

Sicherheitsanforderung

Microsoft SQL Server

Deutsche Telekom Gruppe

Version	8.0
Datum	01.12.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.30	Dokumententyp Sicherheitsanforderung
Version 8.0	Stand 01.12.2025	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.12.2025 - 30.11.2030	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung
Microsoft SQL Server

Copyright © 2025 by Deutsche Telekom AG.

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Inhaltsverzeichnis

1.	Einleitung	4
2.	Grundlegende Sicherheitsanforderungen für Microsoft SQL Server	5
3.	Härtung des Datenbanksystems	6
3.1.	Benutzer und Rollen	6
3.2.	Least Privilege-Prinzip	7
3.3.	SQL-Funktionen und Pakete	11
4.	Datenkommunikation	13
5.	Missbrauchserkennung und -verhinderung	14
6.	MS SQL-spezifische Anforderungen	23

1. Einleitung

Dieses Dokument wurde auf Basis der Vorgaben aus den im Konzern gültigen Sicherheitsrichtlinien erstellt. Die Sicherheitsanforderung dient u.a. als Grundlage zur Freigabe im PSA-Prozess. Sie dient darüber hinaus als Umsetzungsempfehlung für Einheiten, die nicht am PSA-Verfahren teilnehmen. Diese Anforderungen müssen bereits während der Planungs- und Entscheidungsprozesse berücksichtigt werden. Bei der Umsetzung der Sicherheitsanforderung ist das jeweils vorrangige nationale, internationale und supranationale Recht zu beachten.

2. Grundlegende Sicherheitsanforderungen für Microsoft SQL Server

Die nachfolgenden Kapitel beschreiben die speziell für MS SQL Server geltenden Sicherheitsanforderungen.

Req 1	Die Version des MS SQL Servers muss für den produktiven Betrieb lizenzierbar sein.
-------	--

Umsetzungsbeispiel: Mit Hilfe des folgenden Befehls kann der Administrator im MS SQL Server Management Studio feststellen, welche Edition installiert ist:

```
SELECT SERVERPROPERTY ('edition');
```

ID: 3.30-1/8.0

Req 2	Die SQL Server Version muss derart in Support befinden, daß Security Patches bereitgestellt werden.
-------	---

Motivation: Nur für SQL Server Versionen in Mainstream- oder Extended Support werden Security patches bereitgestellt.

ID: 3.30-2/8.0

3. Härtung des Datenbanksystems

Dieses Kapitel enthält die Anforderungen zur Härtung des Datenbanksystems. Die Maßnahmen sind vergleichbar mit denen einer Betriebssystemhärtung und vermindern die Folgen eines Angriffes auf Datenbanksysteme.

3.1. Benutzer und Rollen

Req 3 Das Standard-DB-Administratorkonto (sa) muss deaktiviert werden.

Motivation: Eine Fülle automatisierter Schad-Software (etwa Würmer) versucht, das Default-Administratorkonto (sa) über Brute Force-Angriffe zu kompromittieren, um unbefugten Zugriff auf die Datenbank zu erlangen. Die Deaktivieren des Accounts ist eine einfache, aber wirkungsvolle Präventionsmaßnahme gegen automatisierte Angriffe.

ID: 3.30-3/8.0

Req 4 Built-in Windows Konten oder Gruppen dürfen kein SQL-Login sein.

Motivation: Es wird empfohlen, eine AD Gruppe mit administrativen Rechten ausschließlich für DBA Accounts zu erstellen, statt BUILTIN\Administrators zu nutzen. Bei 'BUILT IN'-haben oft viele Mitglieder und widerlaufen damit den best practices, nur bei Bedarf Rechte zu vergeben.

Umsetzungsbeispiel: Die Gruppe lässt sich durch Ausführen des folgenden Stored Procedures aus der Rolle „sysadmin“ löschen:

```
EXEC sp_dropsvrolemember 'BUILTIN\Administrators' , 'sysadmin';  
GO;
```

ID: 3.30-4/8.0

Req 5 Bei den lokalen Windows Gruppen darf es sich nicht um SQL-Anmeldungen handeln.

Motivation: Es empfiehlt sich, keine Nutzung von anwendungsdefinierten lokalen Windows Gruppen zuzulassen (mit Ausnahme derjenigen, die durch die Installation von Microsoft SQL Server erstellt werden, um SQL-Dienste mit den entsprechenden Berechtigungen bereitzustellen, wie SQLServer2005MSSQLUser\$ComputerName\$InstanceName). Die Zulassung von lokalen Windows Gruppen als SQL-Anmeldungen eröffnet eine Schwachstelle, über die jede Person mit Administratorrechten auf Betriebssystemebene (und ohne SQL Server Rechte) den lokalen Windows Gruppen Benutzer hinzufügen und sich damit selbst oder anderen Zugriff auf die SQL Server Instanz verschaffen könnte.

ID: 3.30-5/8.0

Req 6 Gastbenutzer dürfen keinen Zugriff auf Applikationsdatenbanken erhalten.

Motivation: Nur bekannte Benutzer dürfen auf die Datenbanken zugreifen. Demgegenüber ist sind Gastbenutzer explizit für unbekannte Nutzer gedacht.

Umsetzungsbeispiel:

```
REVOKE CONNECT FROM GUEST;
```

ID: 3.30-6/8.0

Req 7 Installierte Beispieldatenbanken müssen aus der SQL Server Installation entfernt werden.

Bekannte „Beispieldatenbanken“ (pubs, Northwind bzw. jede AdventureWorks-Datenbank) dürfen nicht auf Produktionssystemen installiert sein und sind bei Vorfinden zu entfernen.

ID: 3.30-7/8.0

Req 8	Wird mit der Eigenschaft „Trustworthy“ gearbeitet, darf der Datenbankbesitzer einer nicht zum System gehörenden Trustworthy-Datenbank nicht die Rolle „sysadmin“ ausüben.
-------	---

Die Datenbankeigenschaft TRUSTWORTHY ist für Benutzerdatenbanken standardmäßig deaktiviert (OFF).

Referenz:

<http://blogs.msdn.com/b/sqlsecurity/archive/2007/12/03/the-trustworthy-bit-database-property-in-sql-server-2005.aspx>

ID: 3.30-8/8.0

3.2. Least Privilege-Prinzip

Req 9	Der MS SQL Server darf nicht auf einem Domain-Controller eingerichtet werden.
-------	---

Motivation: Dies ist eine Herstellerempfehlung von Microsoft.

ID: 3.30-9/8.0

Req 10	Die Berechtigungen von Benutzern und Anwendungen müssen auf den zur Erfüllung ihrer Aufgaben benötigten Umfang beschränkt werden.
--------	---

Die Berechtigungen auf einem System müssen so weit eingeschränkt werden, dass ein Benutzer nur auf Daten zugreifen und Funktionen nutzen kann, die er im Rahmen seiner Arbeit benötigt. Entsprechende Berechtigungen sind auch für den Zugriff auf Dateien zu vergeben, die Bestandteil des Betriebssystems oder von Anwendungen sind oder von diesen erzeugt werden (z. B. Konfigurations- und Protokollierungsdateien).

Neben dem Zugriff auf Daten muss auch die Ausführung von Anwendungen und deren Bestandteilen mit möglichst niedrigen Berechtigungen erfolgen. Anwendungen sollten nicht mit Administrator- oder Systemberechtigungen ausgeführt werden.

Motivation: Werden einem Benutzer zu weitreichende Berechtigungen auf einem System gewährt, kann er in einem Umfang auf Daten und Anwendungen zugreifen, der zur Erfüllung der zugewiesenen Aufgaben nicht erforderlich ist. Dies erzeugt ein unnötig erhöhtes Risiko im Falle eines Missbrauchs, insbesondere auch, falls der Benutzer oder dessen Benutzerkonto durch einen Angreifer kompromittiert werden.

Anwendungen, die über zu weitreichende Berechtigungen verfügen, können von einem Angreifer missbraucht werden, um unbefugte Zugänge zu erhalten oder zu erweitern und damit einen Zugriff auf schutzbedürftige Daten und Systembereiche zu erlangen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-23/9.0

Req 11	Das MSSQL Dienstkonto muss ein Windows Domänenkonto, MSA oder virtuelles Konto sein.
--------	--

Motivation: Jeder zusätzliche Dienst mit unnötigen Rechten erhöht das Angriffsrisiko und die Schadenshöhe.

ID: 3.30-11/8.0

Req 12	Das SQLAgent Dienstkonto muss ein Windows Domänenkonto, MSA oder virtuelles Konto sein.
--------	---

Motivation: Jeder zusätzliche Dienst mit unnötigen Rechten erhöht das Angriffsrisiko und die Schadenshöhe.

Req 13	Das SQLFullText Dienstkonto muss sich vom MSSQL Dienstkonto unterscheiden.
--------	--

Referenz:

http://msdn.microsoft.com/en-us/library/ms143504.aspx#Use_startup_accounts

ID: 3.30-13/8.0

Req 14	Der MS SQL Service Account darf kein Windows Administrator sein.
--------	--

Motivation: Die Begrenzung der Accountrechte reduziert die Gefahr einer Systemkompromittierung.

ID: 3.30-14/8.0

Req 15	Der SQLAgent Service Account darf kein Windows Adminstrator sein.
--------	---

Motivation: Die Begrenzung der Accountrechte reduziert die Gefahr einer Systemkompromittierung.

ID: 3.30-15/8.0

Req 16	Der SQL Full-Text Service Account darf kein Windows Adminstrator sein.
--------	--

Motivation: Die Begrenzung der Accountrechte reduziert die Gefahr einer Systemkompromittierung.

ID: 3.30-16/8.0

Req 17	Die Rolle PUBLIC in der Datenbank „msdb“ darf keinen Zugriff auf SQL Agent Proxies erhalten.
--------	--

Motivation: Dies würde es allen Benutzern erlauben, den Proxy anzuwenden, der möglicherweise über weitreichende Privilegien verfügt.

ID: 3.30-17/8.0

Req 18	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss nach spätestens 12 Monaten ein Passwort-Wechsel erfolgen.
--------	---

Die maximal zulässige Nutzungsdauer für Passwörter beträgt 12 Monate.
Erreicht ein Passwort die maximal zulässige Nutzungsdauer, muss es geändert werden.

Das System muss hierzu den Benutzer automatisch bei dessen nächster Systemanmeldung auf die abgelaufene Nutzungsdauer hinweisen und ihn unmittelbar durch einen Passwort-Änderungsdialog führen. Der Zugriff auf das System darf ohne eine erfolgreich abgeschlossene Passwort-Änderung nicht weiter zugelassen werden.

Für technische Benutzerkonten (M2M bzw. Machine-2-Machine), die für die Authentifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt werden, müssen ebenfalls automatisierte Lösungen zur Einhaltung der zulässigen Nutzungsdauer für Passwörter implementiert werden.

Falls eine automatisierte Abbildung des Prozesses zur Passwort-Änderung nicht umsetzbar ist, muss ersatzweise eine wirksame organisatorische Maßnahme angewendet werden, die eine verbindliche manuelle Passwort-Änderung bei Ablauf der zulässigen Nutzungsdauer sicherstellt.

Motivation: Passwörter sind im Gegensatz zu moderneren Authentisierungsmerkmalen leichter angreifbar. Ohne spezifische Maßnahmen einer verlässlichen technisch automatisierten Kompromittierungserkennung kann das Risiko, dass ein Passwort von einem Angreifer ermittelt oder gebrochen wird, über die Zeit deutlich steigen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-30/9.0

Req 19	Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss deren Speicherung unter Einsatz eines für diesen Zweck als ausreichend sicher anerkannten "Password Hashing"-Verfahrens erfolgen, um Offline-Angriffe wie Wörterbuch- und Brute-Force-Attacken stark zu erschweren.
--------	---

Diese Anforderung bezieht sich auf die Speicherung von Passwörtern in sämtlichen Arten von Benutzerdatenbanken, die im vorliegenden System eingesetzt werden, um darüber eingehende Zugriffe (lokal oder aus der Ferne) von Benutzern oder anderen Systemen zu authentisieren.

Gelingt es einem Angreifer, die Kopie einer Benutzerdatenbank des Systems in seinen Besitz zu bringen, kann er diese in einer unabhängigen Umgebung einem automatisierten Wörterbuch- oder Brute-Force-Angriff aussetzen, um enthaltene Passwörter zu ermitteln. Durch Einsatz spezialisierter Werkzeuge in Kombination mit hoher Rechenleistung können bei unzureichenden Schutzmaßnahmen hierbei hohe Erkennungsraten in verhältnismäßig kurzer Zeit erreicht werden. Aufgrund der Unabhängigkeit vom Quellsystem bleibt ein solcher Offline-Angriff auf eine Benutzerdatenbank zudem unbemerkt.

Folgende Maßnahme ist umzusetzen, da diese den größtmöglichen Schutz bei Offline-Angriffen gewährleistet:

- Passwörter müssen unter Verwendung einer für diesen Zweck anerkannt wirksamen, zum aktuellen Stand der Technik als sicher eingestuft, kryptografischen Einwegfunktion gespeichert werden (bekannt als "Password-Hashing" Verfahren)

Hinweis: Zulässige Passwort-Hashing-Verfahren sind im Sicherheitsanforderungsdokument "3.50 / Kryptographische Algorithmen und Sicherheitsprotokolle" beschrieben.

In expliziter Deutlichkeit ist als NICHT ZULÄSSIG hervorzuheben:

- jegliche Speicherung von Passwörtern im Klartext
- jegliche Speicherung von Passwörtern in direkt rückrechenbaren Formaten
- jegliche Speicherung von Passwörtern mittels umkehrbarer Verschlüsselung

Hinweis:

"direkt rückrechenbare Formate" bezieht sich in diesem Kontext auf Formate, die ein Passwort lediglich kodieren, also ohne Einbeziehung eines geheimen Schlüssels transformieren. Da ein Passwort bei Anwendung eines solchen Formats nicht mehr in seinem originalen Klartext lesbar bleibt, werden diese Formate leicht als Schutzmaßnahme missverstanden. Effektiv bieten sie jedoch keinen Schutz, da die dahinterliegende Kodierung fest definiert ist und von einem Angreifer sehr leicht für die Rückrechnung der Inhalte in den ursprünglichen Klartext genutzt werden kann.

Beispiele für direkt rückrechenbare Formate sind: "base64", "rot13"

"Umkehrbar" sind alle Verfahren der Verschlüsselung, die unter Verwendung des passenden Schlüssels ermöglichen, einen verschlüsselten Inhalt zurück in den originalen Inhalt zu transformieren. Entsprechend stellt sich bei umkehrbarer Verschlüsselung stets die Herausforderung, den Schlüssel sicher aufzubewahren und vor unberechtigtem Zugriff zu schützen. Die Umkehrbarkeit ist auf vielen Einsatzgebieten der Verschlüsselung, z. B. für den Transport von vertraulichen Nachrichten, eine benötigte Grundeigenschaft, für das Speichern von Passwörtern jedoch kontraproduktiv: ein gespeichertes Passwort muss zwar mittels technischer Methoden vergleichbar bleiben, aber darf nicht mehr in seinen Klartext rückwandelbar sein, um es vor unberechtigter Einsicht bestmöglich zu schützen.

Beispiele für umkehrbare Verschlüsselung sind: "AES", "CHACHA20", "3DES", "RSA"

Motivation: Ohne entsprechenden Schutz kann ein Angreifer im Besitz der Benutzerdatenbank durch bloßes Durchprobieren von Wörterbuchlisten oder automatisch erzeugten Zeichenkombinationen versuchen, massenhaft Passwörter zu ermitteln, um so entsprechende Benutzerkonten missbräuchlich zu nutzen. Passwörter, die im Klartext oder direkt rückrechenbaren Formaten gespeichert werden, sind bei einem Offline-Angriff vollkommen schutzlos.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.01-24/9.0

Req 20	Falls Passwörter als Authentisierungsmerkmal genutzt werden, müssen diese mindestens 12 Zeichen lang sein und drei der folgenden Zeichenkategorien beinhalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.
--------	--

Ein System darf nur Passwörter akzeptieren, welche die folgende Komplexität erfüllen:

- Mindestlänge 12 Zeichen
- Bestehend aus mindestens drei der folgenden vier Zeichenkategorien:
 - Kleinbuchstaben
 - Großbuchstaben
 - Ziffern
 - Sonderzeichen

Die maximal mögliche Länge für Passwörter sollte 25 Zeichen oder mehr betragen. Dies unterstützt Endbenutzer bei Bedarf mit mehr Freiraum, um individuelle merkbare Passwörter bilden zu können, und hilft so, unerwünschte Verhaltensweisen im Umgang mit Passwörtern zu vermeiden, welche durch stark eingeschränkte maximale Passwortlängen provoziert werden können.

Das System muss bei der Vergabe eines Passwortes sicherstellen, dass das Passwort diesen Bildungsregeln entspricht; vorzugsweise mittels technischer Maßnahmen, falls solche aber nicht umsetzbar sein sollten, ersatzweise mittels organisatorischer Maßnahmen.

Bei Verwendung eines zentralen Systems für die Authentisierung der Benutzer [vgl. Wurzel-Anforderungsdokument "[i]3.69 IAM (Identity Access Management) - Framework"] darf diese Aufgabe an das zentrale System weitergereicht bzw. dorthin ausgelagert werden.

Zulässige Abweichung in der Passwort-Mindestlänge

Unter sicherheitsbezogenen Kriterien lassen sich für ein System potenziell Bedingungen identifizieren, die eine Reduzierung der Passwort-Mindestlänge ermöglichen:

- Allgemein zulässig ist eine Reduzierung der Passwort-Mindestlänge für Systeme, die innerhalb des Authentisierungsprozess zusätzlich zum Passwort weitere unabhängige Authentisierungsmerkmale verwenden (Umsetzung von 2-Faktor oder Multi-Faktor Authentisierung).
- Eine Reduzierung der Passwort-Mindestlänge muss grundsätzlich durch einen fachlichen Sicherheitsberater (z. B. ein PSM der Telekom Security) individuell bewertet und als zulässig bestätigt werden. In der Bewertung müssen umgebende technische, organisatorische und gesetzliche Rahmenparameter berücksichtigt sowie der systemspezifische Schutzbedarf und die potenzielle Schadenshöhe bei Sicherheitsvorfällen einbezogen werden.
- Der absolute Mindestwert von 8 Zeichen Länge darf für Passwörter grundsätzlich nicht unterschritten werden.

Motivation: Passwörter mit der genannten Komplexität bieten eine zeitgemäße Robustheit gegen Angriffe bei gleichzeitig akzeptabler Benutzerfreundlichkeit. In der Praxis haben sich Passwörter mit dieser Komplexität bewährt. Triviale und zu kurze Passwörter sind anfällig für Brute-Force- und Wörterbuch-Angriffe und von einem Angreifer leicht zu ermitteln. Ein ermitteltes Passwort kann dann von einem Angreifer für den unautorisierten Zugriff auf das System und dessen Daten genutzt werden

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-26/9.0

Req 21	Falls Passwörter als Authentisierungsmerkmal für technische Benutzerkonten genutzt werden, müssen diese mindestens 30 Zeichen lang sein und drei der folgenden Zeichenkategorien beinhalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.
--------	--

Technische Benutzerkonten zeichnen sich dadurch aus, dass sie nicht von Personen verwendet werden. Stattdessen werden sie für die Authentifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt.

Ein System darf für technische Benutzerkonten nur Passwörter verwenden, welche die folgende Komplexität erfüllen:

- Mindestlänge 30 Zeichen
- Bestehend aus mindestens drei der folgenden vier Zeichenkategorien:
 - Kleinbuchstaben
 - Großbuchstaben
 - Ziffern
 - Sonderzeichen

Motivation: Technische Benutzerkonten sind aufgrund ihrer Verwendung in Machine-to-Machine (M2M) Kommunikationsszenarien oft mit Berechtigungen ausgestattet, die für einen Angreifer von hohem Interesse sein können, um Infrastrukturen zu kompromittieren. Ohne Mechanismen einer umfassenden Kompromittierungserkennung kann dann das Risiko, dass ein Passwort von einem Angreifer ermittelt oder gebrochen wird, über die Zeit deutlich ansteigen. Eine signifikante Erhöhung der Passwort-Länge wirkt diesen Risiken entgegen und lässt sich zudem in M2M Szenarien besonders leicht umsetzen, da die Handhabung eines sehr langen Passworts für eine Maschine (im Gegensatz zu einer Person) keine besondere Herausforderung darstellt.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Abstreiten von durchgeführten Aktionen

ID: 3.01-27/9.0

3.3. SQL-Funktionen und Pakete

Req 22	Der Zugriff auf alle OLE Automation Stored Procedures muss deaktiviert werden.
--------	--

Die folgenden OLE Automation Stored Procedures muss der Administrator deaktivieren:

- Sp_OACreate
- Sp_OADestroy
- SP_OAGetErrorInfo
- Sp_OAGetProperty
- SP_OAMethod
- SP_OASetProperty

- SP_OAStop

Motivation: Jede unnötige Funktionalität erhöht das Risiko eines erfolgreichen Angriffs auf das System.

Umsetzungsbeispiel:

```
sp_configure 'show advanced options', 1;
GO;
RECONFIGURE;
GO;
sp_configure 'Ole Automation Procedures', 0;
GO;
RECONFIGURE;
GO; .
```

Um zu überprüfen, ob die OLE Automation Stored Procedures deaktiviert sind, ist folgender Befehl auszuführen:

```
EXEC sp_configure 'Ole Automation Procedures';
GO
```

ID: 3.30-22/8.0

Req 23 SQL Mail muss deaktiviert werden.

Motivation: Jede unnötige Funktionalität erhöht das Risiko eines erfolgreichen Angriffs auf das System .

Umsetzungsbeispiel: USE [master]

```
GO
EXECUTE sp_configure 'SQL Mail XPs', 0;
RECONFIGURE;
GO
```

ID: 3.30-23/8.0

Req 24 Falls nicht verwendet, muss Database Mail deaktiviert werden.

Umsetzungsbeispiel: Database Mail ist standardmäßig ausgeschaltet.

```
USE [master]
GO
EXECUTE sp_configure 'Database Mail XPs', 0;
RECONFIGURE;
GO
```

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

ID: 3.30-24/8.0

Req 25 Wenn SSL für den Zugriff auf eine Datenbankinstanz eingesetzt wird, muss die Option „ForceEncryption“ serverseitig auf „JA“ gesetzt werden.

Motivation: Die Verwendung von SSL kann die Übertragung von vertraulichen Daten effektiv schützen.

ID: 3.30-25/8.0

4. Datenkommunikation

In diesem Kapitel sind Requirements zusammengefasst, die sich mit der Abfrage von Daten aus anderen Datenbanksystemen und dem Datenaustausch zwischen DBKS befassen. Dies kann einerseits über sogenannte Ad-hoc-Anfragen (Queries), andererseits über den Aufbau einer Datenverbindung zum Datenaustausch zwischen den Systemen erfolgen. Die Terminologie dafür und die technische Realisierung solcher Datenverbindungen ist bei den Herstellern stark unterschiedlich (MS SQL: Linked servers/Replikation; Oracle: Datenbank links; DB2: connections). Zur Vereinfachung wird im Folgenden allgemein von Datenbankverbindungen gesprochen.

Req 26 Die Funktion „Remote Server“ muss deaktiviert werden.

Die Unterstützung für „Remote Server“ erfolgt in neueren SQL Server-Versionen nur noch aus Gründen der Rückwärtskompatibilität. Neuere Anwendungen müssen stattdessen „Linked Server“ verwenden. „Linked Server“ verfügen über bessere Sicherheitsfunktionen für die Abfrage und Ausführung von Stored Procedures auf entfernten Instanzen von MS SQL Server und anderen OLE DB-Datenquellen (z. B. Oracle, Access, Excel, DB2). „Remote Server“ unterstützen das Konzept der Remote Stored Procedures (RPC).

Die Option „Remote Server“ muss sowohl auf dem lokalen als auch auf dem entfernten Server aktiviert sein, damit eine Verbindung erfolgreich zustande kommt. Bei MS SQL Server-Version 2005 und neuer ist die Option „Remote Server“ aus Sicherheitsgründen standardmäßig deaktiviert. Darüber hinaus muss der Administrator den MS SQL Server Browser Service aktivieren.

Motivation: Die Funktion stellt ein mögliches Einfallstor für Angreifer dar, wie jede remote erreichbare Funktionalität.

Umsetzungsbeispiel: Zur Deaktivierung der „Remote Server“ kann man die Stored Procedure SP_CONFIGURE verwenden:

```
EXECUTE sp_configure 'remote access', 0; RECONFIGURE;  
GO
```

ID: 3.30-26/8.0

Req 27 Wird die Funktion „Linked Server“ für den Zugriff auf nicht-SQL-SERVER-Anbieter genutzt, muss die standardmäßige Anmeldungszuordnung für die Rolle „Public“ gelöscht werden.

Motivation: Die Rolle „Public“ ist eine Standardrolle für alle Benutzer. Sie ermöglicht potenzielle Angriffe auf der Grundlage einer Vielzahl verschiedener Vorgehensweisen.

Umsetzungsbeispiel: Standardmäßig können alle „Verbindungsserver“ und „Remoteserver“ alle Anmeldungen sehen. Zur Deaktivierung der standardmäßigen Anmeldungszuordnung muss die gespeicherte Prozedur „sp_droplinkedserverlogin“ mit NULL als dem Parameter für „lokale Anmeldung“ ausgeführt werden.

```
EXEC sp_droplinkedserverlogin 'linked-server', NULL;
```

ID: 3.30-27/8.0

Req 28 Falls nicht verwendet, müssen named Pipes deaktiviert werden.

Microsoft Best Practices empfiehlt die Deaktivierung aller unnötigen Protokolle. TCP/IP wird Named Pipes gegenüber für WANs und langsame Netzwerke vorgezogen.

ID: 3.30-28/8.0

5. Missbrauchserkennung und -verhinderung

Req 29	Zugriffe auf Datenbanksysteme sowie kritische Datenbank-Procedures und Datenbankinhalte müssen geloggt werden.
--------	--

Für einen sicheren und nachvollziehbaren Betrieb einer Datenbank ist das Loggen wichtiger Betriebsinformationen notwendig. Hierzu zählt zum Beispiel das Erfassen von erfolglosen Loginversuchen, um mögliche Einbruchversuche zu entdecken. Die Protokollierung sicherheitsrelevanter Benutzeraktionen muss in Übereinstimmung mit dem jeweils geltenden nationalen Recht erfolgen. Bei der Umsetzung von Maßnahmen, die sich aus dieser Anforderung ergeben, sind die jeweils geltenden Beteiligungsrechte der zuständigen Sozialpartner sowie die jeweils bestehenden betrieblichen oder tariflichen Regelungen zu beachten.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

ID: 3.16-26/9.0

Req 30	Die SQL Server default trace muss aktiviert sein.
--------	---

Motivation: Durch Default Tracing sollten Informationen über Konfigurations- und DDL-Veränderungen protokolliert werden, um einen rückverfolgbaren Datenbankbetrieb zu gewährleisten.

ID: 3.30-30/8.0

Req 31	Die Anzahl der Fehlerprotokolle muss auf mindestens 12 erhöht werden.
--------	---

SQL Server erstellt standardmäßig nur bis zu 7 Fehlerprotokolle. Bei jedem Neustart des Servers wird ein weiteres erstellt.

Motivation: Für einen sicheren, rückverfolgbaren Datenbankbetrieb müssen wichtige Betriebsdaten protokolliert werden. Fehlerprotokolle sollten daher nicht nach 7 Neustarts des Servers überschrieben werden.

ID: 3.30-31/8.0

Req 32	Die Serverkonfigurationsoption „xp_cmdshell“ muss auf 0 eingestellt sein.
--------	---

Motivation: Durch Aktivierung dieser Option können Nicht-sysadmin-Personen die Möglichkeit erhalten, Betriebssystembefehle auszuführen.

Umsetzungsbeispiel: USE [master]

GO

EXECUTE sp_configure 'xp_cmdshell', 0;

RECONFIGURE;

GO

ID: 3.30-32/8.0

Req 33	Die Serverkonfigurationsoption „Remote Admin Connections“ muss für nicht-cluster Instanzen auf 0 eingestellt sein.
--------	--

Motivation: Diese Option ermöglicht den Remotezugriff auf die dedizierte administrative Verbindung. Diese Option muss jedoch für gruppierte („clustered“) Instanzen aktiviert sein.

Umsetzungsbeispiel: Nicht an einer gruppierten Instanz ausführen.

```
USE [master]
GO
EXECUTE sp_configure 'Remote Admin Connections', 0; RECONFIGURE;
GO
```

ID: 3.30-33/8.0

Req 34 Der „CLR Assembly Permission Set“ muss für alle benutzerdefinierten CLR Assemblys auf SAFE_ACCESS gesetzt sein.

Umsetzungsbeispiel: Umsetzungsbeispiel:
Suche nach benutzererstellten Assemblys:
SELECT name AS Assembly_Name, permission_set_desc FROM sys.assemblies
WHERE is_user_defined = 1
and permission_set_desc <> 'SAFE_ACCESS';
Es sollten keine Zeilen zurückgegeben werden.

Zur Korrektur:
Für jeden in der obigen Abfrage zurückgegebenen Assembly_Name Folgendes ausführen:

```
USE [master] GO
ALTER ASSEMBLY Assembly_Name WITH PERMISSION_SET = SAFE; GO
```

Dies sollte vor dem Produktivbetrieb zuerst in einer Testumgebung geprüft werden, um sicherzustellen, dass die Assembly auch mit der SAFE-Berechtigungseinstellung noch wie vorgesehen funktioniert.

ID: 3.30-34/8.0

Req 35 Sicherheitsrelevante Ereignisse müssen mit einem exakten Zeitstempel und einer eindeutigen Systembezeichnung protokolliert werden.

Sicherheitsrelevant sind jegliche Ereignisse, die Auswirkungen auf die Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) eines Systems haben können oder dessen mißbräuchliche Verwendung anzeigen. Systeme müssen das Auftreten von sicherheitsrelevanten Ereignissen protokollieren.

Um eine Zuordnung und Auswertung dieser Ereignisse zu ermöglichen, müssen diese zusammen mit einer eindeutigen Systembezeichnung (z. B. Hostname, IP- oder MAC-Adresse) und dem genauen Zeitpunkt des Auftretens ("Zeitstempel") protokolliert werden. Der Zeitstempel eines protokollierten Ereignisses muss mindestens folgende Informationen beinhalten:

- Datum des Ereignisses (Jahr, Monat, Tag)
- Uhrzeit des Ereignisses (Stunden, Minuten, Sekunden)
- Zeitzone, auf die sich diese Zeitangaben beziehen

Die Sicherheitsrelevanz konkreter Ereignisse ergibt sich individuell aus Art und Funktion des Systems sowie den darin verarbeiteten Daten. Daher kann keine einheitliche Liste aus Ereignissen, die Sicherheitsrelevanz besitzen, vorgegeben werden. Relevante Ereignisse müssen passend zum System identifiziert werden. Die folgende Auflistung enthält typische sicherheitsrelevante Ereignisse und ist entsprechend als eine grundlegende Orientierungshilfe bei der Identifikation der sicherheitsrelevanten Ereignisse für ein bestimmtes System zu verstehen.

Sicherheitsrelevantes Ereignis	Informationen, die zum Ereignis zu protokollieren sind
Fehlerhafte Anmeldeversuche	• betroffenes Benutzerkonto, • Anzahl der Fehlversuche • Quelle des Zugriffs (IP-Adresse, Client-ID/Client-Name, lokale Konsole, ...)

Systemzugriffe über Benutzerkonten (einschliesslich System-Konten bzw. technischer Benutzerkonten)	• betroffenes Benutzerkonto • Startzeit/Endzeit des Zugriffs (Anmeldung/Abmeldung) • Quelle des Zugriffs (IP-Adresse, Client-ID/Client-Name, lokale Konsole, ...)
Änderungen an Benutzerkonten (einschliesslich System-Konten bzw. technischer Benutzerkonten)	• Benutzerkonto, mit dem die Änderung vorgenommen wurde • Benutzerkonto, an dem die Änderung vorgenommen wurde • Art der vorgenommenen Änderung (Neueinrichtung, Aktivierung, Deaktivierung, Löschung, Passwort-Rücksetzung, ...)
Änderungen der Rollenzuweisungen/Berechtigungen von Benutzerkonten (einschliesslich System-Konten bzw. technischer Benutzerkonten)	• Benutzerkonto, mit dem die Änderung vorgenommen wurde • Benutzerkonto, an dem die Änderung vorgenommen wurde • Bezeichnung der betroffenen Rolle / Typ der betroffenen Berechtigung • Art der vorgenommenen Änderung (Rolle/Berechtigung hinzugefügt, Rolle/Berechtigung entfernt, ...)
Nutzung/Initiierung von kritischen Systemfunktionen	• Benutzerkonto, mit dem die Nutzung vorgenommen wurde • Bezeichnung/Typ der genutzten Systemfunktion
Zugriff auf sensible Daten ("Sensitive Data"), die im System verarbeitet werden	• Benutzerkonto, mit dem der Zugriff vorgenommen wurde • Bezeichnung des betroffenen Datenfelds (der Inhalt des Datenfelds sollte dabei nicht mit protokolliert werden, um einen Datenabfluss über Log-Dateien zu verhindern) • Art des Zugriffs (Lesen, Ändern, Löschen, ...)
Abnormaler Anstieg in der Auslastung von Systemressourcen, wie etwa Arbeitsspeicher, CPU, Netzwerk oder Festplattenzugriffen über einen längeren Zeitraum	• Schwellwert der betroffenen Systemressource • Dauer der Überschreitung des Schwellwerts • Höhe der Überschreitung des Schwellwerts Es müssen abhängig vom individuellen System sinnvolle Schwellwerte definiert werden.
Sonstige Ereignisse, die für versuchte oder erfolgreiche Angriffe gegen das System Hinweise liefern können *)	• individuell abhängig von der Art des Ereignisses

**) Dies erfordert eine Identifizierung der wichtigsten, für das System typischerweise zu erwartenden Angriffsformen und die Sicherstellung, dass zu deren Erkennung relevante Ereignisse durch das System tatsächlich protokolliert werden. In der Regel kann das nur durch den Entwickler/Hersteller des Systems gewährleistet werden.*

Bei der Protokollierung müssen die jeweils geltenden gesetzlichen und betrieblichen Bestimmungen beachtet werden. Letztere umfassen insbesondere auch Vereinbarungen, die mit den betrieblichen Sozialpartnern getroffen wurden. Diese Bestimmungen besagen unter anderem, dass die Protokollierung von Ereignissen nur zweckgebunden erfolgen darf. Die Protokollierung von Ereignissen zum Zweck der Arbeitskontrolle von Mitarbeitern ist nicht zulässig.

Zudem muss - wie für jegliche Daten, die von einem System verarbeitet werden - auch für Protokollierungsdaten ein angemessener Schutzbedarf berücksichtigt und umgesetzt werden; dies gilt für die Speicherung, die Übertragung sowie den Zugriff. Insbesondere falls Wirkdaten in den Protokollierungsdaten enthalten sind, muss derselbe Schutzbedarf berücksichtigt werden, der auch für die reguläre Verarbeitung dieser Wirkdaten innerhalb des Quell-Systems Anwendung findet.

Motivation: Die Protokollierung von sicherheitsrelevanten Ereignissen ist eine Grundvoraussetzung, um laufende Angriffe oder auch Angriffe im Nachhinein erkennen zu können. Nur so ist es möglich, sinnvolle Maßnahmen zur Erhaltung oder auch Wiederherstellung der Systemsicherheit durchzuführen. Des Weiteren dienen die Protokollierungsdaten der Beweissicherung, um rechtlich gegen Angreifer vorgehen zu können.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-33/9.0

Req 36	Für sicherheitsrelevante Protokollierungsdaten, die lokal erfasst werden, müssen geltende Aufbewahrungszeiträume und Löschfristen eingehalten werden.
--------	---

Aus Sicht der IT-Sicherheit wird auf einem System die lokale Erfassung von sicherheitsrelevanten Protokollierungsdaten nicht zwingend gefordert. Da lokal erfasste Protokollierungsdaten bei Systemstörungen beschädigt oder von einem erfolgreichen Angreifer gezielt manipuliert werden können, sind sie für sicherheitstechnische bzw. forensische Analysen nur bedingt belastbar. Entsprechend ist für die IT-Sicherheit relevant, dass Protokollierungsdaten an einen separaten Log Server weitergeleitet werden.

Eine lokale Erfassung kann dennoch erfolgen; beispielsweise falls bei der Erzeugung der Protokollierungsdaten eine lokale Speicherung aufgrund technischer Abläufe zunächst unabdingbar ist oder es begründete betriebliche Interessen gibt, Protokollierungsdaten auch lokal vorzuhalten.

Folgende Grundregelung ist bei einer lokalen Erfassung von Protokollierungsdaten zu berücksichtigen:

- Sicherheitsrelevante Protokollierungsdaten müssen für einen Zeitraum von 90 Tagen aufbewahrt werden.
(Diese Anforderung gilt nur, falls auf dem System keine zusätzliche Weiterleitung an einen separaten Log Server umgesetzt ist und Protokollierungsdaten daher ausschließlich lokal erfasst werden.)
- Nach Ablauf von 90 Tagen muss eine umgehende Löschung von gespeicherten Protokollierungsdaten erfolgen.

Abweichungen

Abweichende Aufbewahrungszeiträume und Löschfristen können durch gesetzliche oder regulatorische Anforderungen (insbesondere im Zusammenhang mit personenbezogenen Daten) bestehen oder durch vertragliche Vereinbarungen definiert sein. In diesen Fällen sind die geltenden Zeiträume individuell mit einem Project Security Manager (PSM) bzw. Datenschutzberater (DSB) abzustimmen oder werden durch diesen vorgegeben.

Motivation: Protokollierungsdaten sind ein immens wichtiges Werkzeug der IT-Sicherheit zur Abwendung, Detektierung und Aufklärung von Systemstörungen, Sicherheits- und Datenschutzvorfällen. Auf der anderen Seite unterliegt die Erfassung von Protokollierungsdaten wie jede andere Datenverarbeitung auch gesetzlichen und regulatorischen Auflagen. Entsprechend müssen Richtlinien eingehalten werden, die beides in Einklang bringen.

Umsetzungsbeispiel: Unter Berücksichtigung der gültigen Gesetzeslage und zutreffenden Datenschutz-Regularien werden folgende Löschfristen für lokal erfasste sicherheitsrelevante Protokollierungsdaten auf einem beispielhaften TK-System umgesetzt:

- Standard System Logs: Löschung nach spätestens 90 Tagen
- Protokollierungen von öffentlichen IP-Adressen: Löschung (oder Anonymisierung) nach spätestens 7 Tagen
- Protokollierungen der Vergabe von dynamischen öffentlichen IP-Adressen durch die TK-Lösung: Löschung nach spätestens 7 Tagen

- Protokollierungen nicht abrechnungsrelevanter Call Detail Records: Löschung nach spätestens 7 Tagen
- Protokollierungen der Kommunikations-Inhalte von E-Mail und SMS: Löschung nach spätestens 24 Stunden
- Protokollierungen der behandelten Domain-Abfragen des DNS-Servers der TK-Lösung: Löschung nach spätestens 24 Stunden

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-34/9.0

Req 37 Sicherheitsrelevante Protokollierungsdaten müssen umgehend nach deren Erzeugung an einen Log-Server weitergeleitet werden.

Die sicherheitsrelevanten Protokollierungsdaten des Systems müssen umgehend nach deren Erzeugung an einen Log-Server weitergeleitet werden.

Im Sinne der Anforderung muss der dafür genutzte Log-Server die folgenden Kriterien erfüllen:

- Der Log-Server muss dediziert für die Vorhaltung von Protokollierungsdaten eingesetzt sein. Er darf keine weiteren Funktionen oder Dienste abbilden, die nicht in Relation zu dieser Aufgabe stehen. Eine zulässige Ausnahme ist die Kombination eines Log Servers mit einer SIEM (Security Information and Event Management) Lösung.
- Der Log-Server muss vom System separiert sein. Er darf nicht als zusätzliches Modul unmittelbar mit auf dem System betrieben werden.
- Der Log-Server muss zentral für die Einsatzumgebung bereitstehen, zu der auch das System gehört.

Zur Übertragung der Protokollierungsdaten an den Log-Server sollten bevorzugt auf diesen Zweck spezialisierte Standard-Protokolle (z. B. Syslog oder SNMPv3) zum Einsatz kommen.

Motivation: Werden Protokollierungsdaten nur lokal gespeichert, können diese im Fall einer erfolgreichen Kompromittierung des Systems durch einen Angreifer manipuliert werden, um dessen Angriff und auf dem System durchgeführte Aktionen zu verschleiern. Aus diesem Grund muss die Weiterleitung von Protokollierungsdaten an einen Log-Server sehr zeitnah nach dem Auftreten eines sicherheitsrelevanten Ereignisses im Quell-System erfolgen. So stehen die angefallenen Protokollierungsdaten separiert vom Quell-System und unabhängig von dessen Zustand jederzeit für Analysen bereit. Die Verwendung eines zentralen Log-Servers für eine Einsatzumgebung stellt sicher, dass auf die Logs sämtlicher IT/NT-Systeme dieser Einsatzumgebung schnell und einheitlich zugegriffen und der Zugriff selbst optimal in die Incident-Prozesse der Umgebung integriert werden kann.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Modifikation von Daten
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-35/9.0

Req 38 Für sicherheitsrelevante Protokollierungsdaten, die an den Log Server weitergeleitet werden, muss die Einhaltung geltender Aufbewahrungszeiträume und Löschfristen sichergestellt werden.

Folgende Grundregelung ist zu berücksichtigen:

- sicherheitsrelevante Protokollierungsdaten müssen auf dem Log Server für einen Zeitraum von 90 Tagen aufbewahrt werden.

- nach Ablauf von 90 Tagen muss eine umgehende Löschung der auf dem Log Server gespeicherten Protokollierungsdaten erfolgen.

Abweichungen

Abweichende Aufbewahrungszeiträume und Löschfristen können durch gesetzliche oder regulatorische Anforderungen bestehen (insbesondere im Zusammenhang mit personenbezogenen Daten) oder durch vertragliche Vereinbarungen definiert sein. In diesen Fällen sind die geltenden Zeiträume individuell mit einem Project Security Manager (PSM) bzw. Datenschutzberater (DSB) abzustimmen oder werden durch diesen vorgegeben.

Log Server in Verantwortung eines Dritten

Sollte der ausgewählte Log Server nicht innerhalb derselben operativen Verantwortung liegen wie das Quellsystem der Protokollierungsdaten, muss sichergestellt werden, dass dem verantwortlichen Betreiber des Log Servers die gültigen Parameter für die zu empfangenden Protokollierungsdaten bekannt sind und durch diesen im Sinne der hier genannten Regelungen eingehalten werden.

Motivation: Protokollierungsdaten sind ein immens wichtiges Werkzeug der IT-Sicherheit zur Abwendung, Detektierung und Aufklärung von Systemstörungen, Sicherheits- und Datenschutzvorfällen. Auf der anderen Seite unterliegt die Erfassung von Protokollierungsdaten wie jede andere Datenverarbeitung auch gesetzlichen und regulatorischen Auflagen. Entsprechend müssen Richtlinien eingehalten werden, die beides in Einklang bringen.

Umsetzungsbeispiel: Unter Berücksichtigung der gültigen Gesetzeslage und zutreffenden Datenschutz-Regularien werden folgende Löschfristen für ausgeleitete sicherheitsrelevante Protokollierungsdaten eines beispielhaften TK-Systems auf dem separaten Log Server umgesetzt:

- Standard System Logs: Löschung nach spätestens 90 Tagen
- Protokollierungen von öffentlichen IP-Adressen: Löschung (oder Anonymisierung) nach spätestens 7 Tagen
- Protokollierungen der Vergabe von dynamischen öffentlichen IP-Adressen durch die TK-Lösung: Löschung nach spätestens 7 Tagen
- Protokollierungen nicht abrechnungsrelevanter Call Detail Records: Löschung nach spätestens 7 Tagen
- Protokollierungen der Kommunikations-Inhalte von E-Mail und SMS: Löschung nach spätestens 24 Stunden
- Protokollierungen der behandelten Domain-Abfragen des DNS-Servers der TK-Lösung: Löschung spätestens nach 24 Stunden

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-36/9.0

Req 39	Sicherheitsrelevante Protokollierungsdaten müssen echtzeitnah an eine Erkennungs- und Reaktionslösung für Sicherheitsvorfälle bereitgestellt werden.
--------	--

Eine zulässige Erkennungs- und Reaktionslösung im Sinne dieser Anforderung muss die folgenden Kriterien erfüllen:

- Es erfolgt eine kontinuierliche Analyse bzw. Korrelation der aus angebundenen IT/NT-Systemen bereitgestellten Protokollierungsdaten.
- Die Identifizierung bedrohlicher Aktivitäten und laufender Angriffe findet auf Basis einer fortlaufend aktuell gehaltenen Erkennungsmuster-Datenbank statt.
- Integrierte Alarmierungsprozesse lösen im Fall eines Fundes die Einleitung von Gegenmaßnahmen aus.
- Sicherheitsexperten sind aktiv involviert in den Betrieb der Lösung sowie die Auswertung von Alarmen.

Eine solche Lösung ist in ihrer Funktion nicht mit einem Log Server gleichzusetzen. Entsprechend muss die Bereitstellung an eine Erkennungs- und Reaktionslösung stets zusätzlich zu einer vorhandenen Weiterleitung an einen Log Server

ver erfolgen. Eine Ausnahme besteht, falls der genutzte Log Server seinerseits die Protokollierungsdaten umgehend nach Erhalt zusätzlich an eine Erkennungs- und Reaktionslösung bereitstellt. In diesem Fall ist es ausreichend, dass das System die Protokollierungsdaten nur an den Log Server weiterleitet.

Die Protokollierungsdaten müssen ab dem Zeitpunkt ihrer Erzeugung im System innerhalb von 5 Minuten an die Erkennungs- und Reaktionslösung bereitgestellt werden ("echtzeitnah").

Die konkret zu unterstützenden technischen Schnittstellen und Protokolle für die Bereitstellung werden durch die im Einsatzumfeld des Systems verfügbare Erkennungs- und Reaktionslösung sowie die technische Basis des Systems bestimmt.

Motivation: IT/NT-Systeme sind permanent sicherheitstechnischen Bedrohungen und Angriffen ausgesetzt. Mittels einer zentralen Analyse und der Korrelation erfasster System-Ereignisse ganzer IT-Landschaften in nahezu Echtzeit können aktuelle Bedrohungen und laufende Angriffe auch über Systemgrenzen hinaus erkannt und zeitnah passende Gegenmaßnahmen eingeleitet werden. Die unverzügerte Bereitstellung von Protokollierungsdaten an die Erkennungs- und Reaktionslösung ist essenziell für deren Effektivität.

Umsetzungsbeispiel: **Beispiel 1:** Ein System auf Basis eines klassischen Servers erfasst sicherheitsrelevante Protokollierungsdaten im lokalen Syslog oder Windows Event Log des Betriebssystems. Die Protokollierungsdaten werden kontinuierlich zur weiteren Analyse, Angriffserkennung und Alarmbehandlung an ein SIEM (Security Information and Event Management) weitergeleitet.

Beispiel 2: Auf einem System wird ein EDR ("Endpoint Detection and Response") Agent ausgeführt. Der EDR-Agent leitet die von ihm auf dem System erfassten sicherheitsrelevanten Protokollierungsdaten kontinuierlich an das zentrale Backend der EDR-Lösung aus, auf dem die weitere Analyse, Angriffserkennung und Alarmbehandlung erfolgt.

Beispiel 3: Netzwerk-Komponenten stellen Ereignisse an ein SIEM bereit, die es ermöglichen, verdächtiges Kommunikationsverhalten wie Netzwerk-Scans, unzulässige Datenflüsse zwischen Netz-Segmenten oder aktive Verbindungen bzw. Verbindungsversuche zu verdächtigen Zielen im Internet zu entdecken. Im speziellen liefern Gateway Router aus dem CNDTAG "Netflow" Logs, während Forward Proxies Zugriffe auf Domänen und/oder IP-Adressen melden und Firewalls blockierte Verbindungsversuche loggen.

Beispiel 4: Auf Basis von Cloud-nativen Funktionen entwickelte Systeme erzeugen Protokollierungsdaten mittels der Cloud-eigenen Protokollierungs- und Überwachungsinfrastruktur direkt aus diesen Funktionen heraus. In einem solchen System wird die Erzeugung sicherheitsrelevanter Protokollierungsdaten in den entsprechenden Konfigurationsoptionen der eingesetzten Cloud-nativen Funktionen gezielt aktiviert. Die entstehenden Protokollierungsdaten werden kontinuierlich zur weiteren Analyse, Angriffserkennung und Alarmbehandlung an ein SIEM (Security Information and Event Management) übertragen. Einige Cloud-Anbieter leisten eine gewisse Angriffsmustererkennung bereits in der Cloud-eigenen Überwachungsinfrastruktur und erzeugen daraus spezifische Cloud-Alarme. Diese werden zusätzlich an das SIEM übertragen.

Beispiel 5: Ein System basiert auf einer SaaS ("Software as a Service") Applikation eines Cloud-Anbieters. Typischerweise verantwortet im SaaS Modell der Cloud-Anbieter alle operativen Aspekte der Applikation, inkl. des Sicherheitsmanagements. Der Cloud-Kunde selbst hat keinen Einfluss auf die zugrunde liegende technische Infrastruktur oder den Betrieb der Applikation. Anhand von Vertragsvereinbarungen, anerkannten Zertifikaten und dokumentierten Selbstauskünften des Cloud-Anbieters wird formell überprüft, dass der Cloud-Anbieter eine Erkennungs- und Reaktionslösung für Sicherheitsvorfälle implementiert hat. Einige Cloud-Anbieter erzeugen zusätzlich dedizierte Protokollierungsdaten über sicherheitsrelevante Aktivitäten innerhalb der separaten Kunden-Mandanten ihrer SaaS Applikation (beispielsweise zu Änderungen von Konfigurationseinstellungen, Berechtigungsvergaben oder Benutzer-Konten innerhalb der Mandanten) und stellen diese den Cloud-Kunden zu Verfügung. Diese sogenannten Audit-Logs werden kontinuierlich zur weiteren Analyse, Angriffserkennung und Alarmbehandlung an ein SIEM (Security Information and Event Management) übertragen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unbemerkt durchführbare Angriffe

ID: 3.01-37/9.0

Req 40	Wichtige Datenbank-Dienste und -Instanzen müssen kontinuierlich auf Missbrauchsszenarien hin überwacht werden.
--------	--

Die Überwachung von Benutzeraktionen auf Missbrauch muss in Übereinstimmung mit dem jeweils geltenden nationalen Recht erfolgen.

Es muss eine Fallstudie zur Art des Dienstes/Nutzerdatens, der Anzahl der Einträge und möglichen Missbrauchsszenarien geben, um das notwendige Maß an Überwachung der Fälle zu definieren.

- Insider-Bedrohungen
- Anomalieerkennung
- Accidental exposure
- Fehlkonfiguration
- Verwundbare Anwendung
- Machine Language Models
- Unsichere Daten im Transit
- ...

Motivation: Die missbräuchliche Nutzung von Datenbanksystemen ist vielfältig denkbar. Benutzer erzeugen eine ungewöhnlich hohe Datenlast beziehungsweise agieren zu ungewöhnlichen Uhrzeiten. Angreifer nutzen bei Datenbankabfragen unübliche und kritische Befehle sowie Tools und Schadcode, um ihre Rechte zu erweitern. Um eine missbräuchliche Nutzung zu erkennen, sollten Datenbanksysteme kontinuierlich auf Missbrauchsszenarien überwacht werden etwa durch Datenbanktrigger und Logüberwachung.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.16-32/9.0

Req 41	Massendatenexfiltration muss erkannt werden, wenn mehr als 100.000 Kundendaten und DSK2 oder DSK3 vorhanden sind.
--------	---

Die Massendatenexfiltrationserkennung ist eine kritische Kontrolle, die überwacht, ob ungewöhnlich große Datenmengen intern übertragen oder das Unternehmensnetzwerk oder die Datenbanksysteme verlassen. Wenn mehr als 100.000 Kundendaten – insbesondere als DSK2 oder DSK3 klassifiziert – abgerufen, kopiert oder übertragen werden, sollten automatisierte Alarmlösungen ausgelöst werden. Diese schwellenwertbasierte Erkennung sollte mit SIEM- und User and Entity Behavior Analytics (UEBA)-Tools integriert werden, um Abweichungen von normalen Zugriffsmustern zu identifizieren. Das System sollte den Zugriffskontext (Benutzerrolle, Zeit, Datensensitivität und Übertragungskanal) korrelieren, um legitime Massenoperationen von potenziellen Exfiltrationsversuchen zu unterscheiden. Nach Entdeckung sollten vordefinierte Vorfalldiagnose-Workflows die Aktivität sofort isolieren, das Sicherheitsoperationszentrum informieren und forensische Beweise für die Untersuchung sichern.

Motivation: Kundendaten sind eines der wertvollsten Vermögenswerte des Unternehmens. Deshalb müssen wir alle Maßnahmen ergreifen, um massenhafte Datenlecks, böswillige Handlungen oder Missbrauch zu vermeiden. Dafür müssen wir wissen, wie wir unsere Datensätze handhaben und nutzen.

Umsetzungsbeispiel: Technische Leitlinien und Implementierungsdetails werden ebenfalls auf dieser Seite bereitgestellt und kontinuierlich gepflegt:

<https://yam-united.telekom.com/pages/psa/apps/wiki/wiki-sicherheitsanforderungen/list>

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.16-33/9.0

6. MS SQL-spezifische Anforderungen

Zusätzlich zu den aus dem Hauptdokument abgeleiteten Sicherheitsanforderungen sind die folgenden herstellerspezifischen Anforderungen zu berücksichtigen.

Req 42	Es muss der Windows-Authentifizierungsmodus verwendet werden.
--------	---

Motivation: Verglichen mit der Windows-Authentifizierung bietet die Mixed-Mode-Authentifizierung nur einen unzureichenden Sicherheitsstandard. Die Windows-Authentifizierung verwendet das Kerberosprotokoll. Außerdem lassen sich die Validierung der Passwortkomplexität, die Kontosperrung und der Passwortablauf über Group Policies erzwingen.

ID: 3.30-42/8.0

Req 43	Die Serverkonfiguration „Cross-database Ownership Chaining“ muss deaktiviert werden.
--------	--

Motivation: Die aktivierte Konfigurationsoption gilt für alle Datenbanken, die auf der Instanz. Die Angriffsfläche wird dadurch für alle Datenbanken unnötig erhöht.

ID: 3.30-43/8.0

Req 44	Die DB-Konfigurationsoption „DB_CHAINING“ muss deaktiviert sein.
--------	--

Motivation: Eine Eingrenzung der Rechte reduziert die Angriffsfläche und erhöht damit die Sicherheit.

Umsetzungsbeispiel: ALTER DATABASE dbname SET DB_CHAINING OFF;
GO

ID: 3.30-44/8.0