Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for Database Systems

Database servers

Protecting database server contents

Database server contents can be protected from unauthorised access (e.g. by the physical theft of a database server or failure to sanitise database server hardware before disposal) through the use of encryption.

Security Control: 1425; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Hard disks of database servers are encrypted using full disk encryption.

Functional separation between database servers and web servers

Placing databases used by web applications on the same physical server as a web server can expose them to an increased possibility of compromise by an adversary.

Security Control: 1269; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Database servers and web servers are functionally separated, physically or virtually.

Communications between database servers and web servers

Data communicated between database servers and web applications, especially over the internet, is susceptible to capture by an adversary.

Security Control: 1277; Revision: 3; Updated: Jun-21; Applicability: O, P, S, TS
Data communicated between database servers and web applications is encrypted.

Network environment

Placing database servers on the same network segment as an organisation's workstations and allowing them to communicate with other network resources exposes them to an increased possibility of compromise by an adversary. Alternatively, 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.

Security Control: 1270; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Database servers that require network connectivity are placed on a different network segment to an organisation's workstations.

Security Control: 1271; Revision: 2; Updated: Jan-20; Applicability: O, P, S, TS

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.

Security Control: 1272; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
If only local access to a database is required, networking functionality of database management system (DBMS) software is disabled or directed to listen solely to the localhost interface.

Separation of production, test and development database servers

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

Security Control: 1273; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Test and development environments do not use the same database servers as production environments.

Further information

Further information on developing Standard Operating Environments for database servers can be found in the operating system hardening section of the ***Guidelines for System Hardening***.

Further information on patching operating systems of database servers can be found in the system patching section of the ***Guidelines for System Management***.

Further information on using cryptography can be found in the ***Guidelines for Cryptography***.

Database management system software

Temporary installation files and logs

DBMS software will often leave behind temporary installation files and logs during the installation process, in case an administrator needs to troubleshoot a failed installation. These files, which can include passphrases in the clear, could be valuable to an adversary.

Security Control: 1245; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
All temporary installation files and logs are removed after DBMS software has been installed.

Hardening and configuration

Poorly configured DBMS software could provide an opportunity for an adversary to gain unauthorised access to database content. To assist organisations in deploying DBMS software, vendors often provide guidance on how to securely configure their DBMS software. Furthermore, DBMS software is often installed with most features enabled by default.

Security Control: 1246; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
DBMS software is configured according to vendor guidance.

Security Control: 1247; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
DBMS software features, stored procedures, accounts and databases that are not required are disabled or removed.

Restricting privileges

If DBMS software operating as a local administrator or root account is compromised by an adversary, it can present a significant security risk to the underlying operating system.

DBMS software is also often capable of accessing files that it has read access to on the database server. For example, an adversary using an SQL injection could use the command *LOAD DATA LOCAL INFILE 'etc/passwd' INTO TABLE Users or*

SELECT load_file("/etc/passwd") to access the contents of a Linux password file. Disabling the ability of the DBMS software to read local files from a server will prevent such SQL injection from succeeding. This could be performed, for example, by disabling use of the 'LOAD DATA LOCAL INFILE' command.

Security Control: 1249; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
DBMS software is configured to run as a separate account with the minimum privileges needed to perform its functions.

Security Control: 1250; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
The account under which DBMS software runs has limited access to non-essential areas of the database server's file system.

Security Control: 1251; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
The ability of DBMS software to read local files from a server is disabled.

Database administrator accounts

DBMS software often comes pre-configured with default database administrator accounts and passphrases that are listed in vendor documentation. These default database administrator accounts should be disabled, renamed or have their passphrases changed.

When sharing database administrator accounts for the performance of administrative tasks, any actions undertaken will not be attributable to an individual database administrator. This can hinder investigations relating to an attempted, or successful, targeted cyber intrusion. Furthermore, database administrator accounts shared across different databases can exacerbate any compromise of a database administrator account by an adversary.

When creating new database administrator accounts, the accounts are often allocated all privileges available to administrators. Most database administrators will only need a subset of all available privileges to undertake their authorised duties.

Security Control: 1260; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Default database administrator accounts are disabled, renamed or have their passphrases changed.

Security Control: 1262; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Database administrators have unique and identifiable accounts.

Security Control: 1261; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Database administrator accounts are not shared across different databases.

Security Control: 1263; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Database administrator accounts are used exclusively for administrative tasks, with standard database accounts used for general purpose interactions with databases.

Security Control: 1264; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Database administrator access is restricted to defined roles rather than accounts with default administrative permissions, or all permissions.

Further information

Further information on authenticating users can be found in the authentication hardening section of the ***Guidelines for System Hardening***.

Further information on patching DBMS software can be found in the system patching section of the ***Guidelines for System Management***.

Databases

Database register

Without knowledge of all the databases in an organisation, and the data they contain, an organisation will be unable to appropriately protect their assets.

Security Control: 1243; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS
A database register is maintained and regularly audited.

Protecting databases

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

Security Control: 1256; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
File-based access controls are applied to database files.

Protecting authentication credentials in databases

Storing authentication credentials such as usernames and passphrases as plaintext in databases poses a significant security risk. An adversary that manages to gain access to a database's contents could extract these authentication credentials to gain access to users' accounts. In addition, it is possible that a user could have reused a username and passphrase for their workstation posing an additional security risk.

Security Control: 1252; Revision: 3; Updated: Jun-19; Applicability: O, P, S, TS
Passphrases stored in databases are hashed with a uniquely salted Australian Signals Directorate Approved Cryptographic Algorithm.

Protecting database contents

Database administrators and database users should know the sensitivity or classification associated with a database and its contents to ensure that sufficient security controls are applied. In cases where all of a database's contents are the same sensitivity or classification an organisation may choose to classify the entire database at this level. Alternatively, in cases where a database's contents are of varying sensitivity or classification levels, and database users have differing levels of access to such data, an organisation may choose to apply classifications at a more granular level within the database.

Limiting database user's ability to access, insert, modify or remove content from databases based on their work duties ensures the need-to-know principle is applied and the likelihood of unauthorised modifications is reduced.

Security Control: 0393; Revision: 8; Updated: Jun-21; Applicability: O, P, S, TS
Databases and their contents are classified based on the sensitivity or classification of data that they contain.

Security Control: 1255; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Database users' ability to access, insert, modify and remove content in databases is restricted based on their work duties.

Security Control: 1268; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
The need-to-know principle is enforced for database contents through the application of minimum privileges, database views and database roles.

Aggregation of database contents

Where concerns exist that the sum, or aggregation, of separate pieces of data from within databases could lead to an adversary determining more sensitive or classified data, database views in combination with database user access roles should be implemented. Alternatively, the data of concern could be separated by implementing multiple databases, each with restricted data sets. If implemented properly, this will ensure an adversary cannot access the sum of data components leading to the aggregated data.

Security Control: 1258; Revision: 2; Updated: Jun-21; Applicability: O, P, S, TS
Where concerns exist that the sum, or aggregation, of separate pieces of data from within databases could lead to a database user determining more sensitive or classified data, database views in combination with database user access roles are implemented.

Separation of production, test and development databases

Using data from production databases in test or development databases could result in inadequate protection being applied to the data.

Security Control: 1274; Revision: 5; Updated: Jun-21; Applicability: O, P, S, TS
Data in production databases is not used in testing or development databases unless the testing or development environments are secured to the same level as the production environment.

Web application interaction with databases

SQL injection is a significant threat to the confidentiality, integrity and availability of database contents. SQL injections can allow an adversary to steal data from databases, 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 database schema to users of the web application. This can be used by an adversary to tailor SQL injection attempts.

Security Control: 1275; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
All queries to databases from web applications are filtered for legitimate content and correct syntax.

Security Control: 1276; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Parameterised queries or stored procedures are used for database interaction instead of dynamically generated queries.

Security Control: 1278; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Web applications are designed to provide as little error information as possible to users about database schemas.

Further information

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