

Sicherheitsanforderung

Oracle-Datenbanksysteme

Deutsche Telekom Gruppe

Version	9.0
Datum	01.12.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 3.29	Dokumententyp Sicherheitsanforderung
Version 9.0	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

Dieses Dokument wurde auf Basis der Vorgaben aus den im Konzern gültigen Sicherheitsrichtlinien erstellt. Ausgehend von der Sicherheitsanforderung „Datenbanksysteme – Allgemeine Sicherheitsanforderungen“ enthält es, mit dem Ziel eines einheitlichen Sicherheitsstandards, herstellerspezifische Sicherheitsanforderungen an Oracle-Datenbanksysteme.

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
1.1.	Verantwortlichkeiten	4
2.	Allgemein	5
3.	Grundlegende Sicherheitsanforderungen	6
3.1.	Version der verwendeten Datenbank	6
4.	Härtung des Datenbanksystems	7
4.1.	Diensteeliminierung	7
4.2.	Benutzer und Rollen	9
4.3.	Passwörter	11
4.4.	Least Privilege-Prinzip	17
4.5.	Externe Prozeduren	18
4.6.	SQL-Erweiterungen mit Betriebssystem- oder Netzwerkzugriff	19
4.7.	Zugriffsrechte	20
5.	Datenkommunikation	23
6.	Systemüberwachung	25
6.1.	Protokollierung	25
7.	Oracle-spezifische Anforderungen	33
7.1.	Authentifizierung	33
7.2.	Listener- und Netzwerkverbindung	34
7.3.	Privilegien für Benutzer und Rollen	35
8.	Technischer Basisschutz von IT-/NT-Systemen	39
8.1.	Authentifizierung und Autorisierung	39

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.

1.1. Verantwortlichkeiten

Der Systemverantwortliche hat die Umsetzung der Sicherheitsanforderungen aus diesem Anforderungsdokument sicherzustellen.

Die Sicherheitsanforderung richtet sich an alle Personen, die für die Entwicklung und den Betrieb von Datenbanksystemen verantwortlich sind oder Datenbanksysteme entwickeln (lassen) sowie beschaffen.

2. Allgemein

Die vorliegende Sicherheitsanforderung beinhaltet zahlreiche kleinere und größere Erweiterungen, Aktualisierungen und Fehlerkorrekturen gegenüber der Vorgängerversion. Eine intensive Beschäftigung mit der aktualisierten Sicherheitsanforderung wird daher dringend empfohlen.

Nachfolgend wird unter dem Begriff „DBA User“, bzw. „DBA Account“ ein Datenbank- Konto/Account verstanden, das DBA (Datenbankadministrator) Berechtigungen hat oder DBA-nahe Tätigkeiten nach dem Funktionstrennungsprinzip (z.B. Benutzerverwaltung, Backup, etc.) wahrnimmt.

3. Grundlegende Sicherheitsanforderungen

3.1. Version der verwendeten Datenbank

Req 1	Die verwendete Datenbank-Software muss vom Hersteller für den produktiven Einsatz empfohlen und freigegeben sein und sich gemäß der Oracle Lifetime Support Policy in der „Premier Support“- oder „Extended Support“-Phase befinden.
-------	--

11.1: Premier Support bis August 2012, Extended Support bis August 2015.

11.2: Premier Support bis Januar 2015, Extended Support bis Januar 2018.

Alle älteren Versionen befinden sich in der Phase „Sustaining Support“, für die der Hersteller keine regelmäßigen Sicherheits-Updates mehr bereitstellt; hierdurch steigt die Möglichkeit eines Angriffs erheblich.

Referenz:

<http://www.oracle.com/us/support/lifetime-support/index.html>

Siehe PDF -> Resources -> „Lifetime Support Policy: Oracle Technology Products“, bzw. Direktlink.

<http://www.oracle.com/us/support/library/lifetime-support-technology-069183.pdf>

Motivation: Nur eine Datenbanksoftwareversion, für die der Hersteller vollständigen Support anbietet, garantiert einen sicheren und stabilen Betrieb des Produktes.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.29-1/9.0

4. Härtung des Datenbanksystems

In diesem Kapitel sind Anforderungen zur Härtung des Datenbanksystems aufgeführt. Die Maßnahmen sind vergleichbar mit denen einer Betriebssystemhärtung. Die folgenden Anforderungen dienen also dazu, die Auswirkungen unautorisierter Zugriffe auf das Datenbanksystem zu minimieren.

4.1. Diensteliminierung

Req 2	Nicht benötigte Komponenten des Oracle-DBMS dürfen nicht installiert werden.
-------	--

Bei der Installation ist darauf zu achten, nur notwendige Komponenten (z.B. nicht Apache-HTTP-Server, APEX, Spatial etc.) zu installieren.

Referenzen:

http://docs.oracle.com/cd/B28359_01/install.111/b32002/install_overview.htm

http://docs.oracle.com/cd/E11882_01/install.112/e24321.pdf

Motivation: Zusätzliche Komponenten erhöhen die Wahrscheinlichkeit des Auftretens von Schwachstellen und erhöhen den Betriebsaufwand unnötig.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.29-2/9.0

Req 3	Der Oracle HTTP Server darf nicht auf dem DBMS-Server installiert sein bzw. muss deaktiviert werden.
-------	--

Zur Einhaltung der N-Tier Architektur darf der Oracle HTTP Server nicht auf der gleichen Betriebssysteminstanz wie das DBMS installiert sein bzw. muss deaktiviert werden.

Ist die Verwendung des Oracle HTTP Servers erforderlich, so müssen die Verantwortlichen sicherstellen, dass dieser auf einem dedizierten Server, getrennt vom Datenbanksystem läuft.

Überprüfung:

Mit dem Befehl `$ORACLE_HOME/apache/apache/bin/apachectl` kann der Administrator nachprüfen, ob der Server aktiv ist.

Motivation: Zusätzliche Funktionalitäten verursachen zusätzliche Sicherheitsschwachstellen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.29-3/9.0

Req 4	Oracle Application Express (APEX) darf nicht auf dem DBMS-Server installiert sein bzw. muss deaktiviert werden
-------	--

Zur Einhaltung der N-Tier Architektur darf der Oracle Application Express (APEX) nicht auf der gleichen Betriebssysteminstanz wie das DBMS installiert sein bzw. muss deaktiviert werden.

Der Oracle Application Express ist ab Oracle 11g, zusammen mit der Datenbank standardmäßig vorinstalliert.

Wird Oracle Application Express benötigt, so müssen die Verantwortlichen sicherstellen, dass dieser auf einem dedizierten Server, getrennt vom Datenbanksystem läuft.

Überprüfung:

Nach Installation von APEX befinden sich Dateien in \$ORACLE_HOME/apex und es existieren Benutzerkonten der Art FLOWS_* in der Datenbank.

Referenzen:

http://docs.oracle.com/cd/E14373_01/install.32/e13366/overview.htm#i46634

http://docs.oracle.com/cd/E14373_01/appdev.32/e11838/sec.htm

<http://www.oracle.com/technetwork/developer-tools/apex/overview/index.html>

http://en.wikipedia.org/wiki/Oracle_Application_Express

<http://www.springer.com/computer/database+management+%26+information+retrieval/book/978-1-4302-4731-9>

Motivation: Zusätzliche Funktionalitäten verursachen zusätzliche Sicherheitsschwachstellen.

Umsetzungsbeispiel: Um APEX zu deinstallieren loggen sich Administratoren ein und rufen @apxremov.sql auf (siehe http://download.oracle.com/docs/cd/E17556_01/doc/install.40/e15513.pdf, S. A-6)

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unbemerkt durchführbare Angriffe
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.29-4/9.0

Req 5	Auf einer Betriebssysteminstanz (Hardwareplattform oder Virtualisierungsgast) darf jeweils nur eine Instanz des Datenbanksystems installiert sein.
-------	--

Motivation: Läuft der Betrieb mehrerer Datenbankinstanzen für verschiedene Aufgaben (z. B. Internet und Intranet) auf einer Betriebssysteminstanz, sind die Instanzen nicht voneinander separiert. Es besteht das Risiko, dass Angreifer auch das zweite Datenbanksystem korrumpieren. Um die einzelnen Datenbankinstanzen zu trennen, lassen sich Virtualisierungslösungen einsetzen.

Umsetzungsbeispiel: Zur Trennung der einzelnen Datenbankinstanzen können Administratoren physikalische Serverhardware, wie auch Virtualisierungslösungen einsetzen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.29-5/9.0

Req 6	Nicht benötigte (Default-) Datenbanken auf dem Datenbanksystem müssen gelöscht werden.
-------	--

Motivation: Bei der Installation von Datenbanksystemen werden oftmals Test- oder Übungsdatenbanken installiert, die im Wirkbetrieb der Datenbank nicht mehr erforderlich sind. In der Vergangenheit zeigten diese Testdatenbanken Schwachstellen, die es einem Angreifer ermöglichen, privilegierte Rechte auf dem Datenbanksystem zu erlangen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 3.16-7/9.0

Req 7	Auf einer Betriebssysteminstanz (mit physikalischer oder virtualisierter Hardware) dürfen nur dann mehrere Datenbankinstanzen zusammen betrieben werden, wenn diese • den gleichen, niedrigen Schutzbedarf haben, • unter einer einzigen Kundenhoheit stehen und • administrativ vom gleichen Personenkreis betrieben werden.
-------	--

Motivation: Durch den gemeinsamen Betrieb mehrerer Datenbankinstanzen steigt die Gefahr, dass Benutzer unrechtmäßigerweise Zugriff auf Instanzen erhalten, für die sie weder fachlich noch administrativ zuständig sind.

Umsetzungsbeispiel: Zur Trennung der einzelnen Datenbankinstanzen können Administratoren physikalische Serverhardware, wie auch Virtualisierungslösungen einsetzen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Unbemerkt durchführbare Angriffe

ID: 3.16-9/9.0

Req 8	Alle Datenbankdienste müssen mit minimalen Rechten (least privilege principle) auf Betriebssystemebene aufgesetzt werden.
-------	--

Motivation: Durch die Verwendung von minimalen Rechten lässt sich die Gefahr der Systemkorrumpierung reduzieren.

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: 3.16-17/9.0

4.2. Benutzer und Rollen

Req 9	(Default-) Benutzerkonten und (Default-) Rollen müssen gelöscht werden, falls diese nicht benötigt werden. Ist dies nicht möglich oder nicht sinnvoll, muss der Benutzerstatus auf „EXPIRED & LOCKED“ gesetzt werden.
-------	--

Achtung: Datenbankbenutzerkonten mit dem Status „EXPIRED & LOCKED“ können weiterhin Aktivitäten in der Datenbankinstanz durchführen, obgleich diese gesperrt sind. Auch ein ggf. aktiviertes Auditing wird in diesem Fall nichts nutzen, da solche Aktivitäten nicht aufgezeichnet werden. Das Vorgehen einer Sperrung birgt daher die Gefahr eines versteckten Missbrauchs in sich (Beispiel automatisierte Jobs). Das Sperren von Benutzern ist somit immer nur die schlechtere Alternative.

Die folgenden Default-Benutzer sind in einer Produktionsumgebung nicht notwendig:

ADAMS
ADLDEMO
ANDY
BLAKE
CDEMOCOR
CEMORID
CEMOUCB
CEMO82

CLARK
 DEMO
 DIANE
 FROSTY
 HLW
 HR
 IX
 JAKE
 JILL
 JONES
 OE
 PM
 QS
 QS_ADM
 QS_CB
 QS_CBADM
 QS_CS
 QS_ES
 QS_OS
 QS_WS
 SCOTT
 SH

Soweit nicht benötigt, sollten die folgenden Benutzer den Status „EXPIRED & LOCKED“ haben:

Account	Explanation
ANONYMOUS	Oracle XML DB
CTXSYS	CTXSYS
DBSNMP	Oracle Enterprise Manager
DIP	Oracle Label Security
DSSYS	Dynamic Services Engine
EXFSYS	Rules Manager & Expression Filter
FLAWS_30000	Oracle Database Application Express
FLAWS_FILES	Oracle Database Application Express
LBACSYS	Oracle Label Security
MDDATA	Oracle Spatial
MDSYS	Oracle Spatial/Oracle Multimedia Locator
MGMT_VIEW	Oracle Enterprise Manager Database Control
ODM	Oracle Data Mining
ODM_MTR	Oracle Data Mining
OLAPSYS	OLAP
ORDDATA	Oracle Multimedia DICOM
ORDPLUGINS	Oracle Multimedia
ORDSYS	Oracle Multimedia
OUTLN	plan stability
ORACLE_OCM	Oracle Configuration Manager
OWBSYS	Oracle Warehouse Builder

REPADMIN	Replication user
SI_INFORMTN_SCHEMA	SQL/MM Still Image Standard
SPATIAL_CSW_ADMIN_USR	Oracle Spatial CSW Cache Manager
SPATIAL_WFS_ADMIN_USR	Oracle Spatial WFS Cache Manager
TRACESVR	Oracle Trace Server
WK_TEST	Oracle Ultra Search
WKPROXY	Oracle Ultra Search
WKSYS	Oracle Ultra Search
WMSYS	Oracle Workspace Manager
XDB	Oracle XML DB
XS\$NULL	internal

Referenzen:

Sample Schemas 11.2 http://download.oracle.com/docs/cd/E11882_01/server.112/e10831.pdf

Default-Passwörter und deren Hash Codes http://www.petefinnigan.com/default/default_password_list.htm

Liste Default User http://www.oraFAQ.com/wiki/List_of_default_database_users

Securing Oracle Database User Accounts

http://docs.oracle.com/cd/E11882_01/server.112/e10575/tdpsg_user_accounts.htm

Motivation: Installationsprogramme von Datenbanksystemen richten oftmals eine Vielzahl von Benutzern und Rollen ein, die die Nutzer der Datenbank nicht benötigen. Diese Rollen sind z. B. für Übungs- und Test-Datenbanken gedacht. Ein Angreifer kann durch die Kenntnis von Default-Usern und Rollen (privilegierten) Zugriff auf das Datenbanksystem erlangen. Daher sind nicht benötigte Benutzer und Rollen zu löschen oder zu sperren (nur Benutzer).

Umsetzungsbeispiel: Für die Löschung dieser Schemata kann keine allgemein gültige Vorgehensweise angegeben werden, diese bitte individuell in „My Oracle Support“ (MOS) nachlesen.

Zum Setzen des Status eines Benutzers auf „EXPIRED & LOCKED“:

```
ALTER USER <Benutzername> ACCOUNT LOCK;
ALTER USER <Benutzername> PASSWORD EXPIRE;
```

Überprüfung: Alle Benutzer mit Status anzeigen:

```
SELECT Username, Status FROM DBA_USERS;
```

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.29-9/9.0

4.3. Passwörter

Req 10 Default-Passwörter müssen geändert werden.

Default-Passwörter müssen unmittelbar nach der Systeminstallation und vor dem Start eines Network Listeners geändert werden.

Überprüfung:

Benutzerkonten mit Default-Passwörtern anzeigen lassen:
`SELECT * FROM dba_users_with_defpwd;`

Befehl zum Ändern eines Passworts:
`ALTER USER <Benutzername> IDENTIFIED BY <neues Passwort>;`

Referenzen: <http://www.oracle.com/technetwork/articles/sql/11g-security-100258.html>

Eine Liste von Default-Passwörtern und deren Hash Codes ist verfügbar unter:
http://www.petefinnigan.com/default/default_password_list.htm

Motivation: Zahlreiche Default-Passwörter sind bekannt und ermöglichen den unmittelbaren Zugriff auf das System oder die Datenbank.

Für diese Anforderung sind folgende Bedrohungen relevant:

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

ID: 3.29-10/9.0

Req 11	Die Anzahl fehlgeschlagener Logins für Non-SYSDBA-Konten muss für alle existierenden Profile durch den Parameter <code>FAILED_LOGIN_ATTEMPTS</code> begrenzt werden.
--------	--

Überprüfung:
`SELECT Username, Profile FROM DBA_USERS;`
`SELECT Profile, Resource_Name, Limit FROM DBA_PROFILES`
`WHERE Resource_Name = 'FAILED_LOGIN_ATTEMPTS';`

Motivation: Die Begrenzung der Loginversuche verringert das Risiko eines Brute-Force-Angriffs auf Passwörter.

Umsetzungsbeispiel: Der Parameter `FAILED_LOGIN_ATTEMPTS` ist für alle verfügbaren Profile auf eine angemessene Zahl zu setzen.

`ALTER PROFILE <Profilname> LIMIT FAILED_LOGIN_ATTEMPTS <Zahl>;`

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.29-11/9.0

Req 12	Die Passwort Lock Time für Non-SYSDBA-Konten muss für alle existierenden Profile definiert werden.
--------	--

Überprüfung:
`SELECT Username, Profile FROM DBA_USERS;`
`SELECT Profile, Resource_Name, Limit FROM DBA_PROFILES`
`WHERE Resource_Name = 'PASSWORD_LOCK_TIME';`

Motivation: Diese Einstellung verringert die Wahrscheinlichkeit eines erfolgreichen Brute-Force-Angriffs auf Passwörter, ohne einen Denial-of-Service-Angriff auf die Konten zu ermöglichen.

Umsetzungsbeispiel: Der Administrator stellt den Parameter `PASSWORD_LOCK_TIME` für alle verfügbaren Profile z.B. auf 1/2880 Tage (= 30 Sek.).

`ALTER PROFILE <Profilname> LIMIT PASSWORD_LOCK_TIME <Zahl>;`

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.29-12/9.0

Req 13	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 14	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

Req 15	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 16	Falls Passwörter als Authentisierungsmerkmal verwendet werden, muss die Wiederverwendung bereits eingesetzter Passwörter unterbunden werden.
--------	--

Für jedes Benutzerkonto muss eine Historie der bisher genutzten Passwörter aufgezeichnet werden. Wird eine Passwort-Änderung für ein Benutzerkonto initiiert, ist das neue Passwort gegen diese Passwort-Historie abzugleichen. Bei erkannter Wiederverwendung eines Passworts muss die Passwort-Änderung abgelehnt werden. Die Umsetzung dieses Validierungsvorgangs muss im System auf Basis von technischen Maßnahmen erfolgen. Bei Verwendung eines zentralen IAM Systems für die Authentisierung der Benutzer darf die Umsetzung an das zentrale IAM System weitergereicht bzw. dorthin ausgelagert werden [vgl. Wurzel-Anforderungsdokument "3.69 IAM (Identity Access Management) - Framework"].

Generell soll mittels der Passwort-Historie sichergestellt werden, dass ein schon einmal verwendetes Passwort niemals erneut einsetzbar ist.

Aufgrund technischer Limitierungen kann eine Passwort-Historie jedoch in vielen IT/NT-Produkten nicht uneingeschränkt aufgezeichnet werden. In diesem Fall ist die folgende Grundregelung zu berücksichtigen:

- ein bereits genutztes Passwort darf für den Zeitraum von mindestens 60 Tagen nicht erneut einsetzbar sein (gemessen ab dem Zeitpunkt, an dem das betroffene Passwort durch ein anderes ersetzt wurde)
- in Systemen, in denen der Zeitraum von mindestens 60 Tagen nicht abgebildet werden kann, muss der längstmögliche Zeitraum konfiguriert werden. Zusätzlich muss durch einen Project Security Manager (PSM) bestätigt werden, dass der konfigurierte Zeitraum im Gesamtkontext des Systems noch ausreichend im Sinne der Sicherheitsanforderung ist.

Anmerkung:

Einige IT/NT-Produkte bieten keinen technischen Konfigurationsparameter an, mit dem die Passwort-Historie direkt an einen Zeitraum gebunden werden kann, sondern ermöglichen nur, die Anzahl der aufzuzeichnenden Passwörter zu definieren. In solchen Fällen darf der Zeitraum alternativ durch eine Verknüpfung der folgend beschriebenen, i. d. R. breit verfügbaren Konfigurationsparameter sichergestellt werden. Innerhalb der resultierenden Policy kann ein Benutzer nur einmal pro Tag sein Passwort ändern und aufgrund der Anzahl der aufgezeichneten Passwörter effektiv nach frühestens 60 Tagen ein altes Passwort erneut einsetzen.

- Minimum Passwort-Alter: 1 Tag
- Passwort-Historie: Aufzeichnung der letzten 60 benutzten Passwörter

In dieser Umsetzungsvariante ist zu beachten, dass das Minimum Passwort-Alter nicht mehr als einen Tag betragen sollte, um den Benutzer nicht unangemessen hinsichtlich der grundsätzlichen Notwendigkeit einzuschränken, das Passwort jederzeit selbstständig ändern zu können.

Motivation: Benutzer favorisieren in der Regel Passwörter, die sie sich gut merken können und verwenden diese in Folge oft wiederkehrend über lange Zeiträume, falls das System dies zulässt. Aus Sicht des Benutzers ist das Verhalten nachvollziehbar, führt aber effektiv zu einer erheblichen Reduzierung der Schutzwirkung dieses Authentisierungsparameters. Mit etwa entsprechenden Kenntnissen über den Benutzer oder erbeuteten Informationen aus zurückliegenden System-Kompromittierungen kann ein Angreifer so Zugriff auf vermeintlich geschützte Benutzerkonten erlangen. Insbesondere auch in Situationen, in denen im Rahmen einer akuten Risikobehandlung zentral neue Initial-

passwörter vergeben werden, die Benutzer diese jedoch unmittelbar aus Bequemlichkeit auf ein vorheriges Passwort zurückändern, bestünde hohe Gefahr, dass ein Angreifer seinen illegalen Zugriff erneut aufnehmen kann. Es ist daher wichtig zu vermeiden, dass Benutzer alte Passwörter erneut einsetzen.

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: 3.01-28/9.0

Req 17	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 18	In der Passwort-Authentisierungsdatei dürfen nur berechtigte User und SYS eingetragen sein.
--------	---

Die Passwortdatei dient der Speicherung von Benutzernamen und Passwörtern, die das SYSDBA-Privileg bzw. das SYSOPER-Privileg besitzen sollen. Durch die Passwortdatei ist eine Authentifizierung solcher Benutzer auch bei nicht laufender DB-Instanz möglich. Auf Grund dieser hohen Berechtigungen ist deren Anzahl auf eine Mindestanzahl zu begrenzen. Eine regelmäßige Kontrolle der in der Passwortdatei enthaltenen Benutzerkonten ist zu etablieren.

Überprüfung:

Der Datenbankview SYS.V\$PWFIL_ USERS zeigt die Benutzer in der Passwortdatei: SELECT Username, Sysdba, Sysoper FROM V\$PWFIL_ USERS; oder
SELECT Username, Sysdba, Sysoper FROM sys.V_\$PWFIL_ USERS;

Motivation: Minimierung der Angriffsfläche durch Minimierung der Berechtigungen.

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: 3.29-18/9.0

4.4. Least Privilege-Prinzip

Req 19	Der „Pseudo-Rolle“ PUBLIC müssen alle Rechte auf das DBMS_OBFUSCATION_TOOLKIT entzogen werden.
--------	--

Das DBMS_OBFUSCATION_TOOLKIT hat Oracle zwar durch das Paket DBMS_CRYPTO ersetzt, es wird aber trotzdem noch für bestimmte Aufgaben benötigt.

Überprüfung:

SELECT Table_Name, Owner, Grantee, Privilege FROM DBA_TAB_PRIVS
WHERE Grantee = 'PUBLIC'
AND Table_Name = 'DBMS_OBFUSCATION_TOOLKIT';

Motivation: Durch Entzug der Rechte der Rolle PUBLIC verhindert der Administrator, dass unautorisierte Anwender die Daten entschlüsseln können.

Umsetzungsbeispiel: REVOKE EXECUTE ON DBMS_OBFUSCATION_TOOLKIT FROM PUBLIC;

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: 3.29-19/9.0

Req 20	Ein Datenbankdienst darf nicht mit Root-Rechten oder anderen administrativen Rechten des Betriebssystems laufen.
--------	--

Ausnahme hierbei sind: Oracle Grid Infrastructure (ASM/RAC), z.B. ora_asm, ora_dism

Überprüfung: Prozesslisten anschauen.

Motivation: Ohne Erfüllung dieser Anforderung könnte eine Sicherheitsschwäche im Datenbankdienst zur Kompromittierung des Betriebssystems führen (z.B. durch einen Pufferüberlauf).

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Angriffe motiviert und erleichtert durch Informationspreisgabe oder erkennbare Sicherheitsschwachstellen

ID: 3.29-20/9.0

4.5. Externe Prozeduren

Req 21	Wenn der Aufruf externer Prozeduren nicht notwendig ist, muss der Konfigurationseintrag „PRO-GRAM=extproc“ aus der Datei listener.ora entfernt werden.
--------	--

Motivation: Diese Konfigurationen ermöglichen es, externe Programme unter dem Betriebssystemkonto ausführen zu lassen, unter dem die DB-Instanz läuft. Zur Absicherung des Datenbanksystems sind diese Einstellungen zu deaktivieren.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.29-21/9.0

Req 22	Falls die Funktionalität „extproc“ benötigt, so muss, zusätzlich zum normalen Datenbank-Listener, ein separater EXTPROC-Listener verwendet werden, welcher unter einem eigenen und unprivilegierten Konto läuft.
--------	--

Motivation: Es besteht die Gefahr, dass jemand eine externe Prozedur als Trojanisches Pferd einschleust und sich auf diese Weise Superuser-Privilegien zu eigen macht. Ein dedizierter Listener unter einem Betriebssystemkonto mit beschränkten Privilegien reduziert die Gefahren solch eines Angriffs.

Umsetzungsbeispiel: Der Administrator legt unter einem unprivilegiertem Benutzerkonto des Betriebssystems eine zusätzliche listener.ora an und konfiguriert darin den Eintrag für den Extproc-Listener.

Referenz:

<http://www.oracle.com/technetwork/database/security/twp-security-checklist-database-1-132870.pdf>

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

Req 23 Der Aufruf externer Prozeduren muss in der Konfigurationsdatei listener.ora auf die ausschließlich erforderlichen Funktionen beschränkt werden.

Motivation: Um einen nicht revisionssicheren Austausch der aufrufbaren externen Prozeduren zu erschweren, darf ausschließlich der EXTPROC-Listener und der Systemadministrator Zugriffsrechte auf die Verzeichnisse haben, in denen die externen Prozeduren gespeichert sind. Applikationsverantwortliche dürfen jedoch keinen Zugriff darauf haben.

Umsetzungsbeispiel: Beschränkung mit der Option EXTPROC DLLS=ONLY:DLL1:DLL2 in der Datei extproc.ora und unter Angabe des absoluten Pfads für jede erforderliche DLL (siehe http://download.oracle.com/docs/cd/E11882_01/appdev.112/e17125.pdf S.14-6).

Bei der Umsetzung sollte darauf geachtet werden, dass die Konfiguration der listener.ora (resp. extproc.ora) eine Beschränkung durch explizites Aufzählen und Benennen der zugelassenen externen Prozeduren setzt. Dies lässt sich mit der ONLY-Option bewirken, z.B. EXTPROC DLLS=ONLY:DLL1:DLL2:..., wobei diese Option dann für die erforderlichen DLLs die Angabe des absoluten Pfads erforderlich macht.

Referenz:

http://download.oracle.com/docs/cd/E11882_01/appdev.112/e17125.pdf Seite.14-6

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
- Störung der Verfügbarkeit

ID: 3.29-23/9.0

4.6. SQL-Erweiterungen mit Betriebssystem- oder Netzwerkzugriff

Req 24 Der Einsatz von Externen Jobs (local external job oder remote external job) muss auf DBA Benutzerkonten beschränkt sein.

Referenz:

http://docs.oracle.com/cd/B28359_01/server.111/b28310/schedover004.htm

Motivation: Die Funktionen ermöglichen Betriebssystemaufrufe lokal, oder auch remote auszuführen. Die Gefährdung ist darin begründet, dass mit der Funktionalität defacto ein Login auf dem Datenbankserver ersetzt wird (wird durch die Funktion selber erledigt). Daher darf diese Funktion nur an DBA Benutzerkonten vergeben 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

ID: 3.29-24/9.0

Req 25 Der Parameter UTL_FILE_DIR darf nicht verwendet werden.

Motivation: Gesonderte Zugriffsrechte auf Verzeichnisse des DB-Servers oder der darin enthaltenen Dateien sind über UTL_FILE_DIR nicht ausreichend konfigurierbar. Es bestehen bei Nutzung des Initialisierungsparameters UTL_FILE_DIR grundsätzlich für alle DB-Benutzer Schreib- und Leserechte auf die Dateien, die in den spezifizierten Verzeichnissen liegen.

Umsetzungsbeispiel: Der Verantwortliche muss den Parameter UTL_FILE_DIR aus der Datei init.ora entfernen. Will ein Anwender dennoch auf Dateien in auf dem DB-Server liegenden Verzeichnissen lesend oder schreibend zugreifen, dann müssen hierfür DB-Objekte vom Typ DIRECTORY angelegt und für den lesenden resp. schreibenden Zugriff freigegeben werden. Danach ist es möglich, Zugriffsrechte auf diese Verzeichnisse pro Benutzer oder Rolle zu vergeben. Es ist zudem unabdingbar, dass das Anlegen von Verzeichnissen, die zum Lesen und Schreiben freigegeben werden sollen, in der Hand der Systemadministratoren verbleibt. Demzufolge darf das Systemprivileg CREATE DIRECTORY ausschließlich an Systemadministratoren und auf keinen Fall an Applikationskonten vergeben 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
- Störung der Verfügbarkeit

ID: 3.29-25/9.0

4.7. Zugriffsrechte

Req 26	Der „Oracle Software Owner“ muss ein Systemkonto sein, das ausschließlich für die Administration des Datenbanksystems verwendet wird.
--------	---

Motivation: Es besteht die Gefahr einer unautorisierten und unkontrollierten Veränderung der Installation.

Umsetzungsbeispiel: Das Systemkonto „root“ oder ein anderes administratives Systemkonto darf nicht als Datenbank-Software Owner genutzt werden. In der Regel lautet das Administrationskonto für die Datenbank „oracle“.

Ausnahme: Oracle Grid Infrastructure (ASM/RAC).

Ergänzend: Umgekehrt darf dieses Systemkonto nicht auch noch gleichzeitig für die Installation anderer Produkte (z.B. Oracle HTTP Server) genutzt werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit

ID: 3.29-26/9.0

Req 27	Die Konten des Oracle Software Owners und die der (personalisierten) Administratoren müssen die einzigen Mitglieder der OS-Gruppe „dba“ in der Datei „/etc/group“ sein.
--------	---

Motivation: Zur Sicherstellung einer kontrollierten Administration sollte es nur ein Datenbankadministratorkonto oder auf andere Weise personalisierte Administratorkonten geben.

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
- Störung der Verfügbarkeit

ID: 3.29-27/9.0

Req 28	Der Oracle Software Owner muss Besitzer von \$ORACLE_HOME/bin und aller darin befindlichen Dateien sein.
--------	--

Motivation: Es besteht die Gefahr eines unkontrollierten Zugriffs bzw. einer unkontrollierten Ausführung.

Umsetzungsbeispiel: Bitte beachten: Die folgenden, ausführbaren Dateien im Verzeichnis \$ORACLE_HOME/bin emtgctl2, extjob, jssu, nmb, nmhs, nmo, oracle, oradism gehören dem Oracle Software Owner oder root und/oder haben das SUID Bit gesetzt. Dies sollten Administratoren nicht ändern.

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
- Störung der Verfügbarkeit

ID: 3.29-28/9.0

Req 29	Die Zugriffsrechte für das bin-Verzeichnis (\$ORACLE_HOME/bin) müssen auf 0755 (rwxr-xr-x) oder weniger gesetzt sein.
--------	---

Motivation: Es besteht die Gefahr des unkontrollierten Zugriffs und der unkontrollierter Ausführung aufgrund fehlerhafter oder falscher Zugriffsrechte für das Oracle bin-Verzeichnis.

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
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 3.29-29/9.0

Req 30	Der Zugriff auf Dateien, die möglicherweise schutzbedürftige Oracle-Daten enthalten, muss auf die DBA-Gruppe beschränkt werden.
--------	---

Dateien, die zu dieser Kategorie gehören, sind:

- Dateien mit Informationen zur Konfiguration und Authentisierung (z. B. init.ora, spfile.ora, snmp_ro.ora, snmp_rw.ora, catsnmp.sql, orapw<SID>, listener.ora, xsqlconfig.xml, soapConf.xml, ...)
- Net8 trace and log files
- data files
- control files
- online redo files
- archive files
- audit files

Motivation: Es besteht die Gefahr eines unautorisierten Zugriffs auf vertrauliche Informationen.

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: 3.29-30/9.0

5. Datenkommunikation

In diesem Kapitel sind diejenigen Requirements zusammengefasst, die die Abfrage aus anderen Datenbanksystemen oder den Austausch von Daten zwischen Datenbanksystemen betreffen. Dies kann einerseits über sogenannte Ad-hoc-Anfragen (Queries), andererseits über den Aufbau einer Datenverbindung zum Datenaustausch zwischen den Systemen erfolgen. Oracle realisiert Datenverbindungen zwischen Datenbanken über sogenannte Datenbank-Links (database link).

Req 31 Public Database Links dürfen nicht verwendet werden.

Motivation: Public Database Links können von jedermann genutzt werden, woraus sich ein Missbrauchspotential ergibt. Für den Fall der Fixed Database Links (= ein Benutzer mit „fixed“ Benutzername/Passwort) liegt die Missbrauchsmöglichkeit auf der Hand. Aber auch der Fall eines connected user database Links ist nicht gewollt, da ein kompromittiertes Passwort auf der Quelldatenbank sofort auch auf der entfernten Datenbank genutzt werden kann, da diese identisch sind.

Umsetzungsbeispiel: Public Database Links löschen und das Privileg CREATE PUBLIC DATABASE LINK den Besitzern entziehen.

Überprüfung:

```
SELECT Owner, Db_Link FROM DBA_DB_LINKS WHERE Owner = 'PUBLIC';  
SELECT COUNT(0), owner, db_link, username FROM sys.dba_db_links  
GROUP BY owner, db_link, username ORDER BY 1,3;
```

Dieses Statement sollte keine Zeilen mit Owner='PUBLIC' und keine Zeilen mit fehlendem Username ausweisen.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit

ID: 3.29-31/9.0

Req 32 Private Database Links müssen nur mit einer „CONNECT TO“-Klausel verwendet werden (Fixed Private Database Links).

Referenz:

http://docs.oracle.com/cd/E11882_01/server.112/e25494/ds_concepts002.htm

Überprüfung:

Bei der folgenden Ausgabe müssen alle Links einen Username eingetragen haben und der Owner darf nicht PUBLIC sein.

```
SELECT Owner, Db_Link, Username, Host FROM DBA_DB_LINKS;  
SELECT COUNT(0), owner, db_link, username FROM sys.dba_db_links  
GROUP BY owner, db_link, username ORDER BY 1,3;
```

Dieses Statement sollte keine Zeilen mit Owner='PUBLIC' und keine Zeilen mit fehlendem Username ausweisen.

Motivation: Private Database-Links ohne „CONNECT TO“-Klausel benötigen identische Benutzerkonten auf der lokalen und der entfernten Datenbank. Dadurch führt ein Kompromittieren des lokalen Datenbankkontos auch zur Kompromittierung des entfernten Benutzerkontos. Ein Private Database Link mit „CONNECT TO“-Klausel erlaubt dem lokalen Nutzer mit dem im Link benannten Nutzer auf die entfernte Datenbank zuzugreifen. Durch die Beschränkung des Links als private Link (nur der Eigentümer kann diesen verwenden) und auf den im Link bestimmten Nutzer lässt sich die Angriffsfläche reduzieren.

Umsetzungsbeispiel: Das folgende Beispiel erstellt einen Private Fixed Database Link mit dem Namen sales.us.americas.example_auto.com zur entfernten Datenbank 'sales_us'. Der aktuelle Benutzer (DB-Link- Owner) nutzt

hierfür den entfernten Benutzer scott mit seinem Passwort password.

```
CREATE DATABASE LINK sales.us.americas.example_auto.com CONNECT TO scott IDENTIFIED BY password  
USING 'sales_us';
```

Soll nun ein weiterer oder anderer Benutzer Zugriff auf die Objekte der entfernten Datenbank erhalten, so wird eine View auf die Objekte des Eigentümers erstellt und dem lokalen Benutzern die notwendigen Privilegien dafür gegeben. Somit setzt nur ein Nutzer den Datenbanklink direkt.

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: 3.29-32/9.0

6. Systemüberwachung

6.1. Protokollierung

Req 33	Die Systemzeit muss zu einer exakten Referenzzeit (Zeitnormal) synchronisiert werden.
--------	---

Als Zeitnormal ist eine Zeitgeber-Quelle heranzuziehen, die ein Zeitsignal auf Basis der koordinierten Weltzeit ("UTC" = "Universal Time Coordinated") liefert.

Anmerkung: die anhand der Zeitgeber-Quelle zu UTC synchronisierte Systemzeit darf auf dem lokalen System mittels entsprechender Zeitzonen-Konfiguration bei der Ausgabe von Zeitinformationen in die Ortszeit transformiert werden, sofern die so stattfindende Zeitzonenanpassung eindeutig erkennbar und nachvollziehbar ist.

Systeme, die zu einer gemeinsamen Sicherheits-Domäne gehören, müssen sich einheitlich an derselben Zeitgeber-Quelle synchronisieren.

Motivation: Zeitsynchronisation kann auf einem System eine technische Voraussetzung sein, um zeitkritische Abhängigkeiten in beispielsweise der Nutzung von Zertifikaten oder Authentisierungsmechanismen korrekt bedienen zu können. Dringend erforderlich sind außerdem exakte Zeitstempel in Protokollierungseinträgen, damit diese bei Sicherheitsvorfällen oder Problemanalysen in eindeutiger zeitlicher Relation auswertbar sind.

Umsetzungsbeispiel: Einige zulässige Zeitgeber-Quellen:

- vertrauenswürdig eingestuftes NTP ("NetworkTimeProtocol") Server im IP-Netzwerk
- DCF77-Funksignal über physisch angebundenes Empfängermodul
- GPS-Funksignal über physisch angebundenes Empfängermodul

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 3.01-32/9.0

Req 34	Zugriffe auf systemkritische Datenbankprozeduren und Datenbankinhalte müssen protokolliert werden.
--------	--

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.

Motivation: Für einen nachvollziehbaren Betrieb einer Datenbank ist eine Protokollierung wichtiger Betriebsinformationen notwendig. Hierzu zählt z. B. das Erfassen von erfolglosen Login-Versuchen, um mögliche Einbruchsversuche zu entdecken.

Umsetzungsbeispiel: Mit Hilfe von Oracle Auditing und der Implementierung von Triggern können nahezu beliebig Zugriffe protokolliert werden.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Abstreiten von durchgeführten Aktionen

ID: 3.29-34/9.0

Req 35	Database Event Trigger dürfen nicht Applikationsobjekte jeglicher Art enthalten. Nur die im Dictionary Schema „SYS“ gespeicherten Prozeduren dürfen aus dem Database Event Trigger heraus aufgerufen werden.
--------	--

Motivation: Ist eine Applikationsprozedur in einem Database Event Trigger enthalten, besteht die Gefahr, dass ein sachkundiger und böswilliger Benutzer einen solchen Trigger ausnutzt, indem er den Prozess-Code manipuliert und seine Benutzerrechte erweitert.

Für diese Anforderung sind folgende Bedrohungen relevant:

- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen

ID: 3.29-35/9.0

Req 36	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 An-

griffe 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 37	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 38	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 39	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 Vereinba-

rungen 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 40	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 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 41	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 42	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

7. Oracle-spezifische Anforderungen

Zusätzlich zu den aus den allgemeinen Datenbanksicherheitsanforderungen abgeleiteten Sicherheitsanforderungen sind die nachfolgend aufgeführten, herstellerspezifischen Anforderungen zu berücksichtigen.

Nachfolgend wird unter dem Begriff „DBA User“, bzw. „DBA Account“ ein Datenbank-Konto/Account verstanden, das DBA (Datenbankadministrator) Berechtigungen hat oder DBA-nahe Tätigkeiten nach dem Funktionstrennungsprinzip (z.B. Benutzerverwaltung, Backup, etc.) wahrnimmt.

7.1. Authentifizierung

Req 43	Es muss sichergestellt sein, dass die Funktion „Proxy Authentication“ nur an technische Accounts und nicht an Accounts natürlicher Personen vergeben wird.
--------	--

Referenzen:

<http://www.oracle.com/technetwork/database/security/index-092912.html>

http://docs.oracle.com/cd/E11882_01/java.112/e16548/proxya.htm

<http://www.databasejournal.com/features/oracle/article.php/3910651/Using-Proxy-Authentication-Methods-in-Oracle-Database-11g.htm>

Motivation: Die Funktion Proxy Authentication wird typischerweise im Zusammenspiel mit Web- und Applicationservern genutzt und ermöglicht es diesen mit einer einzelnen Datenbankverbindung eine Vielzahl von Benutzer-Anmeldungen und -Sitzungen zu handhaben. Der Web- bzw. Applicationserver als „Vertreter“ meldet mit seinem Proxy-Account den Benutzer an der Datenbank an. Somit arbeitet jeder Benutzer der Webanwendung mit dem eigenen individuellen Oracle Account und den damit verbundenen Rechten auf der Datenbank und nicht mit dem globalen technischen Account des Web- bzw. Applicationserverns.

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: 3.29-43/9.0

Req 44	Die Betriebssystemauthentifizierung muss für alle Non-DBA- und nicht operativen Benutzer, die keinen automatischen Login vom Betriebssystem aus benötigen, deaktiviert werden.
--------	--

Überprüfung:

OS-Gruppe dba auf unerwünschte Mitglieder überprüfen.

Nutzer der folgenden Abfrage überprüfen:

```
SELECT Username FROM DBA_USERS
```

```
WHERE PASSWORD = 'EXTERNAL';
```

Motivation: Die Datenbanksicherheit sollte so wenig wie möglich von der Sicherheit des zugrundeliegenden Betriebssystems abhängen.

Umsetzungsbeispiel: Die Mitgliederanzahl in der Betriebssystemgruppe DBA ist zu beschränken. Der Modus IDENTIFIED EXTERNALLY ist nicht in Benutzerprofilen zu verwenden. Konten, die nicht für betriebliche Zwecke verwendet werden und für die kein automatischer Login über das Betriebssystem erforderlich ist (z. B. für Backup), dürfen keine Kontonamen mit dem OS_AUTHENT_PREFIX haben. Der Default-Wert für OS_AUTHENT_PREFIX ist OPS\$.

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: 3.29-44/9.0

Req 45 Die Benutzeranmeldung durch eine externe (remote) Betriebssystem-Authentisierung muss deaktiviert werden.

Motivation: Oracle bietet die Möglichkeit, einer externen (remote) Betriebssystemauthentifizierung für die Benutzeranmeldung zu vertrauen. Da dem Remote-System nicht vertraut werden kann, müssen diese Optionen auf FALSE gesetzt sein.

Umsetzungsbeispiel: Die Parameter in der Konfigurationsdatei init.ora müssen Administratoren wie folgt setzen:

REMOTE_OS_AUTHENT=FALSE

REMOTE_OS_ROLES=FALSE

Bei Oracle 11g ist die Default-Einstellung FALSE.

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
- Unbemerkt durchführbare Angriffe

ID: 3.29-45/9.0

Req 46 Datenbankrollen dürfen nicht über das Betriebssystem vergeben werden.

Motivation: Oracle bietet die Möglichkeit, die Benutzerrollen der Datenbank durch das Betriebssystem verwalten zu lassen. Diese Möglichkeit birgt Sicherheitsrisiken; daher muss der Verantwortliche diese Funktion deaktivieren. Die Aufgaben und Zuständigkeiten von DBA- und Betriebssystem-Administration müssen getrennt sein.

Umsetzungsbeispiel: Der Default-Wert FALSE des Parameters „OS_ROLES“ in init.ora darf nicht geändert 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

ID: 3.29-46/9.0

7.2. Listener- und Netzwerkverbindung

Req 47 Der Zugriff auf den TNS Listener muss durch technische Maßnahmen auf berechnete Rechner begrenzt werden.

Für die Begrenzung des Zugriffs auf berechnete Rechner stehen verschiedene technische Möglichkeiten zur Verfügung.

Dynamische IP Adresse

Für Rechner mit dynamischer IP Adresse wird der Zugang über einen Secure Jumpservice/ Terminalserver oder eine zertifikatsbasierte Authentisierung gefordert, da eine Zugriffsbeschränkung auf IP Ebene nicht mehr zur Verfügung steht.

Feste IP Adresse

Für Rechner mit fester IP Adresse kann die Zugriffsbeschränkung mit Hilfe von Oracle Valid Node Checking, Access Control-Listen (ACLs) und Netzwerk- oder Host-basierenden Firewall-Systemen erfolgen.

Motivation: Durch Zugriffsbeschränkung auf berechnete Rechner, wird die Möglichkeit von Angriffen auf das Datenbanksystem drastisch reduziert.

Umsetzungsbeispiel: Umsetzungsbeispiel Oracle Valid Node Checking:

Für das Oracle Valid Node Checking sind der Konfigurationsdatei sqlnet.ora des Listeners (bei älteren Systemen protocol.ora) folgende Zeilen hinzuzufügen:

TCP.VALIDNODE_CHECKING = YES

TCP.INVITED_NODES = (<host_1>, <host_2>, ...)

(Der Wert für <host_x> entweder eine IP-Adresse oder ein DNS-Name)

Bitte beachten: TCP.INVITED_NODES hat Vorrang vor TCP.EXCLUDED_NODES. Außerdem sollte der Oracle Listener durch den IP-Filter des Betriebssystems geschützt 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

ID: 3.29-47/9.0

Req 48	Der TNS Listener muss vor unautorisierter Konfiguration geschützt werden.
--------	---

Die Absicherung des TNS Listeners vor unautorisierter Konfiguration erfolgt durch das Einfügen des Parameters ADMIN_RESTRICTIONS_<listenername>=ON in die Konfigurationsdatei listener.ora.

Referenzen:

Listener Control Utility

http://docs.oracle.com/cd/B28359_01/network.111/b28317/lsnrctl.htmOracle Corporation: Security Guide, 11g Release 2 (11.2)

http://docs.oracle.com/cd/E14072_01/network.112/e10574.pdf

Integrity: White Paper "Oracle Database Listener Security Guide", April 2007,

http://www.integrity.com/security-resources/whitepapers/Integrity_Oracle_Listener_TNS_Security.pdf

Motivation: Es muss verhindert werden, dass Unbefugte den Listener neu konfigurieren können, da dies Auswirkungen auf die Sicherheit des Datenbanksystems hat.

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
- Störung der Verfügbarkeit

ID: 3.29-48/9.0

7.3. Privilegien für Benutzer und Rollen

Req 49	Es muss sichergestellt werden, dass keine Datenbankprivilegien für Applikationsobjekte an die Benutzergruppe PUBLIC vergeben werden.
--------	--

Überprüfung:

```
SELECT table_name, owner, privilege
```

```
from dba_tab_privs
```

```
where grantee = 'PUBLIC'
```

```
and owner not in ('SYS','SYSTEM','OUTLN','DBSNMP');
```

Der Ausschluss weiterer dem Systembereich zuzuordnender Benutzerkonten (wie z.B. XDB,CTXSYS, WMSYS,...) ist ggf. notwendig, wenn diese Komponenten installiert sein sollten.

Motivation: Die Vergabe von Privilegien für Applikationsobjekte an „PUBLIC“ verletzt das „need-to-Know“-Prinzip und

erhöht das Missbrauchsrisiko durch Freigabe von Ressourcen und Funktionalität, die nicht global benötigt wird. Das Berechtigungskonzept einer Applikation kann auch nur dann als seriös eingestuft werden, wenn die Zugriffe auf Applikationsressourcen oder -funktionalität nur dediziert eingeräumt und nicht pauschal via „PUBLIC“ vergeben werden.

Eine Überprüfung der an PUBLIC vergebenen Rechte kann immer nur für Applikationsobjekte sinnvoll sein und nicht für Objekte, die sich im Data Dictionary befinden.

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: 3.29-49/9.0

Req 50 Der Parameter O7_DICTIONARY_ACCESSIBILITY muss auf FALSE gesetzt werden.

Motivation: Ist der Initialisierungsparameter O7_DICTIONARY_ACCESSIBILITY auf FALSE gesetzt (Defaultwert seit Oracle 9i), so ist kein Zugriff mehr auf Dictionary-Objekte durch ANY-Privilegien möglich.

Umsetzungsbeispiel: Ist ein Zugriff auf Dictionary-Objekte (z. B. für Applikationen und Tools) notwendig, so muss der Administrator die Objektprivilegien für den Zugriff auf diese Dictionary-Objekte individuell vergeben.

Das Privileg GRANT ALL OBJECT PRIVILEGES beinhaltet nicht die Möglichkeit, z.B. das Select-Privileg für die Dictionary View dba_users zu vergeben.

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: 3.29-50/9.0

Req 51	Non-DBA-Benutzer dürfen nicht über Objektprivilegien (unmittelbar oder über Rollen) für folgende Objekte verfügen: • AUD\$ • ALL_SOURCE • DBA_AUDIT_TRAIL • DBA_ROLE_PRIVS • DBA_SYS_PRIVS • DBA_TAB_PRIVS • DBA_USERS • DBMS_FILE_TRANSFER • DBMS_IJOB • DBMS_ISCHED • DBMS_SYS_SQL • DBMS_NETWORK_ACL_ADMIN • DBA_USERS_WITH_DEFPWD • FGA_LOG\$ • LINK\$ • USER\$ • USER_HISTORY\$
--------	---

Motivation: Die genannten Views und Pakete erlauben entweder Zugriff auf vertrauliche Informationen (z. B. Passwordhash in LINK\$) oder die Ausführung von potentiell gefährlichen Aktionen (z. B. Versenden von E-Mails aus der Datenbank mit UTL_MAIL).

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: 3.29-51/9.0

Req 52 Non-DBA-Benutzerkonten dürfen nicht eine der folgenden Rollen besitzen (direkt oder indirekt):

- AQ_ADMINISTRATOR_ROLE
- DATAPUMP_IMP_FULL_DATABASE
- DBFS_ROLE
- DBA
- DELETE_CATALOG_ROLE
- EXECUTE_CATALOG_ROLE
- EXP_FULL_DATABASE
- GATHER_SYSTEM_STATISTICS
- IMP_FULL_DATABASE
- LOGSTDBY_ADMINISTRATOR
- OEM_MONITOR
- OEM_ADVISOR
- RECOVERY_CATALOG_OWNER
- SCHEDULER_ADMIN
- SNMPAGENT
- SELECT_CATALOG_ROLE

Motivation: Diese Rollen verfügen über kritische Objekt- und/oder Systemprivilegien. So umfasst beispielsweise die Rolle DATAPUMP_IMP_FULL_DATABASE, ein Systemprivileg, das es ermöglicht, jedwedem Privileg an jedermann vergeben zu können.

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: 3.29-52/9.0

8. Technischer Basisschutz von IT-/NT-Systemen

8.1. Authentifizierung und Autorisierung

Req 53	Die Nutzung von schutzbedürftigen Funktionen des Systems sowie der Zugriff auf interne oder vertrauliche Daten darf nicht ohne vorhergehende Authentifizierung und Autorisierung ermöglicht werden.
--------	---

Die Nutzung von schutzbedürftigen Funktionen des Systems sowie der Zugriff auf Daten, die als intern oder vertraulich eingestuft sind, darf erst nach einer eindeutigen Identifizierung und erfolgreichen Authentifizierung des Benutzers anhand eines Benutzerkontos ermöglicht werden. Ein Benutzerkonto besteht aus einem eindeutigen Benutzernamen und zugehörigen Authentisierungsmerkmalen. Zudem muss verifiziert werden, dass der Benutzer innerhalb der ihm im System zugeordneten Benutzerrolle für den Zugriff auf die betroffenen Funktionen und Daten legitimiert ist.

Eine Ausnahme hiervon sind Funktionen und Daten, die uneingeschränkt öffentlich genutzt werden dürfen; beispielsweise der Bereich einer Web-Seite im Internet, in dem nur öffentliche Informationen bereitgestellt werden.

Beispiele für Funktionen, die eine vorhergehende Authentifizierung erfordern:

- Fernzugriff auf Netzdienste (wie SSH, SFTP, Web-Dienste)
- lokaler Zugriff auf die Management-Konsole
- lokale Nutzung von Betriebssystem und Anwendungen

Diese Anforderung gilt ohne Einschränkung auch für jegliche maschinellen Zugriffe auf das System (Hier erfolgt die Umsetzung in der Regel durch den Einsatz von sogenannten "technischen Benutzerkonten", auch "Machine-2-Machine" oder "M2M"-Konten genannt).

Motivation: Die eindeutige Authentifizierung und Autorisierung von Zugriffen auf ein System sind elementar, um Funktionen und Daten vor Missbrauch zu schützen.

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: 3.01-19/9.0

Req 54	Benutzerkonten müssen mit mindestens zwei Authentisierungsmerkmalen aus unterschiedlichen Faktoren geschützt werden.
--------	--

Sämtliche Benutzerkonten des Systems müssen vor einer unberechtigten Nutzung geschützt werden. Dies ist durch Verwendung von Authentisierungsmerkmalen umzusetzen, die eine eindeutige Identifizierung des legitimen Benutzers ermöglichen.

Authentisierungsmerkmale werden in übergeordneten Gruppen, sogenannten "Faktoren", differenziert:

- Faktor WISSEN: "etwas, das nur der legitime Benutzer weiss"
- Faktor BESITZ: "etwas, das nur der legitime Benutzer besitzt"
- Faktor INHÄRENZ: "etwas, das nur der legitime Benutzer ist"

Es müssen mindestens zwei Authentisierungsmerkmale miteinander kombiniert werden.

Diese müssen aus unterschiedlichen Faktoren stammen ("Multi-Faktor-Authentisierung"; kurz: "MFA").

Eine Kombination von Authentisierungsmerkmalen desselben Faktors (Beispiel: zwei unterschiedliche PINs) ist nicht

zulässig.

Beispiele für zulässige Authentisierungsmerkmale

- aus dem Faktor WISSEN: PINs, Passphrases (Passwörter*)
- aus dem Faktor BESITZ: Smartcards, FIDO2 Level 2 Security Keys, Device-bound Passkeys, in einem TPM/HSM gespeicherte kryptografische Schlüssel, OTPs (One-Time Passwords) generiert in einer zum Einsatz in der Deutschen Telekom freigegebenen Authenticator App
- aus dem Faktor INHÄRENZ: biometrische Merkmale wie Fingerabdruck, Iris- bzw. Retina-Scans, Gesichtserkennung

***) Wichtiger Hinweis zum Einsatz von Passwörtern**

Passwörter müssen als Authentisierungsmerkmal strikt vermieden werden.

Sie sind nur dann zulässig, falls sicherere Alternativen nicht umgesetzt werden können.

Grundsätzlich nicht zulässig sind Authentisierungsmerkmale, die leicht gefälscht oder manipuliert werden können.

Dazu gehören:

- Rufnummern und Anrufer-IDs
- IP-Adressen
- geografische Standorte
- VPN-Zugehörigkeiten und Netzwerkinformationen
- Status von Clients, etwa von Arbeitsplatzsystemen oder mobilen Endgeräten

Hinweis zu technischen Benutzerkonten

Für den maschinellen Zugriff eingesetzte technische Benutzerkonten (auch unter dem Begriff "Machine-to-Machine" bzw. "M2M"-Konten bekannt) sind von der Verpflichtung zur Multi-Faktor-Authentisierung ausgenommen, da eine solche dort i.d.R. nicht umsetzbar ist.

Motivation: Benutzerkonten, die nicht über angemessene Authentisierungsmerkmale geschützt sind, können von einem Angreifer missbraucht werden, um unberechtigt auf ein System und die darauf gespeicherten Daten und Anwendungen zuzugreifen. Aufgrund vielfältiger gängiger Angriffsmethoden ist der Schutz von Benutzerkonten durch ein einzelnes Authentisierungsmerkmal mittlerweile als schwach zu bewerten, insbesondere, falls hier das klassische Passwort zum Einsatz kommt. Eine Kombination von Authentisierungsmerkmalen aus unterschiedlichen Faktoren erhöht die Sicherheit für Benutzerkonten signifikant.

Umsetzungsbeispiel: Beispiele für MFA

MFA Kombination	Beschreibung	Anmerkung zur Anwendung
Telekom "myCard" plus PIN-Eingabe	1. Faktor: in Hardware implementiertes Zertifikat ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)
FIDO2 Level 2 Security Key plus Fingerabdruck	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: Biometrisches Merkmal ("Inhärenz")	Die Biometrie-Funktion muss vorab konfiguriert werden, da der Biometrie-Sensor sonst nur als "Taste" funktioniert und somit der 2. Faktor ("Inhärenz") nicht gegeben wäre.
Device-bound Passkey in WH4B* auf Nucleus PC plus PIN	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)

Device-bound Passkey in Secure Enclave auf iOS Device plus FaceID	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: Biometrisches Merkmal ("Inhärenz")	(keine)
Passwort plus freigegebene OTP App (z. B. MS Authenticator)	1. Faktor: Passwort ("Wissen") 2. Faktor: spezifisch generiertes One Time Password ("Besitz")	Passwörter sind nur dann zulässig, falls sicherere Alternativen nicht umgesetzt werden können. Die Synchronisation der Authenticator App über einen Clouddienst sowie das Teilen (z. B. über einen Passwortmanager) des OTP ist nicht zulässig.

*) WH4B: "Windows Hello for Business"

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: 3.01-20/9.0

Req 55 Privilegierte Benutzerkonten müssen mit mindestens zwei Authentisierungsmerkmalen geschützt werden, die aus unterschiedlichen Faktoren stammen und erhöhte Resilienz gegen Phishing-Angriffe bieten.

Ein privilegiertes Benutzerkonto ist ein Benutzerkonto, welches über erweiterte Berechtigungen innerhalb eines Systems verfügt. Erweiterte Berechtigungen ermöglichen einen Zugriff auf Konfigurationseinstellungen, Funktionen oder Datenbestände, der regulären Benutzern des Systems nicht zu Verfügung steht. In direkter Abhängigkeit zu den besonderen Aufgaben, die mittels eines privilegierten Benutzerkontos innerhalb eines Systems wahrgenommen werden, können die zugewiesenen erweiterten Berechtigungen spezifisch limitiert sein oder einen vollständig uneingeschränkten Systemzugriff umfassen.

Beispiele für privilegierte Benutzerkonten:

- Konten für Administrations-, Wartungs- oder Entstörungsaufgaben
- Konten für Benutzer-Verwaltungsaufgaben (z. B. Anlegen/Löschen von Benutzern; Zuweisen von Berechtigungen; Passwort-Rücksetzungen)
- Konten, die zur Freigabe, Auslösung oder Unterbindung von geschäftskritischen Vorgängen berechtigt sind
- Konten mit Zugriff auf Daten, die im Interesse des DTAG-Konzerns, dessen Kunden oder der Öffentlichkeit als SCD (Sensitive Customer Data) eingestuft sind
- Konten, die in hohem Umfang auf lt. EU-DSGVO als „personenbezogen“ definierte Daten zugreifen können (z. B. Massenabruf von größeren Teilen oder des vollständigen Datenbestands)

Zum Schutz privilegierter Konten müssen mindestens zwei Authentisierungsmerkmale miteinander kombiniert werden.

Diese müssen aus unterschiedlichen Faktoren ("WISSEN", "BESITZ" oder "INHÄRENZ") stammen.

Eine Kombination von Authentisierungsmerkmalen desselben Faktors ist nicht zulässig.

Mindestens eines der Authentisierungsmerkmale darf nicht anfällig gegenüber Phishing-Angriffen sein.

Bei einem Phishing-Angriff wird der legitime Nutzer trickreich manipuliert, um seine Anmeldedaten dem Angreifer of-

fenzulegen, beispielsweise mittels gefälschter Anmelde-Seiten. Ein Phishing-Angriff kann auch gegen eine Kombination aus mehreren Authentisierungsmerkmalen erfolgen.

Phishing-resiliente Authentisierungsmerkmale verhindern Angriffe anhand ihrer technischen Umsetzung. Diese Authentisierungsmerkmale nutzen kryptographische Verfahren und stellen eine starke Bindung zwischen dem Nutzer, dem Gerät und dem Dienst her. Sie erfordern während der Authentisierung zusätzlich eine manuelle Nutzerinteraktion, die nicht automatisiert werden kann; beispielsweise, einen Fingerabdruck-Scan an einem Hardware Token abzugeben.

Als nicht anfällig gegenüber Phishing-Angriffen gelten

- FIDO2 Level 2 Security Keys
- in Hardware implementierte Zertifikate

Wichtiger Hinweis zum Einsatz von Passwörtern

Passwörter müssen als Authentisierungsmerkmal strikt vermieden werden.

Sie sind nur dann zulässig, falls sicherere Alternativen nicht umgesetzt werden können.

Hinweis zu technischen Benutzerkonten

Für den maschinellen Zugriff eingesetzte technische Benutzerkonten (auch unter dem Begriff "Machine-to-Machine" bzw. "M2M"-Konten bekannt) sind von der Verpflichtung zur Multi-Faktor-Authentisierung ausgenommen, da eine solche dort i.d.R. nicht umsetzbar ist.

Motivation: Privilegierte Benutzerkonten stellen ein erhöhtes Risiko für die Sicherheit eines Systems dar. Kompromittiert ein Angreifer erfolgreich ein solches Benutzerkonto, erhält er weitreichende Berechtigungen, mit denen er das System oder Systemanteile unter seine Kontrolle bringen, die Systemfunktionen stören, verarbeitete Daten einsehen/manipulieren oder geschäftskritische Vorgänge beeinflussen kann. Die Kombination von mehreren Authentisierungsmerkmalen unterschiedlicher Art minimiert das Risiko der Kompromittierung eines Benutzerkontos bereits signifikant, jedoch muss für privilegierte Benutzerkonten in besonderem Maße auf Resilienz gegen Phishing-Angriffe geachtet werden. Die zu beobachtenden Phishing-Angriffe werden zunehmend trickreicher und für Nutzer schwerer zu erkennen, so dass eine Multifaktor-Authentifizierung ohne erhöhte Resilienz gegen Phishing nicht mehr als ausreichend für privilegierte Benutzerkonten zu bewerten ist.

Umsetzungsbeispiel: Beispiele für MFA mit erhöhter Resilienz gegen Phishing-Angriffe

MFA Kombination	Beschreibung	Anmerkung zur Anwendung
Telekom "myCard" plus PIN-Eingabe	1. Faktor: in Hardware implementiertes Zertifikat ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)
FIDO2 Level 2 Security Key plus Fingerabdruck	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: Biometrisches Merkmal ("Inhärenz")	Die Biometrie-Funktion muss vorab konfiguriert werden, da der Biometrie-Sensor sonst nur als "Taste" funktioniert und somit der 2. Faktor ("Inhärenz") nicht gegeben wäre.
FIDO2 Level 2 Security Key plus PIN-Eingabe	1. Faktor: in Hardware gespeicherter Crypto-Schlüssel ("Besitz") 2. Faktor: PIN ("Wissen")	(keine)

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

Req 56 Benutzerkonten müssen die eindeutige Identifizierung des Benutzers sicherstellen.

Benutzer müssen eindeutig von einem System identifiziert werden können.

Dies wird typischerweise dadurch erreicht, dass für jeden Benutzer ein individuelles Benutzerkonto genutzt wird.

Sogenannte Gruppenkonten, die sich dadurch auszeichnen, dass sie von mehreren Personen gemeinsam genutzt werden, dürfen nicht verwendet werden. Dies gilt uneingeschränkt auch für privilegierte Benutzerkonten. Die meisten Systeme verfügen nach der Grundinstallation zunächst nur über ein einzelnes Benutzerkonto mit administrativen Berechtigungen. Soll das System von mehreren Personen administriert werden, muss jede dieser Personen ein persönliches, individuelles Benutzerkonto verwenden, dem entsprechende administrative Berechtigungen bzw. Rollen zugewiesen sind.

Eine Besonderheit stellen sogenannte technische Benutzerkonten dar. Diese werden für Authentifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt und können damit nicht einer konkreten Person zugewiesen werden. Solche Benutzerkonten müssen individuell pro System oder pro Anwendung vergeben werden. Hierbei ist allerdings sicherzustellen, dass eine missbräuchliche Nutzung solcher Benutzerkonten nicht möglich ist.

Möglichkeiten, um eine missbräuchliche Nutzung solcher Benutzerkonten durch Personen zu verhindern, sind:

- Konfiguration eines den Sicherheitsanforderungen entsprechenden Passwortes, dass nur einem kleinstmöglichen Kreis von Administratoren bekannt ist.
- Konfiguration des entsprechenden Benutzerkontos, so dass dieses nur lokal verwendet werden kann und eine interaktive Anmeldung nicht möglich ist.
- Verwendung eines Verfahrens mit öffentlichem und privatem Schlüssel oder Zertifikaten für die Authentifizierung des entsprechenden Benutzerkontos.
- Einschränkung des Zugriffs über ein Netz auf legitimierte Systeme.

Weitere Lösungen sind im Einzelfall auf ihre Verwendbarkeit zu prüfen.

Motivation: Die eindeutige Identifizierung eines Benutzers ist Voraussetzung, um einem Benutzer Berechtigungen zuweisen zu können, die für die Durchführung seiner Aufgaben auf dem System notwendig sind. Nur so kann eine adäquate Zugriffskontrolle auf Daten und Dienste eines Systems erreicht und der missbräuchliche Zugriff verhindert werden. Des Weiteren wird hierdurch ermöglicht, dass Tätigkeiten und Aktionen auf einem System protokolliert und einem Benutzer zugeordnet werden können.

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

Req 57 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 aus-

geführt 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