Australian Government
Australian Signals Directorate

Information Security Manual

Published: 21 September 2023

Guidelines for Database Systems

Database servers

Functional separation between database servers and web servers

Due to the higher threat environment that web servers are typically exposed to, hosting database servers and web servers within the same operating environment increases the likelihood of database servers being compromise by malicious actors. This security risk can be mitigated by ensuring that database servers are functionally separated from web servers.

Control: ISM-1269; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Database servers and web servers are functionally separated.

Communications between database servers and web servers

Data communicated between database servers and web servers, especially over the internet, is susceptible to capture by malicious actors. As such, it is important that all data communicated between database servers and web servers is encrypted.

Control: ISM-1277; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Data communicated between database servers and web servers is encrypted.

Network environment

Placing database servers on the same network segment as user workstations can increase the likelihood of database servers being compromise by malicious actors. Additionally, in cases where databases will only be accessed from their own database server, allowing remote access to the database server poses an unnecessary security risk.

Control: ISM-1270; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Database servers are placed on a different network segment to user workstations.

Control: ISM-1271; Revision: 2; Updated: Jan-20; Applicability: All; Essential Eight: N/A
Network access controls are implemented to restrict database server communications to strictly defined network resources, such as web servers, application servers and storage area networks.

Control: ISM-1272; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
If only local access to a database is required, networking functionality of database management system software is disabled or directed to listen solely to the localhost interface.

Separation of development, testing and production database servers

Using production database servers for development and testing activities could result in accidental damage to their integrity or contents.

Control: ISM-1273; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Development and testing environments do not use the same database servers as production environments.

Further information

Further information on the functional separation of computing environments can be found in the virtualisation hardening section of the *Guidelines for System Hardening*.

Further information on encrypting communications can be found in the cryptographic fundamentals section of the *Guidelines for Cryptography*.

Further information on network segmentation and segregation can be found in the network design and configuration section of the *Guidelines for Networking*.

Further information on database management system software can be found in the server application hardening section of the *Guidelines for System Hardening*.

Databases

Database register

Without knowledge of all the databases in an organisation, and their contents, an organisation will be unable to appropriately protect their assets. As such, it is important that a database register is developed, implemented, maintained and verified on a regular basis.

Control: ISM-1243; Revision: 6; Updated: Dec-22; Applicability: All; Essential Eight: N/A
A database register is developed, implemented, maintained and verified on a regular basis.

Protecting databases

Databases can be protected from unauthorised copying, and subsequent offline analysis, by applying file-based access controls to database files.

Control: ISM-1256; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A
File-based access controls are applied to database files.

Protecting database contents

Database administrators and database users should know the sensitivity or classification associated with databases and their contents. In cases where all of a database's contents are the same sensitivity or classification, an organisation should classify the entire database at this level and protect it as such. Alternatively, in cases where a database's contents are of varying sensitivities or classifications, and database users have varying levels of access to the database's contents, an organisation should protect the database's contents at a more granular level.

Restricting database users' ability to access, insert, modify or remove database contents, based on their work duties, ensures that the likelihood of unauthorised access, modification or deletion of database contents is reduced. Furthermore, where concerns exist that the aggregation of separate pieces of content from within a database could lead to malicious actors determining more sensitive or classified content, the need-to-know principle can be enforced through the use of minimum privileges, database views and database roles. Alternatively, the content of concern could be separated by implementing multiple databases, each with restricted data sets.

Control: ISM-0393; Revision: 8; Updated: Jun-21; Applicability: All; Essential Eight: N/A
Databases and their contents are classified based on the sensitivity or classification of data that they contain.

Control: ISM-1255; Revision: 4; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Database users' ability to access, insert, modify and remove database contents is restricted based on their work duties.

Control: ISM-1268; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A

The need-to-know principle is enforced for database contents through the application of minimum privileges, database views and database roles.

Separation of development, testing and production databases

Using database contents from production environments in development or testing environments could result in inadequate protection being applied to the database contents.

Control: ISM-1274; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Database contents from production environments are not used in development or testing environments unless the environment is secured to the same level as the production environment.

Web application interaction with databases

Structured Query Language (SQL) injection attacks, facilitated by the use of dynamically generated queries, are a significant threat to the confidentiality, integrity and availability of database contents. Specifically, SQL injection attacks can allow malicious actors to steal database contents, modify database contents, delete an entire database or even in some circumstances gain control of the underlying database server. Furthermore, when database queries from web applications fail they may display detailed error information about the structure of databases. This can be used by malicious actors to further tailor their SQL injection attacks.

Control: ISM-1275; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
All queries to databases from web applications are filtered for legitimate content and correct syntax.

Control: ISM-1276; Revision: 3; Updated: Mar-23; Applicability: All; Essential Eight: N/A
Parameterised queries or stored procedures, instead of dynamically generated queries, are used for database interactions.

Control: ISM-1278; Revision: 4; Updated: Mar-23; Applicability: All; Essential Eight: N/A
Web applications are designed or configured to provide as little error information as possible about the structure of databases.

Database event logging

Database events can assist in monitoring the security posture of databases, detecting malicious behaviour and contributing to investigations following cyber security incidents. To facilitate such activities, database event logs should be captured and stored centrally.

Control: ISM-1537; Revision: 3; Updated: Jun-22; Applicability: All; Essential Eight: N/A
The following events are logged for databases:

- *access or modification of particularly important content*
- *addition of new users, especially privileged users*
- *changes to user roles or privileges*
- *attempts to elevate user privileges*
- *queries containing comments*
- *queries containing multiple embedded queries*
- *database and query alerts or failures*
- *database structure changes*
- *database administrator actions*
- *use of executable commands*
- *database logons and logoffs.*

Control: ISM-1758; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: N/A
Database event logs are stored centrally.

Further information

Further information on event logging can be found in the event logging and monitoring section of the *Guidelines for System Monitoring*.