



APP.4.3 Relationale Datenbanken

1. Beschreibung

1.1. Einleitung

Datenbanksysteme (DBS) sind ein oft genutztes Hilfsmittel, um IT-gestützt große Datensammlungen zu organisieren, zu erzeugen, zu verändern und zu verwalten. Ein DBS besteht aus dem so genannten Datenbankmanagementsystem (DBMS) und einer oder mehreren Datenbanken. Eine Datenbank ist eine Zusammenstellung von Daten samt ihrer Beschreibung (Metadaten), die dauerhaft im Datenbanksystem abgelegt werden. Da Datenbanksysteme oft eine zentrale Bedeutung in einer IT-Infrastruktur einnehmen, ergeben sich an sie wesentliche Sicherheitsanforderungen. Meist sind Kernprozesse einer Institution von den Informationen aus den Datenbanken abhängig. Dadurch ergeben sich entsprechende Verfügbarkeitsanforderungen. Zusätzlich bestehen oft hohe Anforderungen an die Vertraulichkeit und Integrität der in den Datenbanken gespeicherten Informationen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, relationale Datenbanksysteme sicher betreiben zu können sowie die Informationen, die in Datenbanken verarbeitet und gespeichert werden, angemessen zu schützen. Dazu werden Anforderungen beschrieben, mit denen sich Datenbanksysteme sicher planen, umsetzen und betreiben lassen und durch die Gefährdungen reduziert werden können.

1.3. Abgrenzung und Modellierung

Der Baustein APP.4.3 *Relationale Datenbanken* ist auf jedes relationale Datenbanksystem einmal anzuwenden.

In diesem Baustein werden Anforderungen an relationale Datenbanksysteme beschrieben. Sicherheitsanforderungen an nicht-relationale Datenbanksysteme sind nicht Gegenstand des vorliegenden Bausteins.

Um die Informationen in den Datenbanken durchgängig zu schützen, sollten bereits in der Anwendungsentwicklung Sicherheitsanforderungen an den Aufbau der Datenbanktabellen und den Zugriff auf die Datenbank beachtet werden. Anforderungen zu diesen Themen werden jedoch nicht in diesem Baustein aufgeführt.

Ebenso geht der Baustein nicht auf Gefährdungen und Anforderungen ein, die das Betriebssystem und die Hardware betreffen, auf denen das Datenbanksystem installiert ist. Aspekte dazu finden sich in den

entsprechenden betriebssystemspezifischen Bausteinen der Schicht *SYS IT-Systeme*, z. B. *SYS.1.3 Server unter Linux und Unix* oder *SYS.1.2.3 Windows Server*.

Relationale Datenbanksysteme sollten grundsätzlich im Rahmen der Bausteine *OPR.4 Identitäts- und Berechtigungsmanagement*, *OPS.1.1.3 Patch- und Änderungsmanagement*, *CON.3 Datensicherungskonzept*, *OPS.1.2.2 Archivierung*, *OPS.1.1.5 Protokollierung* sowie *OPS.1.1.2 Ordnungsgemäße IT-Administration* mit berücksichtigt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein *APP.4.3 Relationale Datenbanken* von besonderer Bedeutung.

2.1. Unzureichende Dimensionierung der Systemressourcen

Verfügt die Hardware eines Datenbanksystems nicht über genügend Systemressourcen, kann die Datenbank ganz ausfallen oder fehlerhaft arbeiten. Dadurch können beispielsweise Daten nicht gespeichert werden. Auch können zu Stoßzeiten die Ressourcen stark ausgelastet werden. Dadurch kann sich die Performance verschlechtern. Dies wiederum kann dazu führen, dass Anwendungen nicht oder nicht fehlerfrei ausgeführt werden.

2.2. Aktivierte Standard-Konten

Bei der Erstinstallation bzw. im Auslieferungszustand eines Datenbankmanagementsystems sind Standard-Konten (Konten der Benutzenden und Administrierenden) häufig nicht oder nur mit Passwörtern gesichert, die öffentlich bekannt sind. Dadurch kann es passieren, dass diese Konten missbräuchlich genutzt werden. Beispielsweise können sich Angreifende mit den öffentlich bekannten Anmeldedaten am Datenbankmanagementsystem als Benutzende oder sogar als Administrierende anmelden. Danach können sie die Konfiguration oder die gespeicherten Daten auslesen, manipulieren oder löschen.

2.3. Unverschlüsselte Datenbankanbindung

In der Standardkonfiguration verbinden sich viele Datenbankmanagementsysteme unverschlüsselt mit den Anwendungen. Wird zwischen Anwendungen und Datenbankmanagementsystem unverschlüsselt kommuniziert, können übertragene Daten und Zugangsinformationen mitgelesen oder auf dem Transportweg manipuliert werden.

2.4. Datenverlust in der Datenbank

Durch Hardware- oder Softwarefehler sowie durch menschliches Versagen können Daten in der Datenbank verloren gehen. Da in Datenbanken meist wichtige Informationen für Anwendungen gespeichert sind, können Dienste ausfallen oder ganze Produktionsprozesse stillstehen.

2.5. Integritätsverlust der gespeicherten Daten

Durch falsch konfigurierte Datenbanken, Softwarefehler oder manipulierte Daten kann die Integrität der Informationen in der Datenbank verletzt werden. Wird dies nicht oder erst spät bemerkt, können Kernprozesse der Institution stark beeinträchtigt werden. Werden beispielsweise die Integritätsbeziehungen (referenzielle Integrität) zwischen den Tabellen nicht korrekt definiert, kann dies dazu führen, dass die Daten in der Datenbank fehlerhaft sind. Wird dieser Fehler erst im

Produktivbetrieb oder gar nicht bemerkt, müssen nicht nur die inkonsistenten Daten aufwändig bereinigt und rekonstruiert werden. Es kann mit der Zeit auch ein großer Schaden entstanden sein, beispielsweise wenn es sich um kritische Daten, zum Beispiel steuerrelevante Daten, Rechnungsdaten oder gar um Steuerungsdaten für ganze Produktionssysteme handelt.

2.6. SQL-Injections

Eine häufige Angriffsmethode auf Datenbanksysteme sind SQL-Injections. Greift eine Anwendung auf die Daten einer SQL-Datenbank zu, so werden Befehle in Form von SQL-Anweisungen an das DBMS übermittelt. Werden Eingabedaten innerhalb der Anwendung unzureichend validiert, können Angreifende eigene SQL-Befehle in die Anwendung einschleusen, die dann mit der Berechtigung des Dienstkontos der Anwendung bearbeitet werden. Angreifende können so Daten lesen, manipulieren, löschen, neue Daten hinzufügen oder auch Systembefehle aufrufen. Obwohl SQL-Injections primär die Anwendungen im Frontend betreffen, wirken sie sich auch erheblich auf das Datenbanksystem selbst und die damit verbundene Infrastruktur aus.

2.7. Unsichere Konfiguration des Datenbankmanagementsystems

Häufig sind in der Standardkonfiguration des Datenbankmanagementsystems nicht benötigte Funktionen aktiviert, die es bei einem potenziellen Angriff erleichtern, Informationen aus der Datenbank auszulesen oder zu manipulieren. Beispielsweise können sich Angreifende aufgrund einer unveränderten Standardinstallation mit einer von der Institution nicht benutzten Programmierschnittstelle verbinden, um das DBMS zu administrieren, ohne sich dafür authentifizieren zu müssen. Dadurch können sie unerlaubt auf die Datenbanken der Institution zugreifen.

2.8. Malware und unsichere Datenbank-Skripte

Bei vielen Datenbankmanagementsystemen ist es möglich, bestimmte Aktionen über Skripte zu automatisieren, die im Kontext der Datenbank ausgeführt werden, z. B. mithilfe der Procedural Language/Structured Query Language (PL/SQL). Dazu gehören unter anderem auch sogenannte Datenbanktrigger. Werden diese jedoch von den Zuständigen ungeprüft benutzt, könnten die Datenbankskripte nicht den Anforderungen an die Softwareentwicklung der Institution genügen.

Ebenfalls können bei Angriffen Kernfunktionen einer Datenbank, wie z. B. Data Dictionary Tables manipuliert werden, beispielsweise mithilfe von Schadprogrammen oder Datenbank-Skripten. Diese Art von Angriffen ist nur schwer zu entdecken. Qualitätsmängel in diesen Skripten und Malware können sowohl die Vertraulichkeit als auch die Integrität und die Verfügbarkeit der in den Datenbanken abgelegten Daten gefährden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.4.3 *Relationale Datenbanken* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Entwickelnde

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.4.3.A1 Erstellung einer Sicherheitsrichtlinie für Datenbanksysteme (B)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für Datenbanksysteme erstellt werden. Darin MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie Datenbanksysteme sicher betrieben werden sollen. Die Richtlinie MUSS allen im Bereich Datenbanksysteme zuständigen Mitarbeitenden bekannt sein. Sie MUSS grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem oder der ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

APP.4.3.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.4.3.A3 Basishärtung des Datenbankmanagementsystems (B)

Das Datenbankmanagementsystem MUSS gehärtet werden. Hierfür MUSS eine Checkliste mit den durchzuführenden Schritten zusammengestellt und abgearbeitet werden. Passwörter DÜRFEN NICHT im Klartext gespeichert werden. Die Basishärtung MUSS regelmäßig überprüft und, falls erforderlich, angepasst werden.

APP.4.3.A4 Geregeltetes Anlegen neuer Datenbanken (B)

Neue Datenbanken MÜSSEN nach einem definierten Prozess angelegt werden. Wenn eine neue Datenbank angelegt wird, MÜSSEN Grundinformationen zur Datenbank nachvollziehbar dokumentiert werden.

APP.4.3.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.4.3.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.4.3.A7 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.4.3.A8 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.4.3.A9 Datensicherung eines Datenbanksystems (B)

Es MÜSSEN regelmäßig Systemsicherungen des DBMS und der Daten durchgeführt werden. Auch bevor eine Datenbank neu erzeugt wird, MUSS das Datenbanksystem gesichert werden. Hierfür SOLLTEN die dafür zulässigen Dienstprogramme benutzt werden.

Alle Transaktionen SOLLTEN so gesichert werden, dass sie jederzeit wiederherstellbar sind. Wenn die Datensicherung die verfügbaren Kapazitäten übersteigt, SOLLTE ein erweitertes Konzept erstellt

werden, um die Datenbank zu sichern, z. B. eine inkrementelle Sicherung. Abhängig vom Schutzbedarf der Daten SOLLTEN die Wiederherstellungsparameter vorgegeben werden (siehe CON.3 *Datensicherungskonzept*).

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.4.3.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.4.3.A11 Ausreichende Dimensionierung der Hardware (S)

[Fachverantwortliche]

Datenbankmanagementsysteme SOLLTEN auf ausreichend dimensionierter Hardware installiert werden. Die Hardware SOLLTE über genügend Reserven verfügen, um auch eventuell steigenden Anforderungen gerecht zu werden. Zeichnen sich trotzdem während des Betriebs Ressourcenengpässe ab, SOLLTEN diese frühzeitig behoben werden. Wenn die Hardware dimensioniert wird, SOLLTE das erwartete Wachstum für den geplanten Einsatzzeitraum berücksichtigt werden.

APP.4.3.A12 Einheitlicher Konfigurationsstandard von Datenbankmanagementsystemen (S)

Für alle eingesetzten Datenbankmanagementsysteme SOLLTE ein einheitlicher Konfigurationsstandard definiert werden. Alle Datenbankmanagementsysteme SOLLTEN nach diesem Standard konfiguriert und einheitlich betrieben werden. Falls es bei einer Installation notwendig ist, vom Konfigurationsstandard abzuweichen, SOLLTEN alle Schritte von dem oder der ISB freigegeben und nachvollziehbar dokumentiert werden. Der Konfigurationsstandard SOLLTE regelmäßig überprüft und, falls erforderlich, angepasst werden.

APP.4.3.A13 Restriktive Handhabung von Datenbank-Links (S)

Es SOLLTE sichergestellt sein, dass nur Zuständige dazu berechtigt sind, Datenbank-Links (DB-Links) anzulegen. Werden solche Links angelegt, MÜSSEN so genannte Private DB-Links vor Public DB-Links bevorzugt angelegt werden. Alle von den Zuständigen angelegten DB-Links SOLLTEN dokumentiert und regelmäßig überprüft werden. Zudem SOLLTEN DB-Links mitberücksichtigt werden, wenn das Datenbanksystem gesichert wird (siehe APP.4.3.A9 *Datensicherung eines Datenbanksystems*).

APP.4.3.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.4.3.A15 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.4.3.A16 Verschlüsselung der Datenbankanbindung (S)

Das Datenbankmanagementsystem SOLLTE so konfiguriert werden, dass Datenbankverbindungen immer verschlüsselt werden. Die dazu eingesetzten kryptografischen Verfahren und Protokolle SOLLTEN den internen Vorgaben der Institution entsprechen (siehe CON.1 *Kryptokonzept*).

APP.4.3.A17 Datenübernahme oder Migration (S) [Fachverantwortliche]

Es SOLLTE vorab definiert werden, wie initial oder regelmäßig Daten in eine Datenbank übernommen werden sollen. Nachdem Daten übernommen wurden, SOLLTE geprüft werden, ob sie vollständig und unverändert sind.

APP.4.3.A18 Überwachung des Datenbankmanagementsystems (S)

Die für den sicheren Betrieb kritischen Parameter, Ereignisse und Betriebszustände des Datenbankmanagementsystems SOLLTEN definiert werden. Diese SOLLTEN mithilfe eines Monitoring-Systems überwacht werden. Für alle kritischen Parameter, Ereignisse und Betriebszustände SOLLTEN Schwellwerte festgelegt werden. Wenn diese Werte überschritten werden, MUSS geeignet reagiert werden. Hierbei SOLLTEN die zuständigen Mitarbeitenden alarmiert werden. Anwendungsspezifische Parameter, Ereignisse, Betriebszustände und deren Schwellwerte SOLLTEN mit den Zuständigen für die Fachanwendungen abgestimmt werden.

APP.4.3.A19 Schutz vor schädlichen Datenbank-Skripten (S) [Entwickelnde]

Werden Datenbank-Skripte entwickelt, SOLLTEN dafür verpflichtende Qualitätskriterien definiert werden (siehe CON.8 *Software-Entwicklung*). Datenbank-Skripte SOLLTEN ausführlichen Funktionstests auf gesonderten Testsystemen unterzogen werden, bevor sie produktiv eingesetzt werden. Die Ergebnisse SOLLTEN dokumentiert werden.

APP.4.3.A20 Regelmäßige Audits (S)

Bei allen Komponenten des Datenbanksystems SOLLTE regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und diese korrekt konfiguriert sind. Dabei SOLLTE geprüft werden, ob der dokumentierte Stand dem Ist-Zustand entspricht und ob die Konfiguration des Datenbankmanagementsystems der dokumentierten Standardkonfiguration entspricht. Zudem SOLLTE geprüft werden, ob alle Datenbank-Skripte benötigt werden. Auch SOLLTE geprüft werden, ob sie dem Qualitätsstandard der Institution genügen. Zusätzlich SOLLTEN die Protokolldateien des Datenbanksystems und des Betriebssystems nach Auffälligkeiten untersucht werden (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen*). Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert sein. Sie SOLLTEN mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.4.3.A21 Einsatz von Datenbank Security Tools (H)

Es SOLLTEN Informationssicherheitsprodukte für Datenbanken eingesetzt werden. Die eingesetzten Produkte SOLLTEN folgende Funktionen bereitstellen:

- Erstellung einer Übersicht über alle Datenbanksysteme,
- erweiterte Konfigurationsmöglichkeiten und Rechtemanagement der Datenbanken,
- Erkennung und Unterbindung von möglichen Angriffen (z. B. Brute Force Angriffe auf Konten, SQL-Injection) und
- Auditfunktionen (z. B. Überprüfung von Konfigurationsvorgaben).

APP.4.3.A22 Notfallvorsorge (H)

Für das Datenbankmanagementsystem SOLLTE ein Notfallplan erstellt werden, der festlegt, wie ein Notbetrieb realisiert werden kann. Die für den Notfallplan notwendigen Ressourcen SOLLTEN ermittelt werden. Zusätzlich SOLLTE der Notfallplan definieren, wie aus dem Notbetrieb der Regelbetrieb wiederhergestellt werden kann. Der Notfallplan SOLLTE die nötigen Meldewege, Reaktionswege, Ressourcen und Reaktionszeiten der Fachverantwortlichen festlegen. Auf Basis eines Koordinationsplans zum Wiederanlauf SOLLTEN alle von der Datenbank abhängigen IT-Systeme vorab ermittelt und berücksichtigt werden.

APP.4.3.A23 Archivierung (H)

Ist es erforderlich, Daten eines Datenbanksystems zu archivieren, SOLLTE ein entsprechendes Archivierungskonzept erstellt werden. Es SOLLTE sichergestellt sein, dass die Datenbestände zu einem späteren Zeitpunkt wieder vollständig und konsistent verfügbar sind.

Im Archivierungskonzept SOLLTEN sowohl die Intervalle der Archivierung als auch die Vorhaltefristen der archivierten Daten festgelegt werden. Zusätzlich SOLLTE dokumentiert werden, mit welcher Technik die Datenbanken archiviert wurden. Mit den archivierten Daten SOLLTEN regelmäßig Wiederherstellungstests durchgeführt werden. Die Ergebnisse SOLLTEN dokumentiert werden.

APP.4.3.A24 Datenverschlüsselung in der Datenbank (H)

Die Daten in den Datenbanken SOLLTEN verschlüsselt werden. Dabei SOLLTEN vorher unter anderem folgende Faktoren betrachtet werden:

- Einfluss auf die Performance,
- Schlüsselverwaltungsprozesse und -verfahren, einschließlich separater Schlüsselaufbewahrung und -sicherung,
- Einfluss auf Backup-Recovery-Konzepte,
- funktionale Auswirkungen auf die Datenbank, beispielsweise Sortiermöglichkeiten.

APP.4.3.A25 Sicherheitsprüfungen von Datenbanksystemen (H)

Datenbanksysteme SOLLTEN regelmäßig mithilfe von Sicherheitsprüfungen kontrolliert werden. Bei den Sicherheitsprüfungen SOLLTEN die systemischen und spezifischen Aspekte des herstellenden Unternehmens der eingesetzten Datenbank-Infrastruktur (z. B. Verzeichnisdienste) sowie des eingesetzten Datenbankmanagementsystems betrachtet werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat im Rahmen der Allianz für Cybersicherheit zum Themenfeld Datenbanksicherheit folgende Partnerbeiträge veröffentlicht:

- Oracle: Datenbank-Sicherheit - Grundüberlegungen
- McAfee: Datenbanksicherheit in Virtualisierungs- und Cloud-Computing-Umgebungen

Die Deutsche Telekom Gruppe hat im Rahmen ihres Privacy and Security Assessment Verfahrens (PSA-Verfahren) das Dokument „Sicherheitsanforderung Datenbanksysteme“ zum Themenfeld Datenbanken veröffentlicht.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel BA2.3 Protection of Databases Vorgaben für die Absicherung von relationalen Datenbanksystemen.