# Untersuchung von opensource Datenbanksystemen auf Härtungsmaßnahmen unter Betrachtung des BSI IT-Grundschutz-Kompendium

Wirtschaftsingenieurwesen
- Informationtechnology and Management -

Henner Bendig

23. Juli 2020

WINGS-FERNSTUDIUM
AN DER HOCHSCHULE WISMAR
macht erfolgreicher

# Aufgabenstellung

*» In dieser Arbeit sind verschiedene Opensource Datenbanksysteme (DBS) nach den Anforderungen des IT-Grundschutzkompendiums des Bundesministeriums für Sicherheit in der Informationstechnik (BSI) zu untersuchen.*

*Hierbei ist vorrangig das Kapitel „APP.4.3: Relationale Datenbanken“ zu betrachten, wobei die anzuwendenden Maßnahmen ebenso auf die Umsetzbarkeit in Nicht-Relationalen Datenbanken untersucht werden sollen.*

*Es sind weiterhin zu analysieren, welche technischen und organisatorischen Maßnahmen zur Härtung der Datenbanksysteme eingesetzt werden können. Anhand von Beispiel-Datenbanken sind die Erkenntnisse prototypisch zu illustrieren. «*

# Überblick

**Einleitung**

**Umsetzung**

**Auswertung**

**Diskussion**

# Überblick

**Einleitung**

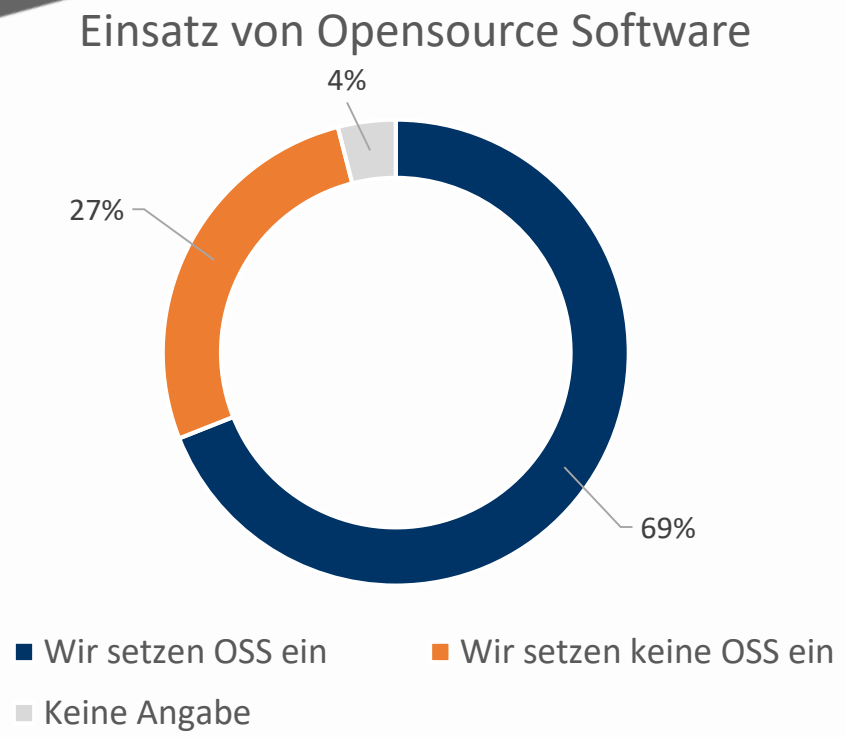
Umsetzung

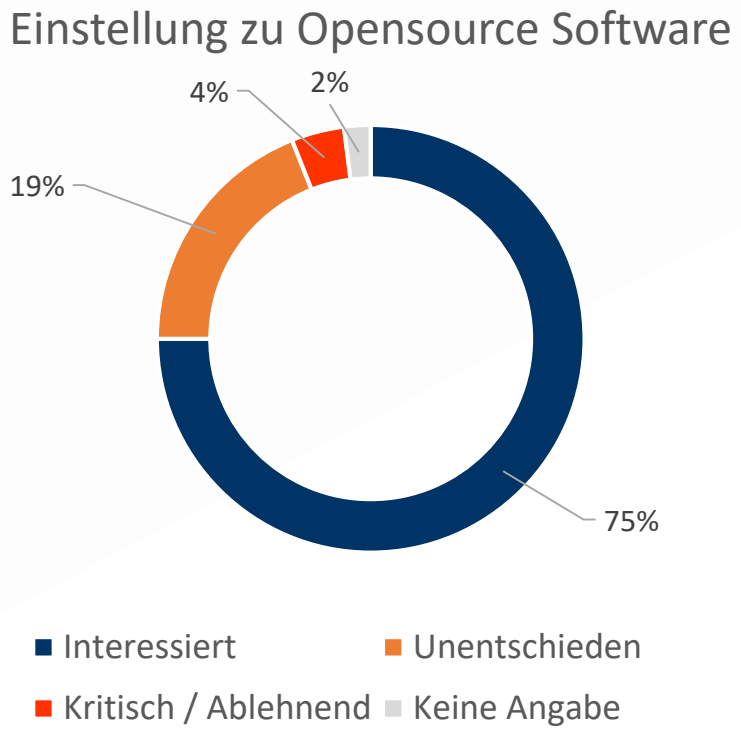
Auswertung

Diskussion

# Open Source Monitor 2019

bitkom




„Open Source Monitor – Studienbericht 2019“, Bitkom e.V., Berlin 2019

(n = 804)

*» Technology continues to play a profound role in shaping the global risks landscape. Concerns about data fraud and cyber-attacks were prominent again in the GRPS, which also highlighted a number of other technological vulnerabilities: [ … ]*

***There were further massive data breaches in 2018, new hardware weaknesses were revealed, and research pointed to the potential uses of artificial intelligence to engineer more potent cyberattacks. Last year also provided further evidence that cyber-attacks pose risks to critical infrastructure,*** *prompting countries to strengthen their screening of cross-border partnerships on national security grounds. «*

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

„The Global Risks Report 2019, 14th Edition“,
World Economic Forum®, Genf 2019

# Top 5 Global Risks in Terms of Likelihood

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Economic | Environmental | Geopolitical | Societal | Technological

Top 5 Global Risks in Terms of Likelihood

| | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1st | Asset price collapse | Asset price collapse | Storms and cyclones | Severe income disparity | Severe income disparity | Income disparity | Interstate conflict with regional consequences | Large-scale involuntary migration | Extreme weather events | Extreme weather events | Extreme weather events |
| 2nd | Slowing Chinese economy (<6%) | Slowing Chinese economy (<6%) | Flooding | Chronic fiscal imbalances | Chronic fiscal imbalances | Extreme weather events | Extreme weather events | Extreme weather events | Large-scale involuntary migration | Natural disasters | Failure of climate-change mitigation and adaptation |
| 3rd | Chronic disease | Chronic disease | Corruption | Rising greenhouse gas emissions | Rising greenhouse gas emissions | Unemployment and underemployment | Failure of national governance | Failure of climate-change mitigation and adaptation | Major natural disasters | Cyber-attacks | Natural disasters |
| 4th | Global governance gaps | Fiscal crises | Biodiversity loss | Cyber-attacks | Water supply crises | Climate change | State collapse or crisis | Interstate conflict with regional consequences | Large-scale terrorist attacks | Data fraud or theft | Data fraud or theft |
| 5th | Retrenchment from globalization | Global governance gaps | Climate change | Water supply crises | Mismanagement of population | Cyber-attacks | High structural unemployment or underemployment | Major natural catastrophes | Massive incident of data fraud/theft | Failure of climate-change mitigation and adaptation | Cyber-attacks |

„The Global Risks Report 2019, 14th Edition“, World Economic Forum®, Genf 2019

# Top 5 Global Risks in Terms of Likelihood

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Economic | Environmental | Geopolitical | Societal | Technological

Top 5 Global Risks in Terms of L

| | 2009 | 2010 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|---|---|---|
| 1st | Asset price collapse | Asset price collapse | income | Income disparity | Interstate conflict with regional consequences | Large-scale involuntary migration | Extreme weather events | Extreme weather events | Extreme we events |
| 2nd | Slowing Chinese economy (<6%) | Slowing Chinese economy (<6%) | fiscal | Extreme weather events | Extreme weather events | Extreme weath events | Large-scale involuntary migration | Natural disasters | Failure of climate-cha mitigation a adaptation |
| 3rd | Chronic disease | Chronic disease | greenhouse | Unemployment and underemployment | Failure of national governance | Failure of climate-change mitigation and adaptation | Major natural disasters | Cyber-attacks | Natural disa |
| 4th | Global governance gaps | Fiscal crises | supply | Climate change | State collapse or crisis | Interstate confl with regional consequences | Large-scale terrorist attacks | Data fraud or theft | Data fraud |
| 5th | Retrenchment from globalization | Global governan gaps | nagement ulation | Cyber-attacks | High structural unemployment or underemployment | Major natural catastrophes | | | |

| 2009 | 2010 |
|---|---|
| Asset price collapse | Asset price collapse |
| Slowing Chinese economy (<6%) | Slowing Chinese economy (<6%) |
| Chronic disease | Chronic disease |
| Global governance gaps | Fiscal crises |
| Retrenchment from globalization | Global governance gaps |

„The Global Risks Rep nomic Forum®, Genf 2019

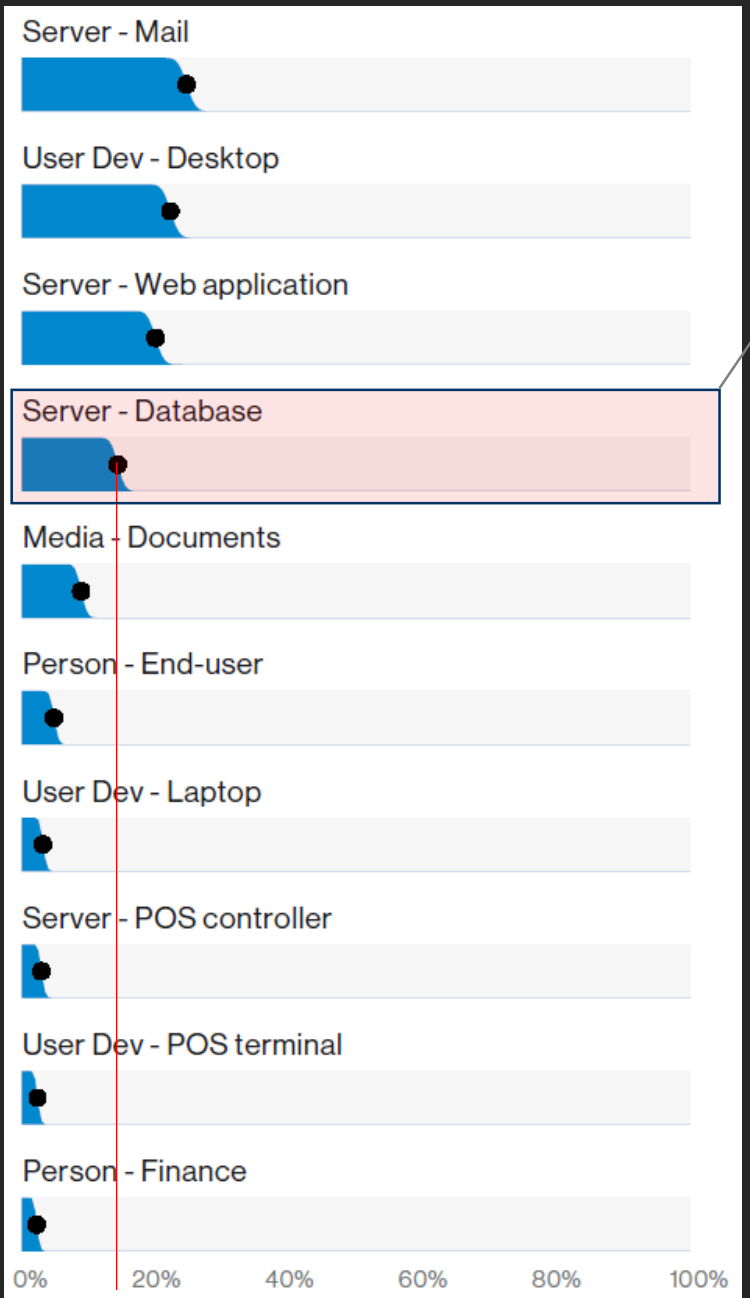



**Figure 25.** Top asset varieties in breaches (n=1,699)

Mit etwa 15% die am 4. häufigsten Ziele von Cyberangriffen

„2019 Data Breach Investigation Report,“
Verizon Communications Inc., New York City, 2019

# Zusammengefasst…

Das Interesse und der Einsatz von OSS steigt

Insbesondere Datenbanken sind schon heute stark betroffen

Die Gefahr von Cyper-Angriffen und Datendiebstählen steigt

*» Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. «*

**Der IT-Grundschutz**

Ein einheitlicher Schutzstandard um » *das Niveau der Informationssicherheit in Behörden und Unternehmen jeder Größenordnung zu erhöhen.* «

- BSI-Standard 200-1:
  „Managementsysteme für Informationssicherheit“
- BSI-Standard 200-2:
  „IT-Grundschutz-Methodik“
- BSI-Standard 200-3:
  „Risikoanalyse auf Basis von IT-Grundschutz“
- BSI-Standard 100-4:
  „Notfallmanagement“

Bundesamt
für Sicherheit in der
Informationstechnik

*» Das IT-Grundschutz-Kompendium ist die grundlegende Veröffentlichung des IT-Grundschutzes. Zusammen mit den BSI-Standards bildet es die Basis für alle, die sich umfassend mit dem Thema Informationssicherheit befassen möchten. «*

- ***„Basis Anforderungen*** *sind das Minimum dessen […], was vernünftiger Weise an Sicherheitsvorkehrungen umzusetzen ist.“*
- **Standard Anforderungen** sind nach dem BSI als *„angemessene Sicherheit“* beschrieben.
- **Anforderungen für erhöhten Schutzbedarf** haben sich, nach dem BSI, *„in der Praxis bewährt“* und *„zeigen auf, wie eine Institution sich […] zusätzlich absichern kann“*.

# IT–Grundschutz–Kompendium

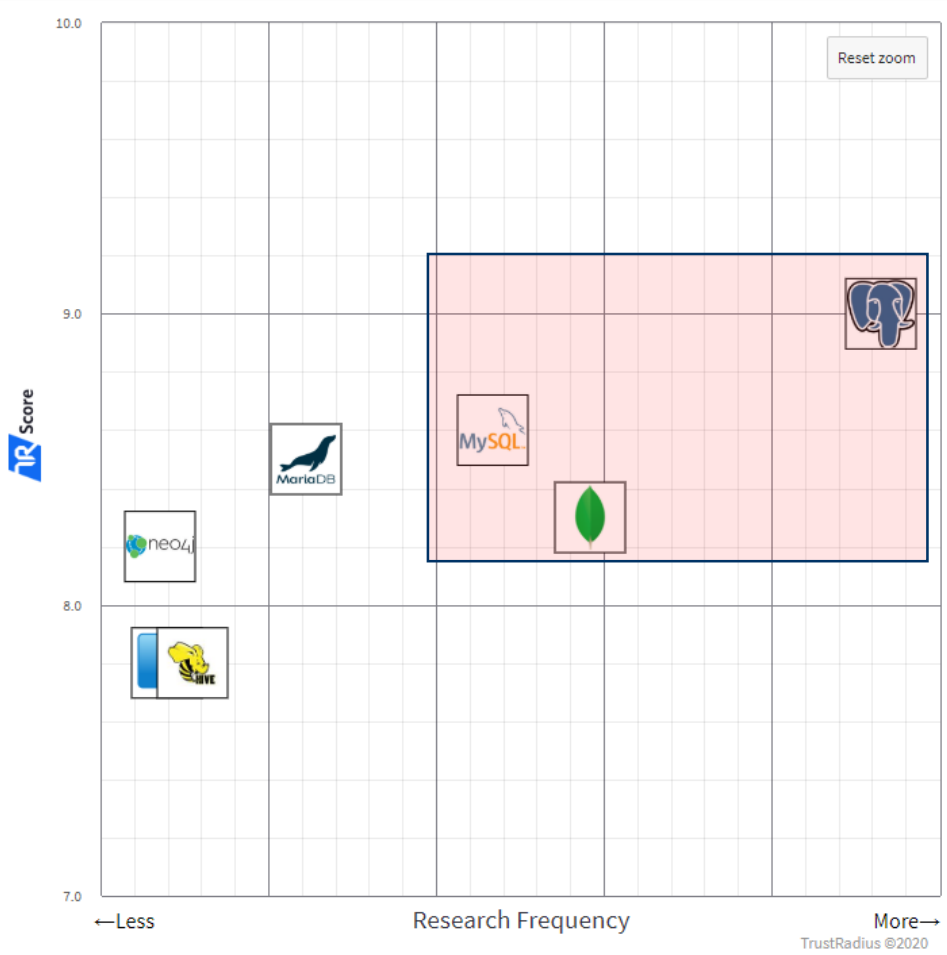
# Die Testsysteme

# Die Testsysteme

Opensource

| Rang | | | Datenbanksystem |
|---|---|---|---|
| **März 2020** | Februar 2020 | März 2019 | |
| **1.** | 1. | 1. | Oracle |
| **2.** | 2. | 2. | MySQL |
| **3.** | 3. | 3. | Microsoft SQL-Server |
| **4.** | 4. | 4. | PostgreSQL |
| **5.** | 5. | 5. | MongoDB |
| **6.** | 6. | 6. | IBM DB2 |
| **7.** | 7. | 8. | Elasticsearch |
| **8.** | 8. | 7. | Redis |
| **9.** | 9. | 9. | Microsoft Access |
| **10.** | 10. | 10. | SQLite |

solidIT consulting & software development gmbh, „DB Engines,“ März 2020.




TrustRadius Inc., „List of Top Open-Source Database Software 2020”, Mai 2020

# Überblick

**Einleitung**

**Umsetzung**

Auswertung

Diskussion

# Der Systembaustein APP.4.3

Schicht: „Anwendungen“
Teilschicht: „Businessanwendungen“
Baustein: „Relationale Datenbanken“
Abkürzung: „APP.4.3“

25 Anforderungen aufgeteilt nach:

- 9 Basis-Anforderungen
- 11 Standard-Anforderungen
- 5 Anforderungen an erhöhte Sicherheit

# APP.4.3.A9 Datensicherung eines Datenbanksystems

*» Es MÜSSEN regelmäßig Systemsicherungen des DBMS und der Daten durchgeführt werden. Auch bevor eine Datenbank neu erzeugt wird, MUSS das Datenbanksystem gesichert werden. Hierfür SOLLTEN die dafür zulässigen Dienstprogramme benutzt werden. Alle Transaktionen SOLLTEN so gesichert werden, dass sie jederzeit wiederherstellbar sind. Wenn die Datensicherung die verfügbaren Kapazitäten übersteigt, SOLLTE ein erweitertes Konzept erstellt werden, um die Datenbank zu sichern, z. B. eine inkrementelle Sicherung. Abhängig vom Schutzbedarf der Daten SOLLTEN die Wiederherstellungsparameter vorgegeben werden. «*

**Umsetzungsvorschlag**
Gemäß der Anforderungsbeschreibung wurden die DBS auf unterschiedliche Sicherungsarten untersucht:

- Volle Datenbank-Sicherung
- Inkrementelle Datenbank-Sicherung
- Sicherung der Transaktionen

# APP.4.3.A9
# Datensicherung eines Datenbanksystems

## MySQL

### Volle Datenbank-Sicherung

mysqldump

```
mysqldump --all-databases --single-transaction --quick --lock-tables=false > full-backup-
$(date +%F).sql -u root -p
```

### Inkrementelle Datenbank-Sicherung

Workaround: Binlog / binary logs

```
[mysqld]
log_bin              = /var/log/mysql/mysql-bin.log   # Speicherort und Dateiname
expire_logs_days     = 2                              # Ablaufdatum der Logs
max_binlog_size      = 100M                           # Erlaubte Größe pro Inkrement
binlog-do-db         = Uni                            # Zu sichernde Datenbank
```

### Sicherung der Transaktionen

General Logs

```
general_log_file     = /var/log/mysql/mysql.log       # Pfad und Dateiziel
general_log          = 1                              # General Log aktivieren
```

# APP.4.3.A9
# Datensicherung eines Datenbanksystems

## PostgreSQL

Volle Datenbank-Sicherung

pg_dump

```
pg_dumpall > full-backup-$(date +%F).sql
```

Inkrementelle Datenbank-Sicherung

Nicht unterstützt

Sicherung der Transaktionen

Write Ahead Log (WAL)

```
archive_mode = 'on'
archive_command = 'cp %p /var/lib/pgsql/12/archives/%f'          # gibt an, wo die Archive
                                                                 # gesichert werden
```

# APP.4.3.A9
# Datensicherung eines Datenbanksystems

## MongoDB

Volle Datenbank-Sicherung

mongodump

```
mongodump --out /var/log/mongodb/backup/    # erzeugt eine Sicherung am angegeben
                                            # Verzeichnis
```

Inkrementelle Datenbank-Sicherung

Nicht unterstützt

Sicherung der Transaktionen

Workaround: Oplog / Operative Logs

```
mongod --config=/etc/mongo.config --replSet=rs0
rs.initiate()
```

# APP.4.3.A9
# Datensicherung eines Datenbanksystems

| | Volle Datenbank-Sicherung | Inkrementelle Datenbank-Sicherung | Sicherung der Transaktionen |
|---|---|---|---|
| MySQL | ✓ | ✓ | ✓ |
| PostgreSQL | ✓ | ✗ | ✓ |
| mongoDB | ✓ | ✗ | ✓ |

# 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:*

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

**Umsetzungsvorschlag**

Betrachtung der DBS hinsichtlich:

- Generelle Verschlüsselung von Datensätzen
- Schlüsselmanagement
- Performance
- Funktionale Auswirkung

# APP.4.3.A24 Datenverschlüsselung in der Datenbank

**MySQL**

- Die Community-Variante bietet eine symmetrische Verschlüsselung der Daten an, Zellenweise über die Funktion „AES_ENCRYPT( )“
- Standardmäßig wird ein 128Bit Schlüssel genutzt, maximal bis 256 Bit möglich
- Oracle Corp. warnt explizit davor, längere Schlüssel zu nutzen, da es starke Performanceeinbußungen gibt
- In MySQL ist kein Schlüsselmanagement eingebunden, das hierfür genutzt werden kann
- Keine Funktionen auf den Daten möglich
- Kein Einfluss auf Backup-Konzepte

**Nicht für standardmäßige, vollumfängliche Verschlüsselung geeignet**

>> MySQL Enterprise bietet eine integrierte Datenverschlüsselung an

- Schlüsselmanagement integriert
- Richtlinienkonform zu HIPPA, SOx und PCI-DSS

# APP.4.3.A24 Datenverschlüsselung in der Datenbank

**PostgreSQL**

- In PostgreSQL kann das Plugin „pg_crypto“ aktiviert werden
- Dieses bietet die zellenweise, symmetrische Datenverschlüsselung an, über die Funktion *„pgp_sym_encrypt(data, pw, options)“*
- Unterstützt unterschiedliche, kryptografische Algorithmen: SHA in den Varianten 1 und 2, Blowfish und AES
- Kein Schlüsselmanagement enthalten
- Keine Funktionen auf den Daten möglich
- Kein Einfluss auf Backup-Konzepte

**Nicht für standardmäßige, vollumfängliche Verschlüsselung geeignet**

# APP.4.3.A24 Datenverschlüsselung in der Datenbank

**MongoDB**

- Für die Community-Variante keine Verschlüsselung integriert

>> MongoDB Enterprise bietet eine integrierte Datenverschlüsselung an

- „Data at Rest“
- Kein Schlüsselmanagement
- Richtlinienkonform zu HIPPA, FERPA und PCI-DSS
- AES-256 (Cipher Block Chaining (CBC) oder Galois/Counter-Mode(GCM))

# APP.4.3.A24
# Datenverschlüsselung in der Datenbank

| | Verschlüssel-ung Allgemein | Schlüssel-management | Performance | Funktionale Auswirkung |
|---|---|---|---|---|
| MySQL | ∅ | ✗ | ✗ | ✗ |
| PostgreSQL | ∅ | ✗ | ✗ | ✗ |
| mongoDB | ✗ | ✗ | ✗ | ✗ |

# 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*. «

**Umsetzungsvorschlag**

Zur Umsetzung dieser Anforderung wurde ein Stammdatenblatt entworfen, welches die fachlichen, technischen und sicherheitstechnischen Punkte aufnimmt. Es wurde ein Prozess definiert, welcher die beteiligten Personen einbindet und ein geregeltes Vorgehen zur Definition der Daten im Stammblatt vorgibt.

# APP.4.3.A4
# Geregeltes Anlegen neuer Datenbanken

| Rolle | Beschreibung |
|---|---|
| Anfragender / Nutzer | Die fachliche Person, in der Regel ein Mitarbeiter einer Abteilung, hat den Bedarf an einer neuen Datenbank durch einen Geschäftsvorfall oder eine neue Aktion. |
| Fachlich Verantwortlicher | Die dem Nutzer vorgesetzte Person, die den Geschäftsvorfall fachlich verantwortet und die Kosten rechtfertigen muss. |
| Technisch Verantwortlicher | Ein Mitarbeiter aus der Abteilung „Informationstechnik“, der für die technische Umsetzung der Anforderungen aus dem Geschäftsbereich zuständig ist. |
| Sicherheit Verantwortlicher | Der ISB oder eine von dem ISB beauftragte Person, die die Informationssicherheit für diesen Geschäftsbereich verantwortet. |

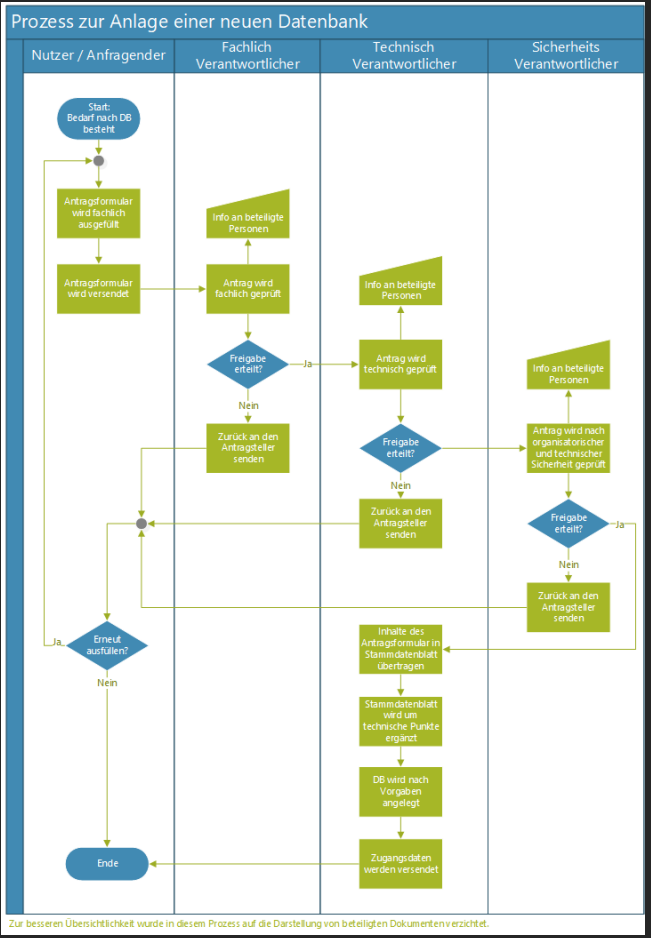
# APP.4.3.A4
# Geregeltes Anlegen neuer Datenbanken

**Stammdatenblatt**

- **Eindeutiger Bezeichner der Datenbank**
- **Verantwortliche Personen (Fachlich, Technisch, Sicherheit)**
- **Administratoren mit Berechtigungen**
- **Technische Daten (Datenbanktyp, Hersteller, Version, Patch, Standort/Cloud)**
- **Zweck / Zugehörigkeit**
- **Kostenstelle**
- **Angelegt am / Laufzeit / Löschung am**
- **Backupstrategie / Aufbewahrungsfrist**
- **Für APP.4.3.A13: Enthaltende DB-Links**

# APP.4.3.A4
# Geregeltes Anlegen neuer Datenbanken

## Prozess



# APP.4.3.A4
# Geregeltes Anlegen neuer Datenbanken

**Organisatorische Maßnahmen werden nicht spezifisch für ein DBS umgesetzt, sondern sind losgelöst von technischen Rahmenbedingungen umzusetzen.**

# Überblick

**Einleitung**

**Umsetzung**

**Auswertung**

**Diskussion**

# Auswertung

Einsatz der Auditorencheckliste mit vier Kategorien:

| Kategorie | Bedeutung | Punkte |
|---|---|---|
| Ja | Voll umsetzbar | 2 |
| Teilweise | Teilweise umsetzbar | 1 |
| Nein | Nicht umsetzbar | 0 |
| Nicht zutreffend | Organisatorisch | 0 |

Organisatorische Maßnahmen wurden mit der Punktzahl 0 aus der Wertung heraus genommen, da diese Maßnahmen nicht Datenbank spezifisch sind.

Von insgesamt 25 Maßnahmen, sind 10 organisatorisch.
Somit bleiben 15 technische Maßnahmen.

Daher ist eine erreichbare Gesamtpunktzahl von **(2 x 15 =) 30 Punkten** möglich.

# Auswertung

| Anforderung | Titel | MySQL | Postgre SQL | Mongo DB |
|---|---|---|---|---|
| **APP.4.3.A2** | Installation des Datenbankmanagementsystems | 1 | 0 | 1 |
| **APP.4.3.A3** | Basishärtung des Datenbankmanagementsystem | 2 | 2 | 1 |
| **APP.4.3.A5** | Benutzer- und Berechtigungskonzept | 2 | 2 | 2 |
| **APP.4.3.A6** | Passwortänderung | 2 | 1 | 0 |
| **APP.4.3.A7** | Zeitnahes Einspielen von Sicherheitsupdates | 2 | 2 | 2 |
| **APP.4.3.A8** | Datenbank-Protokollierung | 2 | 2 | 0 |
| **APP.4.3.A9** | Datensicherung eines Datenbanksystems | 2 | 1 | 1 |
| **APP.4.3.A12** | Einheitlicher Konfigurationsstandard von Datenbankmanagementsystemen | 2 | 2 | 2 |
| **APP.4.3.A13** | Restriktive Handhabung von Datenbank-Links | 0 | 1 | 0 |
| **APP.4.3.A14** | Überprüfung der Datensicherung eines Datenbanksystems | 0 | 0 | 0 |
| **APP.4.3.A16** | Verschlüsselung der Datenbankanbindung | 2 | 2 | 2 |
| **APP.4.3.A18** | Überwachung des Datenbankmanagementsystems | 2 | 2 | 2 |
| **APP.4.3.A19** | Schutz vor schädlichen Datenbank-Skripten | 1 | 1 | 1 |
| **APP.4.3.A21** | Einsatz von Datenbank Security Tools | 1 | 1 | 0 |
| **APP.4.3.A24** | Datenverschlüsselung in der Datenbank | 1 | 1 | 0 |
| **Summe** | | **22** | **20** | **14** |

# Auswertung

| Datenbanksysteme | Punktzahl | Prozent |
|---|---|---|
| **MySQL** | 22 | 73,33% |
| **PostgreSQL** | 20 | 66,67% |
| **MongoDB** | 14 | 46,67% |

# Überblick

**Einleitung**

**Umsetzung**

**Auswertung**

**Diskussion**

# Diskussion

In dieser Arbeit wurde die Prozesse fiktiv umgesetzt. In realer Umgebung sollten die in mehreren Iterationen vertestet und angepasst werden.

In der nicht-relationalen MongoDB konnten lediglich 46,67% umgesetzt werden.

- MongoDB erlaubt keine Einbindung von Erweiterungen/Plugins
- Die Anforderungsliste ist für relationale DBS entworfen. Eine Liste für nicht-relationale DBS ist in Planung.

Sofern die Funktionen vorhanden waren, mussten diese explizit aktiviert werden, was tendenziell dazu führt, dass sie inaktiv bleiben. Ein standardmäßiges Aktivieren der Funktionen würde wahrscheinlich zu vermehrten Einsatz dieser Funktionen führen (Opt-In zu Opt-Out).

Diese Arbeit hat sich rein mit den Härtungsmaßnahmen der konkreten DBS befasst. Zu einer umfassenden Absicherung müssen aber auch die Netzwerke und Hostsysteme betrachtet werden.

# Thesen

1. Viele Sicherheitsmaßnahmen sind organisatorischer Natur und bedürfen die Mitarbeit aller Beteiligten, daher sollten alle in die Sicherheitsprozesse eingewiesen werden. Die Unterstützung muss von höchster Stelle kommen.

# Thesen

2. Die Umsetzung der organisatorischen Maßnahmen benötigt Erfahrung im IT-Sicherheitsbereich und in Management. Die Prozesse sollten in enger Abstimmung mit den Fachverantwortlichen und den Mitarbeitern erarbeitet werden, da diese Maßgeblich an der Durchführung beteiligt sind.

# Thesen

3. MySQL konnte ca. 73% und PostgreSQL ca. 67% der technischen Maßnahmen umsetzen. Hierzu mussten aber Drittanbieter Plugins und Software eingesetzt werden.

# Thesen

4. MongoDB konnte lediglich ca. 47% der Maßnahmen umsetzen. Das System ermöglicht keine Einbindung von Drittanbieter-Plugins.

# Thesen

5. Opensource Software wird stark von den zumeist dahinterstehenden Unternehmen getrieben. Kritische Funktionen, wie z.B. Sicherheitsmechanismen, bleiben oftmals einer kommerziellen Variante der Opensource Software vorbehalten.

# Thesen

6. Es sind viele Sicherheitsfunktionen vorhanden, die bspw. vom BSI gefordert werden. Diese müssen aber explizit aktiviert werden (Opt-In-Verfahren) und sind in Standardinstallationen daher nicht aktiv.

# Thesen

7. Das Bundesamt für Sicherheit in der Informationstechnik hat mit dem IT-Grundschutzkompendium einen umfassenden Maßnahmenkatalog zur Verbesserung der IT-Sicherheit veröffentlicht. Bei neueren Technologien müssen aber noch Bausteine nachgearbeitet werden.

Vielen Dank für Ihre Aufmerksamkeit!

WINGS-FERNSTUDIUM
AN DER HOCHSCHULE WISMAR
macht erfolgreicher