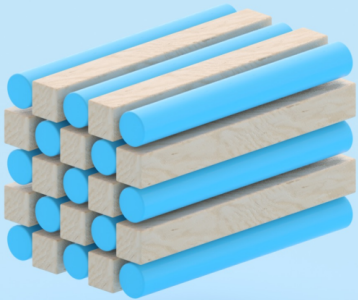
Sicherer PostgreSQL-Betrieb

Nach BSI-Grundschutz

NetApp



Michael Banck <michael.banck@netapp.com>
Postgres Team Lead
PGConf.DE 2023

© 2023 Netapp, Inc. Alle Rechte vorbehalten.

BSI IT-Grundschutz

`www.bsi.bund.de/grundschutz`

© 2023 Netapp, Inc. Alle Rechte vorbehalten.

BSI IT-Grundschutz

”Als IT-Grundschutz bezeichnet die Bundesverwaltung eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Vorgehensweise zum Identifizieren und Umsetzen von Sicherheitsmaßnahmen der unternehmenseigenen Informationstechnik (IT).”

`https://de.wikipedia.org/wiki/IT-Grundschutz`

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Alternative internationale Konzepte

- PCI Compliance
- Common Criteria
- DISA STIG

UNCLASSIFIED

PostgreSQL 9.x Security Technical Implementation Guide

Version: 1

20 Jan 2017

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

BSI IT-Grundschutz

- Üblicherweise ein Konzern/Behörden-weites Projekt
  - Projekt-Team
  - Externe Unterstützung/Schulung
- Verschiedene (teils jährlich wieder kehrende) Phasen
  - Planungs-Phase, Schutzbedarfsfeststellung
  - Konzepterstellungs-Phase
  - Umsetzungs- und Dokumentations-Phase
  - Auditierung (von Teilen)
  - Zertifizierung (von Teilen)
- DBAs sind als Teil des Projekts in bestimmte relevante Bausteine eingebunden
- Evtl. Zusammenarbeit mit Kunden (insbesondere wenn Zertifizierung von diesen verlangt)

© 2023 Netapp, Inc. Alle Rechte vorbehalten.

ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung:

”Die Institutionsleitung MUSS die Gesamtverantwortung für Informationssicherheit in der Institution übernehmen. Dies MUSS für alle Beteiligten deutlich erkennbar sein. Die Institutionsleitung MUSS den Sicherheitsprozess initiieren, steuern und kontrollieren. Die Institutionsleitung MUSS Informationssicherheit vorleben.”

”Die Institutionsleitung MUSS die Zuständigkeiten für Informationssicherheit festlegen. Die zuständigen Mitarbeitenden MÜSSEN mit den erforderlichen Kompetenzen und Ressourcen ausgestattet werden.”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

BSI IT-Grundschutz

- Elementare Gefährdungen
- Bausteine
- Gefährdungslage
- Anforderungen (Maßnahmen)
  - Basis-Anforderungen (MUSS)
    - Unbedingt erforderlich
  - Standard-Anforderungen (SOLLTE)
    - Normalerweise umzusetzen
    - Gründe können dagegen sprechen
    - Sorgfältige Abwägung und Begründung
  - Anforderungen bei erhöhtem Schutzbedarf
- Umsetzungshinweise

© 2023 Netapp, Inc. Alle Rechte vorbehalten.

Bausteine

IT-Grundschutz in verschiedene Bausteine aufgeteilt

- ISMS: Sicherheitsmanagement
- ORP: Organisation und Personal
- CON: Konzeption und Vorgehensweise
- OPS: Betrieb
- DER: Detektion und Reaktion
- APP: Anwendungen
- SYS: IT-Systeme
- IND: Industrielle IT
- NET: Netze und Kommunikation
- INF: Infrastruktur

© 2023 Netapp, Inc. Alle Rechte vorbehalten.

Bausteine

Für relationale Datenbanken relevante Unter-Bausteine:

- ORP.4 Identitäts- und Berechtigungsmanagement
- CON.3 Datensicherungskonzept
- OPS.1.1.2 Ordnungsgemäße IT-Administration
- OPS.1.1.3 Patch- und Änderungsmanagement
- OPS.1.1.5 Protokollierung
- OPS.1.2.2 Archivierung
- OPS.2.2 Cloud-Nutzung
- DER.3.1 Audits und Revisionen
- DER.4 Notfallmanagement
- APP.4.3 Relationale Datenbanksysteme

© 2023 Netapp, Inc. Alle Rechte vorbehalten.

Bausteine

Für relationale Datenbanken relevante Unter-Bausteine:

- ORP.4 Identitäts- und Berechtigungsmanagement
- CON.3 Datensicherungskonzept
- OPS.1.1.2 Ordnungsgemäße IT-Administration
- OPS.1.1.3 Patch- und Änderungsmanagement
- OPS.1.1.5 Protokollierung
- OPS.1.2.2 Archivierung
- OPS.2.2 Cloud-Nutzung
- DER.3.1 Audits und Revisionen
- DER.4 Notfallmanagement
- APP.4.3 Relationale Datenbanksysteme

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Schutzbedarf

- Verletzung der Grundwerte
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
- Auswirkung auf Aufgabenerfüllung und Geschäftstätigkeit bei Vorfällen/Risiken
- Drei Stufen der Schadensauswirkung
  - Normal - begrenzt und überschaubar
  - Hoch - möglicherweise beträchtlich
  - Sehr Hoch - möglicherweise existentiell bedrohlich, katastrophal
- Im Allgemeinen normaler Schutzbedarf
- Schutzbedarfsfeststellung

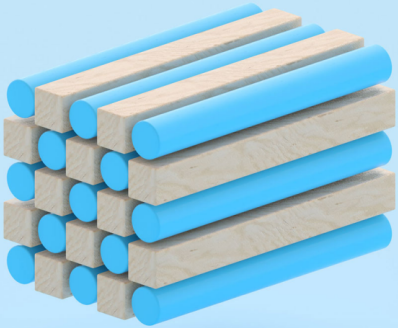
 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Planung und Umsetzung

- Modellierung des Schutzbedarfs aller Komponenten, Maximalprinzip
- Entwickeln konkreter Sicherheitsmaßnahmen
  - Dokumentation, warum Maßnahmen ausreichend sind
  - Sortierung der Maßnahmen nach Priorität
  - Umsetzungsplan aufführen
  - Verantwortliche definieren - wer ist verantwortlich für deren
    - Initialisierung
    - Umsetzung
    - Kontrolle (z.B. Audit)
    - Revision
- Umsetzung zeitnah garantiert? Kontrolliert und protokolliert?
- Angemessenheits- und Wirtschaftlichkeits-Betrachtung
  - Wie teuer sind welche Maßnahmen?
  - Ist das sinnvoll? Wer hat die Entscheidung notfalls zu verantworten?

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Generelle Betrachtungen



 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

APP 4.3.1.3. Abgrenzung und Modellierung

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

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Baustein APP.4.3 “Relationale Datenbanksysteme”

Gefährdungslage

- 2.1 Unzureichende Dimensionierung der Systemressourcen
- 2.2 Aktivierte Standard-Konten
- 2.3 Unverschlüsselte Datenbankanbindung
- 2.4 Datenverlust in der Datenbank
- 2 5 Integritätsverlust der gespeicherten Daten
- 2.6 SQL-Injections
- 2.7 Unsichere Konfiguration des Datenbankmanagementsystems
- 2.8 Malware und unsichere Datenbank-Skripte

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Betriebshandbuch

OPS.1.1.1.A3 Erstellen von Betriebshandbüchern für die betriebene IT:

”Für alle betriebenen IT-Komponenten SOLLTEN die Betriebsaufgaben geplant und in Betriebshandbüchern erfasst werden. Die Betriebshandbücher SOLLTEN stets verfügbar sein [...]. Die Betriebshandbücher SOLLTEN regelmäßig und anlassbezogen geprüft und angepasst werden.”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Betriebshandbuch

- Beschreibung der Arbeitsabläufe
- Am Besten keine dynamischen Daten (aktuelle Liste der Datenbanken o.ä.)
- Bestimmte Bereiche (z.B. Monitoring) können ausgelagert sein
- Checklisten für übliche Arbeitsabläufe
  - Installation/Entfernung von Instanzen
  - Falls kein Konfigurations-Management vorhanden

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Benötigte Konzepte

ISMS.1.A10 Erstellung eines Sicherheitskonzepts:

”Für den festgelegten Geltungsbereich (Informationsverbund) SOLLTE ein angemessenes Sicherheitskonzept als das zentrale Dokument im Sicherheitsprozess erstellt werden.”

CON.3.A1 Erhebung der Einflussfaktoren für Datensicherungen:

”Der IT-Betrieb MUSS für jedes IT-System und darauf ausgeführten Anwendungen die Rahmenbedingungen für die Datensicherung erheben. Dazu MÜSSEN die Fachverantwortlichen für die Anwendungen ihre Anforderungen an die Datensicherung definieren.

CON.3.A2 Festlegung der Verfahrensweisen für die Datensicherung:

Der IT-Betrieb MUSS Verfahren festlegen, wie die Daten gesichert werden.”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Benötigte Konzepte

Grundlegend und Übergeordnet

- Sicherheitskonzept

Nötig

- Benutzer- und Berechtigungskonzept
- Datensicherungskonzept
- Protokollierungskonzept

Sinnvoll

- Logauswertungskonzept
- Monitoringkonzept

© 2023 Netapp, Inc. Alle Rechte vorbehalten.

Trennung der Arbeitsbereiche

- Technische DBAs (TDBAs):
  - Einrichtung Server, Instanzen, Backups
  - Erstellung Nutzer/Gruppen und Datenbanken
  - Evtl. Erstellung Schemas
- Fachliche DBAs (FDBAs):
  - Erstellung Datenbank-Objekte
  - Verwendung FDBA/Schema-Owner Rolle (`SET ROLE`)
  - Tuning von Abfragen
- Auftragsberechtigter
  - Klare Benennung, wer von fachlicher Seite aus Änderungen beantragen darf
- Systemadministration
  - Root-Kennung kann von anderer Gruppe (Systemverwaltung) betreut werden
  - Start/Stopp von PostgreSQL per sudo für TDBAs
- In der Praxis gibt es oft keine FDBAs und die Auftragsberechtigten sind Liaison zu externen Entwicklern/Software-Hersteller

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Separierung von Test- und Produktivdaten

OPS.1.1.6.A13 Trennung der Testumgebung von der Produktivumgebung:

”Die Testumgebung SOLLTE von der Produktivumgebung getrennt betrieben werden

APP.4.3.A19 Schutz vor schädlichen Datenbank-Skripten:

”Datenbank-Skripte SOLLTEN ausführlichen Funktionstests auf gesonderten Testsystemen unterzogen werden, bevor sie produktiv eingesetzt werden.”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Separierung von Test- und Produktivdaten

- Mögliche Separierung in PostgreSQL:
  - Host/VM/Container
  - Instanz
  - Datenbank
    - Rollen sichtbar
  - Schema
    - Objekte sichtbar
- Produktive und Entwicklungs/Test-Instanzen sollten jeweils auf eigenem Server laufen
- Verschiedene Kunden sollten (wenn möglich) jeweils eigene Instanzen erhalten
- Ressourcen-Management ohne VMs/Container bei vielen Instanzen schwierig
- Datenbank-Änderungen zunächst in Entwicklungs/Test/Staging-Umgebung testen (lassen)

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Notfall-Vorsorge

Anforderung bei erhöhtem Schutzbedarf

APP.4.3.A22 Notfallvorsorge:

”Für das Datenbankmanagementsystem SOLLTE ein Notfallplan erstellt werden, der festlegt, wie ein Notbetrieb realisiert werden kann. Die für den Notfallplan notwendigen Ressourcen SOLLTEN ermittelt werden. Zusätzlich SOLLTE der Notfallplan definieren, wie aus dem Notbetrieb der Regelbetrieb wiederhergestellt werden kann. Der Notfallplan SOLLTE die nötigen Meldewege, Reaktionswege, Ressourcen und Reaktionszeiten der Fachverantwortlichen festlegen.”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Notfall-Vorsorge

- Notfall-Nutzer
  - Für Bereitschafts-Mitarbeiter, die keinen regulären Zugang haben
  - Passwort in Keystore oder Tresor gelagert
- Notfall-Jump-Host
  - Alternativer Jump-Host, falls üblicher Jump-Host Down ist
- Notfall-Plan
  - Anweisungen für den Notfall
  - Alarmierungs/Eskalationskette
- Notfall-Übung
  - Typischerweise einmal im Jahr
  - Test des Notfall-Plans

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Datenbank Lebenszyklus

APP.4.3.A4 Geregeltes Anlegen neuer Datenbanken:

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

APP.4.3.A5 Benutzer- und Berechtigungskonzept (seit 2021 Entfallen):

”Es MUSS ein Prozess etabliert werden, der regelt, wie Datenbankbenutzer und deren Berechtigungen angelegt, genehmigt, eingerichtet, modifiziert und wieder entzogen bzw. gelöscht werden”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Datenbank Lebenszyklus

- Beantragung
  - Per Formular, Ticket o.ä.
    - Möglichst wenig Auswahl
- Inbetriebnahme
  - Check-Liste, Playbook etc.
  - Abnahme durch Kunden
- Änderungen
  - Neue Datenbanken, Nutzer
  - Zusätzliche Erweiterungen
  - Konfigurations-Änderungen
- Patching, Major Upgrade
- Aussonderung
  - Check-Liste, Playbook etc.

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Dokumentation von Änderungen/Störungen

Relativ egal wie, solange Auditierbar

- Sharepoint
- Ausgefüllte PDF-Formulare
- Text-Dateien
- Tickets
- Git

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Verwendete Version und Patch-Plan

APP.4.3.A2 Installation des Datenbankmanagementsystems:

”Es MUSS sichergestellt sein, dass die Installationspakete des Datenbankmanagementsystems aus sicheren Quellen stammen. Bereits veröffentlichte Patches MÜSSEN eingespielt werden, bevor das DBMS betrieben wird.”

APP.4.3.A7 Zeitnahes Einspielen von Sicherheitsupdates (seit 2021 Entfallen):

”Vorhandene Sicherheitsupdates für das Datenbankmanagementsystem [...] MÜSSEN zeitnah installiert werden. Vorab MUSS auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen.”

”Des Weiteren MUSS geprüft werden, ob die Update-Intervalle des Datenbankmanagementsystems auf die Update-Zyklen des Herstellers abgestimmt werden können.”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Verwendete Version und Patch-Plan

- PostgreSQL Major-Releases werden 5 Jahre lang unterstützt
  - Neue Major-Versionen nach 2-3 Point Releases bereit für Produktiv-Einsatz
  - Point-Releases jeweils am zweiten Donnerstag des zweiten Monats eines Quartals
  - Zeitplan: `https://www.postgresql.org/developer/roadmap/`
  - Security Team für Sicherheitsvorfälle; Notfalls außerordentliche Point-Releases
- Distributions-Pakete für alle supporteten Versionen für Red Hat / CentOS / SLES und Debian / Ubuntu
  - `http://yum.postgresql.org`
  - `http://zypp.postgresql.org`
  - `http://apt.postgresql.org`
- Patchen benötigt Einspielen der Pakete und Neustart der Instanz
  - Beendet laufende Abfragen und Sessions
  - Wartungsfenster oder organisatorischer Vorlauf (inkl. Ansprechpartner) nötig
  - Zunächst Test-Instanzen, z.B. eine Woche später Produktions-Instanzen
- Major-Versionsupgrades müssen sorgfältig geplant, getestet und durchgeführt werden

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Härtung der Standard-Berechtigungen

APP.4.3.A3 Basishärtung des Datenbankmanagementsystems:

”Das Datenbankmanagementsystem MUSS gehärtet werden. Hierfür MUSS eine Checkliste mit den durchzuführenden Schritten zusammengestellt und abgearbeitet werden.”

”Die Basishärtung MUSS regelmäßig überprüft und, falls erforderlich, angepasst werden.”

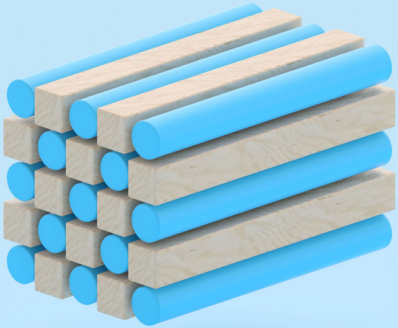
 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Härtung der Standard-Berechtigungen

- PostgreSQL erlaubt standardmäßig allen Nutzern sich an Datenbanken anzumelden
  - `REVOKE ALL ON DATABASE dbname FROM PUBLIC;`
  - `GRANT CONNECT ON DATABASE dbname TO "user-Group";`
- PostgreSQL erlaubt (vor v15) standardmäßig allen Nutzern im `public`-Schema Objekte anzulegen
  - `REVOKE ALL ON SCHEMA public FROM PUBLIC;`
- Manchmal können Standard-Anwendungen nur mit dem `public`-Schema umgehen, Ausnahmen nötig

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

System- und Datenbank-Zugriff



 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

System-Zugriff

- Der `postgres`-Nutzer sollte sich nicht via SSH einloggen dürfen
- TDBA muss sich mit persönlichem Account von Jump-Host aus einloggen
  - Wenn nötig dann Aufschaltung auf `postgres`-Nutzer via sudo
- Jump-Host sollte nur via VPN erreichbar sein, nicht direkt per SSH
- Keinen direkten Root-Login erlauben
  - In der Praxis wird Root/Admin-Account oft von anderen Teams verwaltet

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

postgres-Systembenutzer

- `postgres`-Systembenutzer (oder Instanz-Besitzer) wird für Starten/Stoppen der Instanz benötigt
- PostgreSQL Daten-Verzeichnis kann nur von `postgres`-Nutzer gelesen werden
  - Ab v11 kann einer Gruppe Zugriff gewährt werden
- Am Besten Einschränkung auf konkrete Sudo-Befehle, keine allgemeine Shell
  - In der Praxis oft schlecht umsetzbar

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Kennungen und Passwörter

APP.4.3.A5 Benutzer- und Berechtigungskonzept (seit 2021 Entfallen):

”Das Benutzer- und Berechtigungskonzept der Institution MUSS um die für Datenbankmanagementsysteme notwendigen Berechtigungen für Rollen, Profile und Benutzergruppen erweitert werden.”

”Es MUSS ein Prozess etabliert werden, der regelt, wie Datenbankbenutzer und deren Berechtigungen angelegt, genehmigt, eingerichtet, modifiziert und wieder entzogen bzw. gelöscht werden.”

APP.4.3.A6 Passwortänderung [Fachverantwortliche] (seit 2021 Entfallen):

”Alle Passwörter der Datenbankbenutzer MÜSSEN der Passwortrichtlinie der Institution entsprechen.”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Kennungen und Passwörter

- Passwort-Manager für generelle Passwörter auf TDBA-Seite
- Postgres bietet keine Möglichkeiten für Passwort-Richtlinien wie Komplexität, oder regelmäßige Änderungen
- Technische Nutzer für Anwendungsserver usw.
  - SCRAM Passwörter/Authentifizierung (`scram-sha-256`)
  - Regelmäßige Passwort-Wechsel technisch schwer zu überprüfen
  - FDBAs/Anwendungsbetreuer sollten Kenntnis/Absicht darüber bestätigen
- Personalisierte Nutzer
  - Einer bestimmten Person zugeordnet
  - Keine Gruppen-Accounts
  - Passwort-Richtlinien via LDAP/Active-Directory (`ldap`) umsetzbar
    - Verschlüsselte Verbindung, da LDAP-Passwort im Klartext vom Client übertragen wird
  - Alternativ `gssapi` für komplett verschlüsselte Authentifizierung mit Active Directory
    - Kompliziert (Kerberos), vor allem wenn keine Kontrolle über AD-Server besteht

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

IP-Freischaltungen und Verbindungsaufbau

APP.4.3.A16 Verschlüsselung der Datenbankanbindung:

”Das Datenbankmanagementsystem SOLLTE so konfiguriert werden, dass Datenbankverbindungen immer verschlüsselt werden.”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

IP-Freischaltungen und Verbindungsaufbau

- Zugriff für TDBAs nur über personalisierte Kennung oder `local` via `peer`
- Nur benötigte Quell-IP-Adressen in `pg_hba.conf` freischalten
  - Bzw. IP-Bereiche nach Minimal-Prinzip
- TCP/IP Datenbank-Verbindungen sollten generell verschlüsselt sein (`hostssl`)
  - Seit v10 ist ein Austausch des Server-Zertifikats ohne Neustart der Instanz möglich
- Feingranulare Einstellungen von Rollen und Datenbanken möglich, aber in der Praxis oft schnell unübersichtlich
  - Unterscheidung IP-Adressen von technischen Nutzern (`scram-sha-256`) und personalisierten Kennungen (z.B. `ldap`)
  - Vergabe von Gruppen an die entsprechenden Rollen z.B. `scram-Group` und `ldap-Group` und Verwendung in `pg_hba.conf`

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Beispiel pg_hba.conf

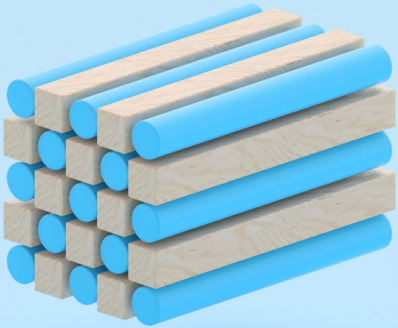
```
# TYPE  DATABASE USER         ADDRESS         METHOD
local   all      postgres                     peer
local   all      +tdba-Group                  peer

hostssl all      +scram-Group 10.1.0.23/32    scram-sha-256
hostssl all      +scram-Group 10.1.0.65/30    scram-sha-256

hostssl all      +ldap-Group  172.16.43.75/24 ldap
    ldapserver=domain.foo.de ldapprefix="FOO" ldapport="389"
    ldapsuffix="" ldaptls=1
hostssl all      +ldap-Group  172.16.13.88/24 ldap
    ldapserver=domain.foo.de ldapprefix="FOO" ldapport="389"
    ldapsuffix="" ldaptls=1
```

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Sicherer Betrieb



 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Protokollierung

APP.4.3.A8 Datenbank-Protokollierung (seit 2021 Entfallen):

”Sicherheitsrelevante Ereignisse des Datenbanksystems MÜSSEN mit einem eindeutigen Zeitstempel protokolliert werden. Dabei MÜSSEN sich Art und Umfang der Protokollierung am Schutzbedarf der zu verarbeitenden Informationen orientieren.”

”Es SOLLTE so protokolliert werden, dass die Protokolldateien nicht nachträglich verändert werden können.”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Protokollierung

- Protokollierungs-Konzept
- Revisionssichere Logdateien
- Versand via syslog-ng an Log-Server (verschlüsselt)
  - `log_destination = 'stderr,syslog'`
  - `syslog_facility = 'local7'`
  - `syslog_ident = 'postgres-$HOST-$INSTANZ'`
- TDBAs haben dort höchstens Lese-Rechte
- Möglichkeit FDBAs die Logdateien (ohne SSH-Zugang zum DB-Server) bereitzustellen
- Aufbewahrungsfristen beachten (30 Tage üblich)

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Auditierung

- Logging von Verbindungen (`log_connections`/`log_disconnections`)
  - Leider unflexibel; oft sehr viel Rauschen durch technische Nutzer
- Logging von DDL / Konfigurations-Änderungen (`log_statement = 'ddl'`)
- Logging von DML der TDBAs (`log_statement = 'mod'` pro TDBA Rolle)
  - Eigenschutz
- Bei Instanzen mit hohem hohem Schutzbedarf `log_statement = 'mod'`
- Bei Instanzen mit hohem sehr hohem Schutzbedarf `log_statement = 'all'`
- Wenn möglich `pgaudit`-Erweiterung für gezieltere Auditierung verwenden
  - Audit-Ereignisse werden in das normale Postgres-Log geschrieben
- Auditierung von Konfigurations-Änderungen nicht einfach
  - Änderungen während einer Downtime werden nicht geloggt
  - Periodische Auditierung der `postgresql.conf` Werte gegen SOLL-Daten

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Backup/Restore(-Tests)

APP.4.3.A9 Datensicherung eines Datenbanksystems:

”Es MÜSSEN regelmäßig Systemsicherungen des DBMS und der Daten durchgeführt werden. [...] Hierfür SOLLTEN die dafür zulässigen Dienstprogramme benutzt werden.”

”Alle Transaktionen SOLLTEN so gesichert werden, dass sie jederzeit wiederherstellbar sind.”

APP.4.3.A14 Überprüfung der Datensicherung eines Datenbanksystems (seit 2021 Entfallen):

”Die vorgenommenen Datensicherungen SOLLTEN regelmäßig daraufhin überprüft werden, ob die Integrität der Sicherungsdateien noch gewährleistet ist. Die verantwortlichen Mitarbeiter SOLLTEN zudem regelmäßig üben, wie sich Datenbanken im Notfall schnell wiederherstellen lassen.”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Backup/Restore(-Tests)

- Datensicherungs-Konzept
- Ab einer gewissen Größe physische Backups nötig
  - Sinnvoll ein fertiges Produkt wie pgBackRest, Barman zu verwenden
  - Bei kleineren Instanzen auch Dumps (oft lokale Skripte)
- Definierte Retention-Time
  - Üblich 2-5 Tage, Auslagerung auf externe Storage-Lösungen
  - Evtl. Aufbewahrung Monats/Jahressicherungen (ggf. zusätzlich im Dump-Format)
  - Beachtung evtl. Archivierungs-Pflichten des letzten Backups nach Aussonderung
- Automatisierte Restore-Tests der produktiven Instanzen (z.B. jede Woche)
  - Bei Point-in-Time-Recovery nachfolgender Dump empfohlen

© 2023 Netapp, Inc. Alle Rechte vorbehalten.

Monitoring

APP.4.3.A18 Überwachung des Datenbankmanagementsystems:

”Die für den sicheren Betrieb kritischen Parameter, Ereignisse und Betriebszustände des DBMS SOLLTEN definiert werden. Diese SOLLTEN mithilfe eines Monitoring-Systems überwacht werden. Für alle kritischen Parameter, Ereignisse und Betriebszustände SOLLTEN Schwellwerte festgelegt werden. Wenn diese Werte überschritten werden, MUSS geeignet reagiert werden.”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Monitoring

- Oftmals zentrales Monitoring vorhanden
  - Manchmal für TDBAs nicht verfügbar
  - Oder irgendein Enterprise-Tool ohne Postgres-Integration
- Icinga-Monitoring mit Alerting im Prinzip ausreichend
- Zusätzliche Checks/Metriken hilfreich
  - `check_postgres`
  - InfluxDB/Grafana für Graphen
- Alternativ
  - Prometheus
  - `{node,sql,postgres}_exporter`
  - AlertManager
  - Grafana Dashboards

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Datenverschlüsselung in der Datenbank

Anforderung bei erhöhtem Schutzbedarf

APP.4.3.A24 Datenverschlüsselung in der Datenbank:

Die Daten in den Datenbanken SOLLTEN verschlüsselt werden. Dabei SOLLTEN vorher unter anderem folgende Faktoren betrachtet werden: 1. Einfluss auf die Performance, 2. Schlüsselverwaltungsprozesse und -verfahren, einschließlich separater Schlüsselaufbewahrung und -sicherung, 3. Einfluss auf Backup-Recovery-Konzepte, 4. funktionale Auswirkungen auf die Datenbank, beispielsweise Sortiermöglichkeiten."

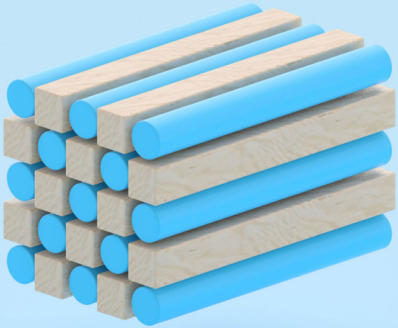
 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Datenverschlüsselung in der Datenbank

- Festplattenverschlüsselung evtl. eine Alternative
- Transparent Data Encryption (TDE) bisher nicht in PostgreSQL verfügbar
  - “TDE key management patches”: `https://commitfest.postgresql.org/43/3985/`
  - `https://github.com/cybertec-postgresql/postgres/`
- Spaltenbasierte Verschlüsselung möglich, aber nicht komfortabel
  - `pgcrypto`-Erweiterung
  - “automatic client-side column-level encryption”: `https://commitfest.postgresql.org/42/3718/`

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Schlussbemerkungen



 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Schlussbemerkungen

- Ab einer gewissen (Team-)Größe sind viele der Anforderungen sinnvoll
- Selbstschutz für DBAs
  - Auftragsberechtigte
  - Paper Trail
  - Protokollierung/Auditierung
- Nicht die BSI-Keule schwingen
- Umsetzung mit Augenmaß
  - Vieles lässt sich (sinnvoll) Verargumentieren oder Begründen
- Argumentations-Grundlage gegenüber Kunden
  - “Das muss Ihr ISB freigben / Ihr Behördenleiter abzeichen”
  - “Da brauchen wir eine Risiko-Übernahme”

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Risiko-Übernahme

https://twitter.com/derpupe/status/963496089608441856

 © 2023 Netapp, Inc. Alle Rechte vorbehalten.

Thank you

© 2023 NetApp, Inc. Alle Rechte vorbehalten.