?
- Is a password expiration policy enforced?

Evaluate Controls Required by Applicable Regulations:
- e.g.,HIPAA, PCI, Sarbanes Oxley

Secure the Database Configuration

Evaluate DB Backup / BCP Strategy
- Are backups working as planned?
- How are backups transferred and secured?

Evaluate Software Patch Configuration
- Is database patched with latest security patches?

Evaluate Directory Structure and Security
- Are directories containing database control files and data files secured?

Evaluate Database Authentication
- Can an unauthorized user gain access to the database?

Evaluate Database Audit Policy
- What database activities are being audited?
- Are the audit logs monitored?

Evaluate SQLNet Configuration
- Is the SQLNET configuration password protected?
- Are log files set to minimum levels?
- Is EXTPROC removed from the sqlnet.ora configuration file?
- Is the listener port set to something other than default 1521?
- In a multi-tiered environment, are all servers blocked with the exception of the appropriate application and administration servers?

Secure Data Ingress/Egress

Evaluate Application Security
- Are applications using the database secured against OWASP Top 10 attacks?
- Are database credentials stored in scripts for internal "applications" that access the data?

Evaluate Interface Security
- Are interfaces and supporting systems/processes holistically secured?
- Are data feeds validated & provable?
- Are feeds encrypted?

Evaluate Reporting/BI Security
- Is direct SQL access to the databse appropriately restricted?
- Is access to business critical data monitored?
- How are user-generated reports stored/secured?

Evaluate Third Party Security
- Are security controls specified in third party agreements for data analytics/processing?
- Is security attestation required from third parties handling sensitive data?

Secure the Database Server

Evaluate Host Security
- Is there a comprehensive approach to patch, vulnerability and configuration management?
- Is privileged access to the host appropriately limited?
- Is access to the host logged? Are the logs monitored?
- Are key configuration files protected against modification?

Evaluate Segregation of Duty
- Do administrator login rights adhere to the principle of least privilege?
- Are all users using unique passwords?
- Are DBA, System Admin, and Security Admin roles segregated?

Secure the Network

Evaluate Network Security
- Are critical connections to the database environment secured in transit?
- Are the DBA workstations secure?

Evaluate Environment Segregation
- Are Dev, Staging, and Prod environments fully segregated?
- Is Prod data kept out of Dev and Staging environments?

Secure the Physical Environment

Evaluate Physical Security
- Are physical access controls in place to prevent unauthorized access to the data, systems, and networks the data resides on?
- Are physical/logical access controls in place for mobile devices?
- Are secure disposal controls in place for media/systems containing sensitive data?

Because data is only as secure as the systems & processes it relies on – a holistic approach to data security is essential. This roadmap is not meant to be exhaustive but rather to stimulate the necessary thought process to put you on the path to good data security. That's a benefit to you - and your customers! See our 27001 (and OWASP) roadmap for a comprehensive approach to building a robust Information Security Management System.