Untersuchung von Nicht-relationalen Datenbank-systemen mit Fokus auf Härtungsmaßnahmen

- Motivation
- Grundlagen Datenbanken und IT-Grundschutz
- Modellierung Informationsverbund
- Durchführung Härtungsanalysen
- Auswertung Härtungsanalysen
- Fazit und Ausblick

Sebastian Kavalir

Hochschule Wismar \ Fakultät für Ingenieurwissenschaften \ Bereich Elektrotechnik und Informatik

HOCHSCHULE WISMAR
UNIVERSITY OF APPLIED SCIENCES TECHNOLOGY, BUSINESS AND DESIGN

Motivation

- **„Most Important Global Business Risks (DEU)“ [(1)]:**
  1. Business interruption: 50%
  2. Cyber incidents: 48%
  3. Pandemic outbreak: 35%
- **Herausforderungen SARS-CoV2-Pandemie**
  - Homeoffice
  - Zeitkritische Umsetzung vs. IT-Sicherheit
- **Angriffe auf Datenbanken**
  - Ca. 15% der Vorfälle „Cyber incidents“

Allianz

ALLIANZ RISK BAROMETER

IDENTIFYING THE MAJOR BUSINESS RISKS FOR 2021

Beispiele „Cyber incidents“:

- Cyberkriminalität
- Versagen von IT
- Daten-Leaks

Quellen:

(1) Allianz Global Corporate & Specialty: *„ALLIANZ RISK BAROMETER“*

Motivation

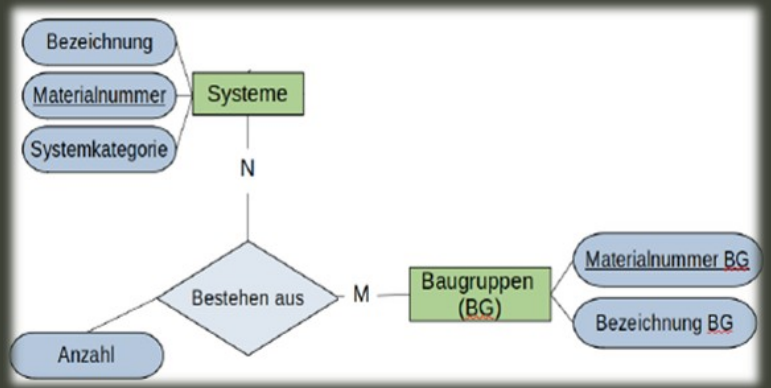
- **Hohes Schadenspotenzial bei IT-Vorfällen mit Datenbanken**
  - Veröffentlichung firmeninterner Betriebsdaten
  - Pers. Daten der Belegschaft
- **Marktposition: relationale DBS**
  - Entwicklung von IT-Sicherheitskonzepten
- **Neue Anforderungen der Industrie**
  - Anzahl NoSQL-DBS: 225 [2]
  - Oftmals Open-Source Lösungen

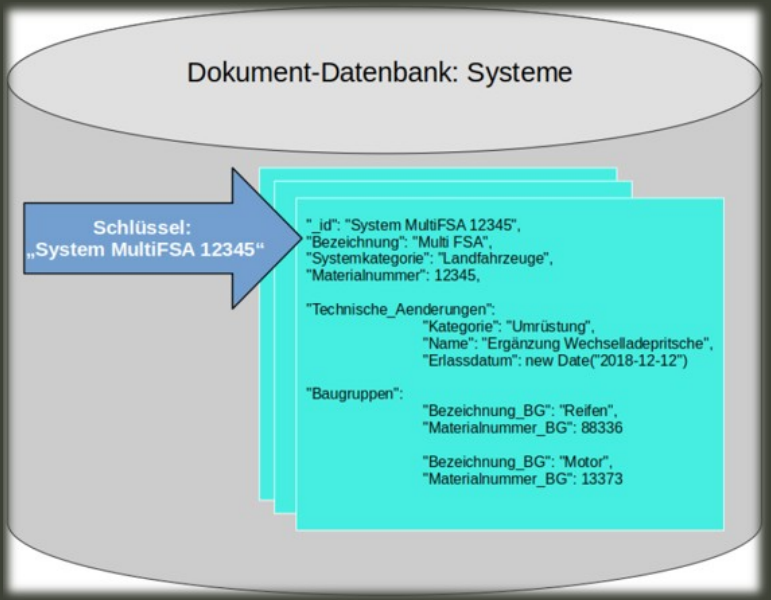
Quellen:

[2] NoSQL-Archiv: „List of NoSQL Database Management Systems.“ (19.10.2021)

Grundlagen Datenbanken

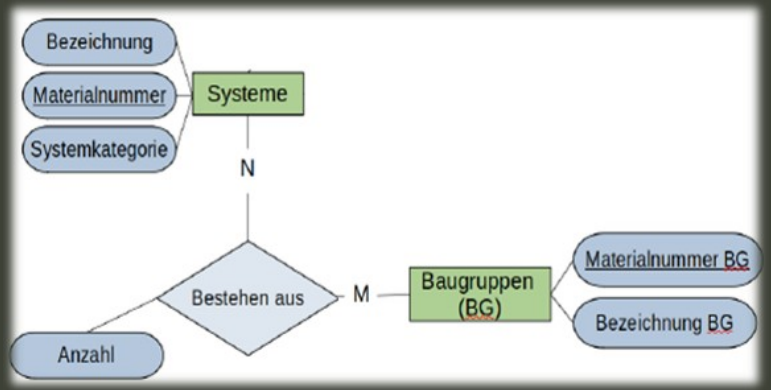
- **Relationale DBS vs. NoSQL-DBS**
- **Vorteile NoSQL-DBS:**
  - Performance / Latenzzeiten
  - Verfügbarkeit
  - Mehrfachzugriff
  - Mögliche Datenvielfalt
    - Neue „Datentypen“
- **Größter Nachteil NoSQL-DBS**
  - Oftmals fehlende Härtung

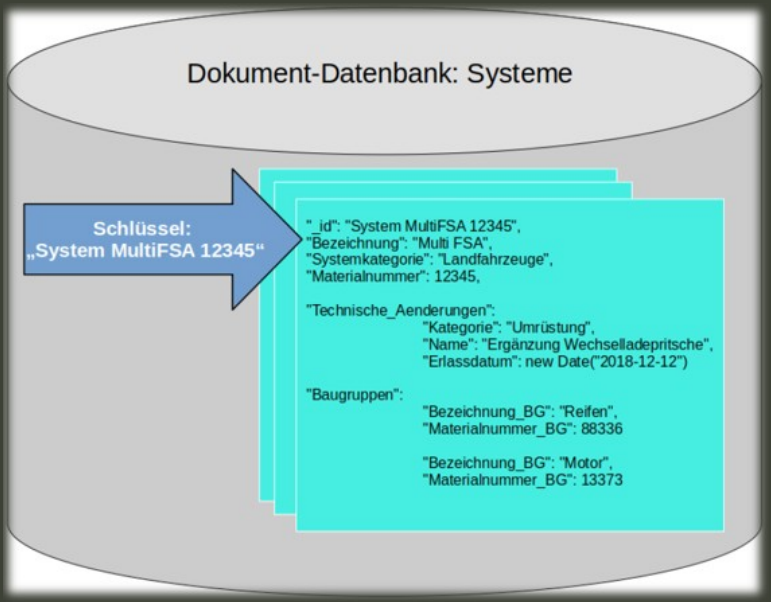




Grundlagen Datenbanken

Datenmodell	Leistung	Skalierbarkeit	Flexibilität	Komplexität
Key-Value	hoch	hoch	hoch	keine
Spalten-orientiert	hoch	hoch	mittel	gering
Dokument-orientiert	hoch	Unterschiedlich (hoch)	hoch	gering
Graphen-orientiert	unterschiedlich	unterschiedlich	hoch	hoch
Relational	unterschiedlich	unterschiedlich	gering	mittel





Grundlagen IT-Grundschutz

- **Leitfaden Umsetzung ISMS (national)**
- **Weitere Konzepte (international)**
  - „Common Criteria“ (4)
  - „Security Technical Implementation Guides“ (5)
- **Aufbau IT-Grundschutz des BSI**
  - BSI-Standards 200-1 bis 200-3 (100-4)
    - BSI-Standard 200-2: IT-Grundschutz-Methodik
  - IT-Grundschutz-Kompendium
    - System- und Prozessbausteine zur Modellierung

Bundesamt für Sicherheit in der Informationstechnik

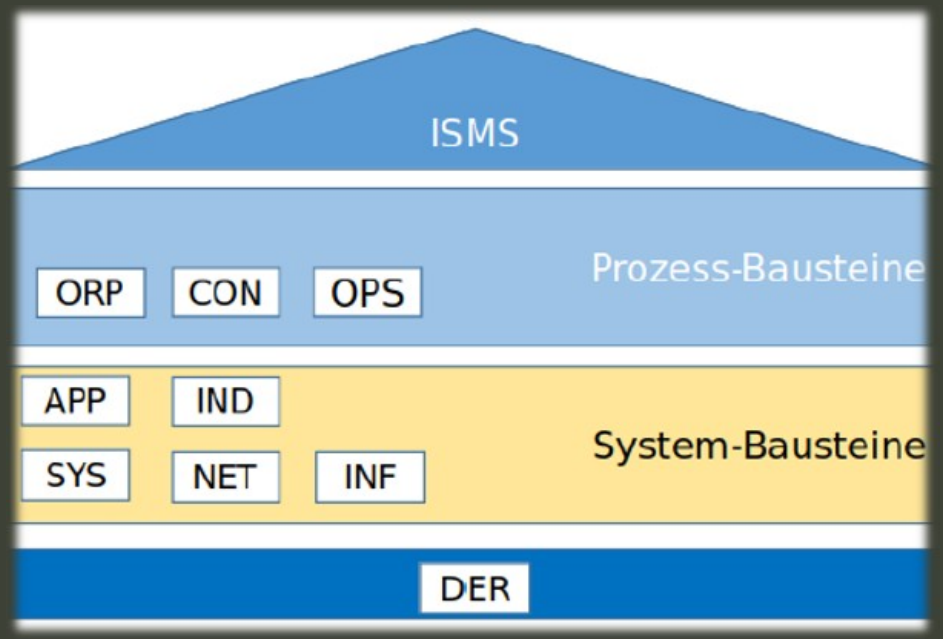


Abb: Schichtenmodell des BSI (3)

Quellen:
(3) Bundesamt für Sicherheit in der Informationstechnik: „IT-Grundschutz-Kompendium“
(4) Common Criteria: *“The Common Criteria for Information Technology Security Evaluation.”* (23.09.2021)
(5) DoD Cyber Exchange: *„Security Technical Implementation Guides.“* (23.09.2021)

Grundlagen IT-Grundschutz

- **Schicht ISMS**
  - **Grundlage für alle weiteren Aktivitäten: Baustein *„Sicherheitsmanagement“***
- **Schicht ORP**
  - **Organisatorische und personelle Sicherheitsaspekte, z.B. Baustein *„Organisation und Personal“***
- **Schicht CON**
  - **Konzepte und Vorgehensweisen, z.B. Baustein *„Datenschutz“***
- **Schicht OPS**
  - **Sicherheitsaspekte betrieblicher Art, z.B. Baustein *„Schutz vor Schadprogrammen“***

Bundesamt für Sicherheit in der Informationstechnik

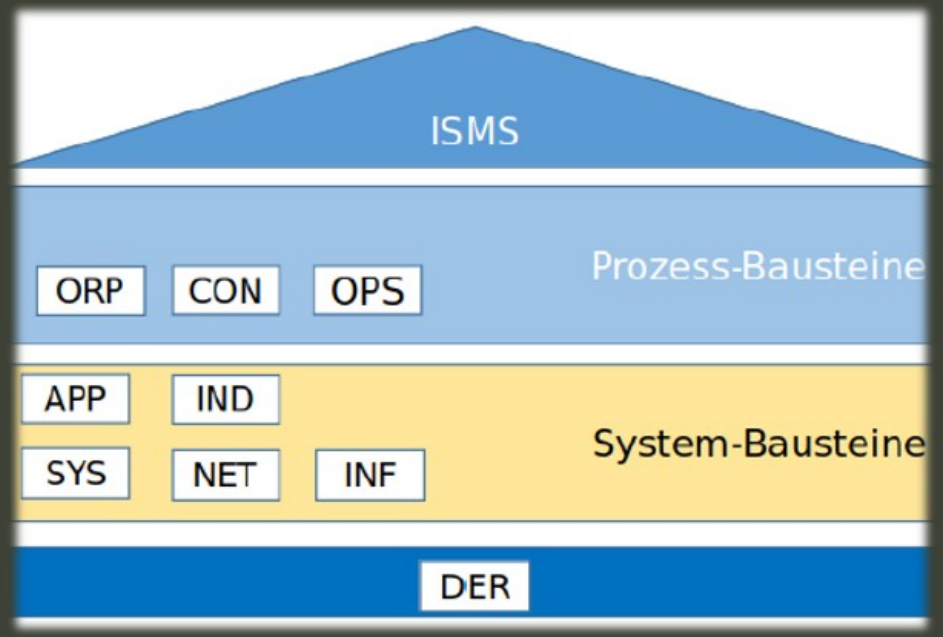


Abb: Schichtenmodell des BSI [3]

Quellen:
[3] Bundesamt für Sicherheit in der Informationstechnik: „IT-Grundschutz-Kompendium“

Grundlagen IT-Grundschutz

- **Schicht DER**
  - **Überprüfung der umgesetzten Sicherheitsmaßnahmen, z.B. Baustein *„Vorsorge für IT-Forensik“***

Bundesamt für Sicherheit in der Informationstechnik

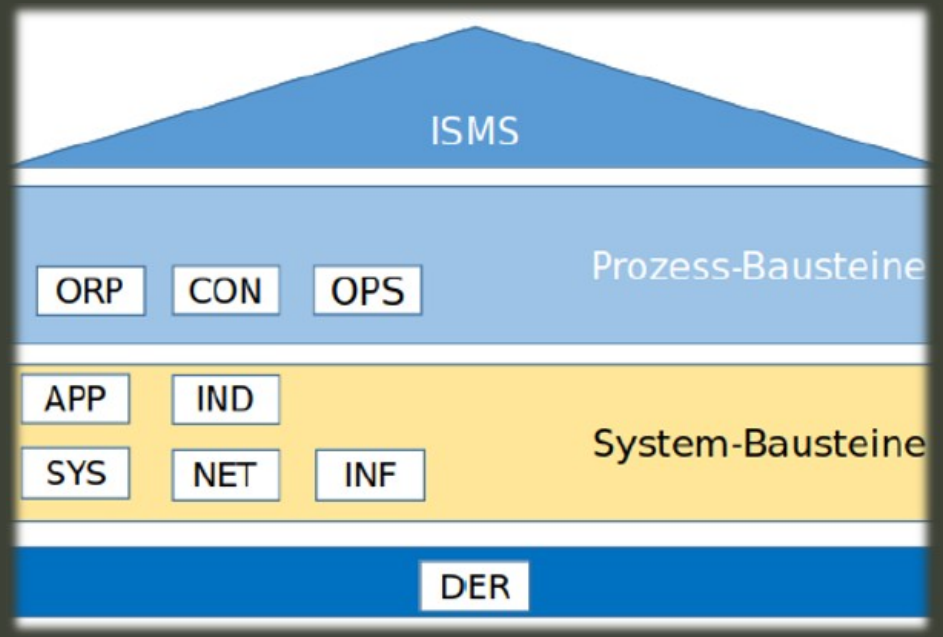


Abb: Schichtenmodell des BSI [3]

Quellen:

[3] Bundesamt für Sicherheit in der Informationstechnik: „IT-Grundschutz-Kompendium“

Grundlagen IT-Grundschutz

- **Schicht APP**
  - **Absicherung von Anwendungen, z.B. *„Relatioanle Datenbankmanagementsysteme“***
- **Schicht SYS**
  - **IT-Systeme des Informationsverbundes, z.B. *„Server, Drucker, Router“***
- **Schicht IND**
  - **Sicherheitsaspekte industrieller IT-Komponenten, z.B. *„Allgemeine ICS-Komponenten“***
- **Schicht NET**
  - **Betrachtung der Vernetzungsaspekte, z.B. Baustein „Firewall“**
- **Schicht INF**
  - **Betrachtung der baulich-technischen Gegebenheiten**

Bundesamt für Sicherheit in der Informationstechnik

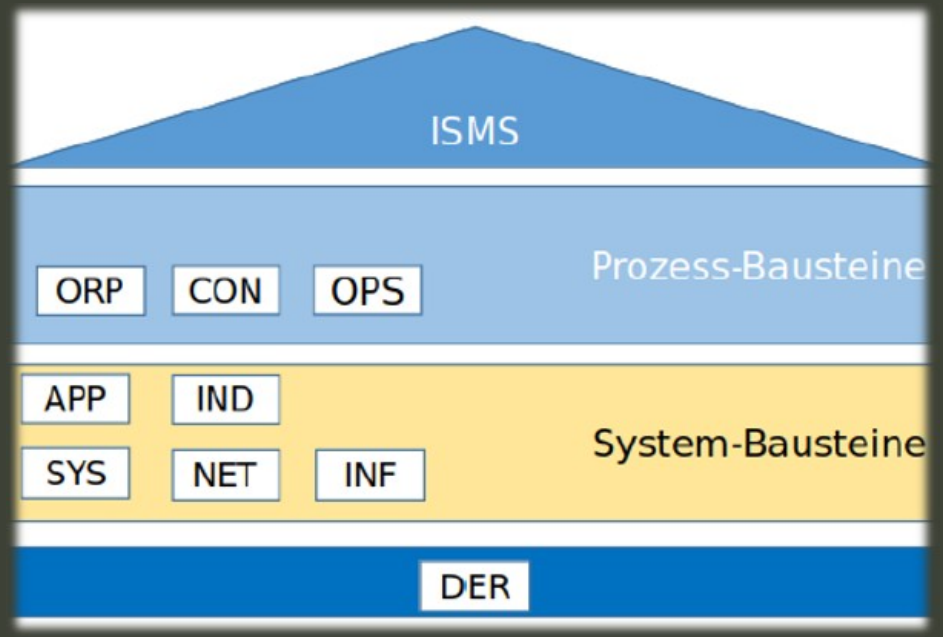


Abb: Schichtenmodell des BSI [3]

Quellen:

[3] Bundesamt für Sicherheit in der Informationstechnik: „IT-Grundschutz-Kompendium“

Modellierung Informationsverbund

- **Betrachtung eines Teilprozessschrittes**
  - „Modellierung“
- **Output aus „Strukturanalyse“**
  - „Auflistung aller IT-Komponenten“
  - Erhebung aus Netzplänen oder vorhandenen Inventarlisten
  - Erhebungsaufwand gering
  - Kombinierbar z.B. mit ITIL-Framework
- **Baukastenprinzip: Aufwand reduzieren**

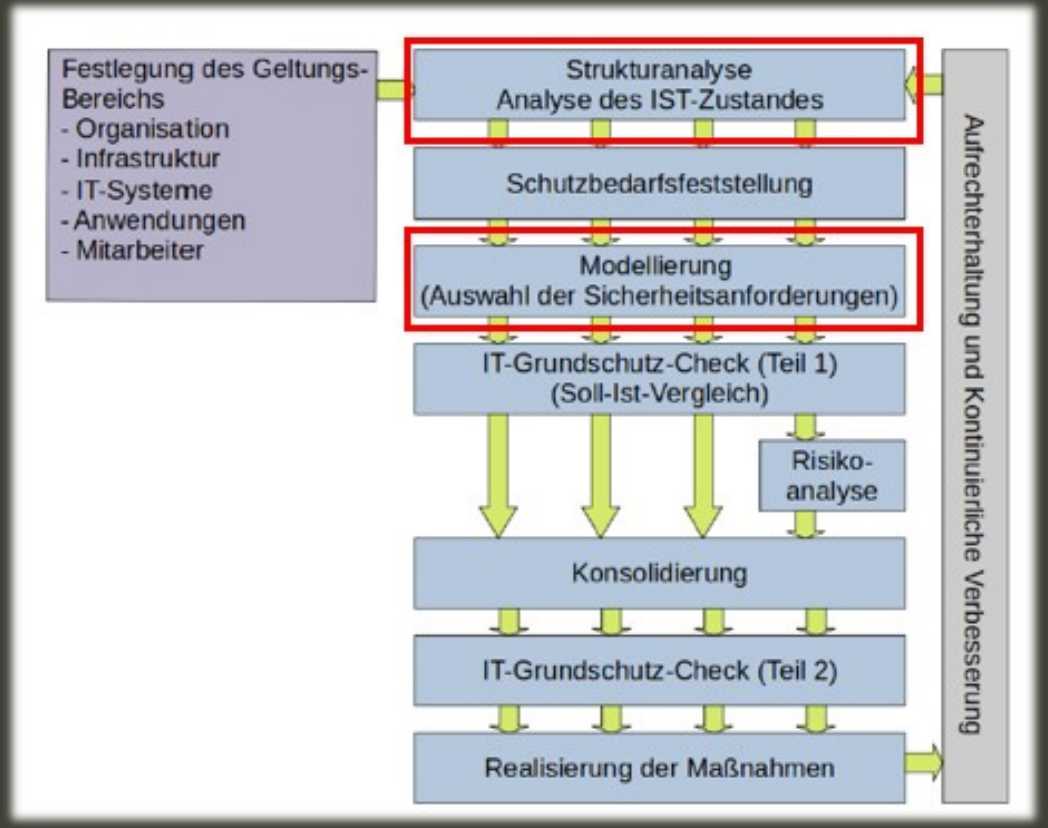


Abb: Vorgehensweise Sicherheitskonzeption nach Standard-Absicherung [6]

Quellen:

[6] Bundesamt für Sicherheit in der Informationstechnik: *„BSI-Standard 200-1“.*

Modellierung Informationsverbund

- **Von der Auflistung der IT-Komponenten zur Modellierung**

Bezeichnung	Beschreibung Zielobjekt/Gruppe	Plattform / Baustein
R1	Router Internetanbindung	Router/Switch
F1	Firewall Internet-Eingang	Firewall
SW1	Switch Verteilung	Router/Switch
S1	Print-Server	Server
S2	Server Allgemein	Server
VM1-3	Server Datenbanken	Virtuelle Server
C1-12	Mitarbeiter APC	Clients
...	...	...

Abb: Auflistung der IT-Komponenten

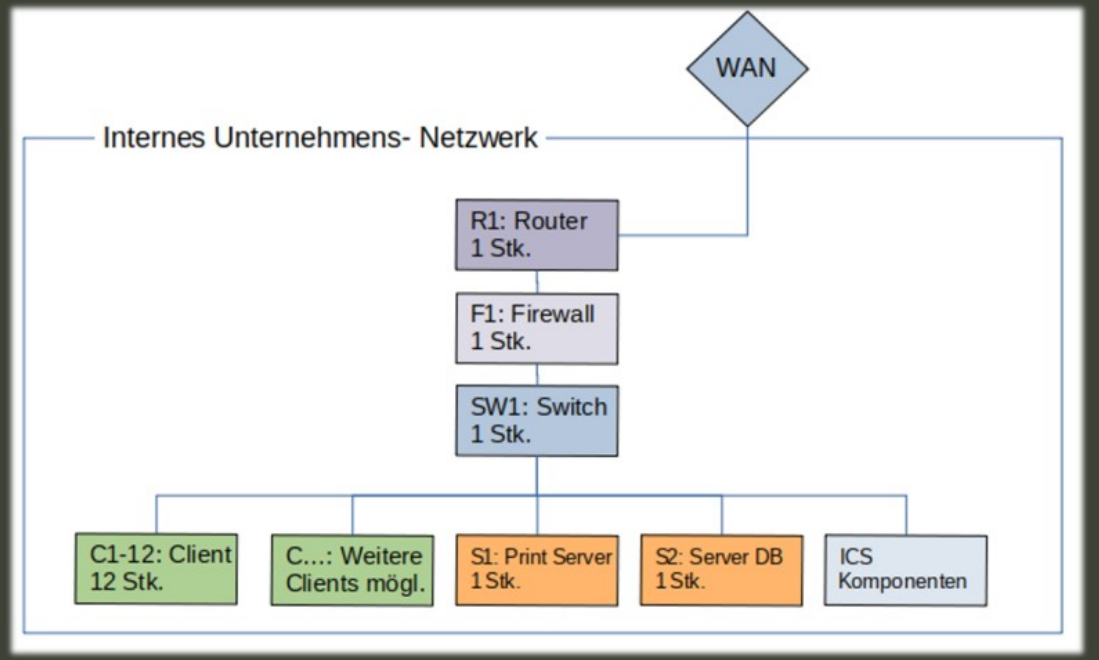
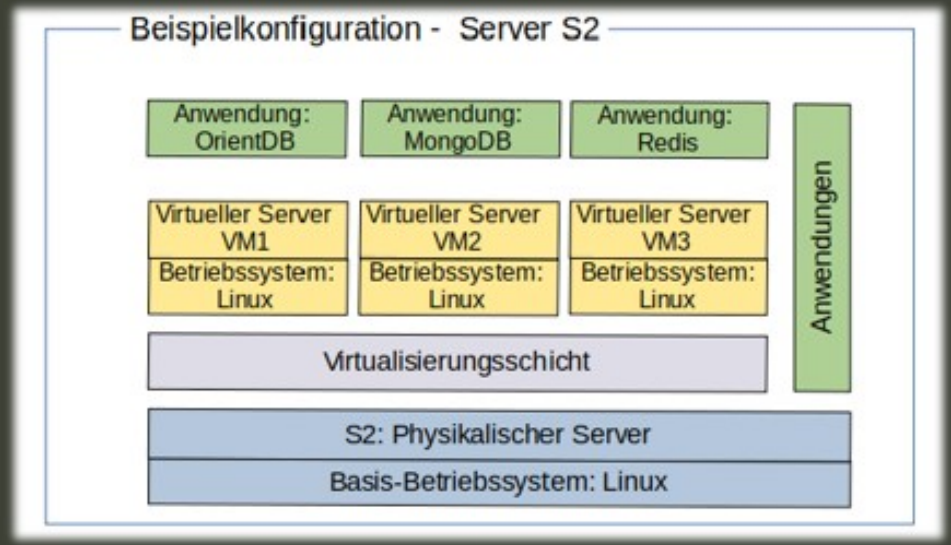


Abb: Zusammenfassung und Gruppenbildung

Modellierung Informationsverbund

- **Zusammenhänge verdeutlichen**
  - Beispiel: Server S2 und virtuelle Server VM1-VM3



Baustein Nr.	Relevanz	Priorität	Zielobjekt
…	…	…	…
SYS.1.1 - Allgemeiner Server	Ja	R2	IT-System (Phys. Server S2)
SYS.1.3 - Server unter Unix	Ja	R2	IT-System (Phys. Server S2)
SYS.1.5 - Virtualisierung	Ja	R2	IT-System (Phys. Server S2)
SYS.1.1 - Allgemeiner Server	Ja	R2	Gruppe aus VM1-VM3
SYS.1.3 - Server unter Unix	Ja	R2	Gruppe aus VM1-VM3
APP.4.3 - Relationale Datenbanken	Ja	R2	DBMS auf VM1 (OrientDB)
…	…	…	…

Vorbetrachtung Härtungsanalysen

- **Auswahl der betrachteten DBS**
  - Ziel: Variation NoSQL-DBS gewährleisten
- **Auswahl der relevanten Bausteine aus dem IT-Grundschutz-Kompendium**
  - Kern-Baustein: „APP.4.3 - Relationale Datenbank-managementsysteme“
  - Weitere betrachtete Bausteine:
    - APP.6 - Allgemeine Software
    - OPR.4 - Identitäts- und Berechtigungsmanagement
    - OPS.1.1.3 - Patch- und Änderungsmanagement
    - OPS.1.1.5 - Protokollierung

Durchführung Härtungsanalysen

- **Strukturierung der Anforderungen** [3]
  - Basisanforderungen
  - Standardanforderungen
  - Anforderungen für erhöhten Schutzbedarf

- **Technisch umsetzbare Anforderungen**
  - Konkrete Überprüfung der Umsetzbarkeit an den DBS (siehe Anlage E zur MT)

- **Organisatorische Anforderungen**
  - Umsetzungsvorschläge (z.B. Prozessgestaltung)

Quellen:
[3] Bundesamt für Sicherheit in der Informationstechnik: „IT-Grundschutz-Kompendium“

Durchführung Härtungsanalysen

Beispiel der Umsetzbarkeit einer technischen Anforderung

- APP.4.3.A9 – „Datensicherung eines Datenbanksystems“ [8]
  - »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.
- Ableitung Untersuchungskriterien
  - Arten von Systemsicherungsfunktionen
  - Einrichtung Automatischer Systemsicherung
  - Wiederherstellbarkeit Transaktionen
  - Inkrementelle Sicherung
  - Backup-Wiederherstellungsparameter

Quellen:
[8] Bundesamt für Sicherheit in der Informationstechnik: „Baustein APP.4.3 – Relationale Datenbanksysteme“

Durchführung Härtungsanalysen

Beispiel der Umsetzbarkeit einer technischen Anforderung

- APP.4.3.A9 – „Datensicherung eines Datenbanksystems“

Arten von Systemsicherungsfunktionen

BACKUP / RESTORE

```
orientdb {db=testdb}> BACKUP DATABASE
/tmp/orient_backup/backup1
Executing full backup of database ’testdb’ to: DATABASE
/tmp/orient_backup/backup1...
```

Einrichtung Autom. Systemsicherung

```
<handler class="com.orientechnologies.orient.server.handler.OAutomaticBackup">
    <parameters>
        <parameter value="false" name="enabled"/>
        <parameter value="${ORIENTDB_HOME}/config/automatic-backup.json" name=
    </parameters>
</handler>
```

Wiederherstellbarkeit Transaktionen

*Keine Unterstützung**

Inkrementelle Sicherung

(Nur Enterprise Version)

Backup-Wiederherstellungsparameter

Konfigurationsdatei für Parameter: „/config/automatic-backup.json“

*** Als implementierte Datenbankfunktion nicht unterstützt**

Durchführung Härtungsanalysen

Beispiel der Umsetzbarkeit einer technischen Anforderung

- APP.4.3.A9 – „Datensicherung eines Datenbanksystems“

Arten von Systemsicherungsfunktionen

mongodump / mongorestore

- mongodump --out=/data/mongodb/backup --collection= myCollection --db=test
- mongorestore /data/mongodb/backup

Einrichtung Autom. Systemsicherung

*Keine Unterstützung**

Wiederherstellbarkeit Transaktionen

*Keine Unterstützung**

Inkrementelle Sicherung

(Nur Enterprise Version)

Backup-Wiederherstellungsparameter

Konfigurationsdatei für Parameter: „mongo.conf“

*** Als implementierte Datenbankfunktion nicht unterstützt**

Durchführung Härtungsanalysen

Beispiel der Umsetzbarkeit einer technischen Anforderung

- APP.4.3.A9 – „Datensicherung eines Datenbanksystems“

Arten von Systemsicherungsfunktionen

RDB / save / bgsave
>./redis-cli
127.0.0.1:6379> AUTH default xxx
127.0.0.1:6379> save
OK

Einrichtung Autom. Systemsicherung

127.0.0.1:6379> save 60 100

Wiederherstellbarkeit Transaktionen

AOF
127.0.0.1:6379> set appendonly yes
127.0.0.1:6379> set appendonly everysec

Inkrementelle Sicherung

*BGWRITEAOF**

Backup-Wiederherstellungsparameter

Konfigurationsparameter (Auszug):
M, N, appendfsync

*** Ermittlung der kürzesten Befehlssequenz zur Herstellung des aktuellen DB-Zustands**

Durchführung Härtungsanalysen

Beispiel der Umsetzbarkeit einer Organisatorischen Anforderung

- APP.4.3.A17 – „Datenübernahme oder Migration“ [8]
  - » Es SOLLTE vorab definiert werden, wie initial oder regelmäßig Daten in eine Datenbank übernommen werden sollen. Nachdem Daten übernommen wurden, SOLLTE geprüft werden, ob sie vollständig und unverändert sind.

- Datenmigrationen oftmals nicht zeitlich planbar
- Möglichkeiten der „präventiven Planung“
  - Dimensionspuffer beim Anlegen neuer DB
- Faktoren zur Festlegung der Migrationsmethoden
  - Vorhandene Ressourcen
  - Ausfallzeiten der Datenbank/en
  - Risiken bei der Migration
  - Konsistenz der Daten

Quellen:
[8] Bundesamt für Sicherheit in der Informationstechnik: „Baustein APP.4.3 – Relationale Datenbanksysteme“

Durchführung Härtungsanalysen

Beispiel der Umsetzbarkeit einer Organisatorischen Anforderung

- APP.4.3.A17 – „Datenübernahme oder Migration“

Formblatt X.11: Anforderung zum Anlegen neuer Date

Vom Anfordernden auszufülle

Name der Datenbank	**Zweck der Date**
Kundenstammdatenbank	Speichern von Ku Vertriebsmitarbei
Name Anfordernder	**Fachabteilung**
Mustermann	Vertrieb/Verkauf

Zu speichernde Daten/Informationen

Art der Daten	**Geschätzter Umfang der Daten**
- Kundenname - Kundennummer - Adresse - Telefonnummer - Kategorisierung	Ca. 1000 Datensätze pro Kunde

Formblatt X.12: Anforderung der Datenmigration in eine Datenbank

Vom Anfordernden auszufüllen

Name der Ziel-Datenbank	**Name Anfordernder**
Kundenstammdatenbank	Mustermann
Grund der Migration	**Fachabteilung**
Migration auf neuen DB-Server; Dimensionierung aktueller DB-Server nicht ausreichend	Vertrieb/Verkauf

Zu migrierende Daten

Art der Daten und Quellformat	**Umfang der zu migrierenden Daten**	**Gewünschter Zeitraum der Migration**
- Kundenname, String - Kundennummer, Integer - Adresse, String - Telefonnummer, String - Kategorisierung, String	Ca. 200.000 Datensätze	Oktober 2021
Quellsystem / Quell-DB	**Version Quell-DB**	**Turnus der Migration (nur bei regelmäßigen Migrationen)**
SAP HANA	X.Y 3	
Faktoren der Migration		

Welcher Migrationsfaktor hat die größte Bedeutung für den Antragsteller?
Bitte einen Schwerpunkt gemäß der folgenden Faktoren definieren

Geringe Ausfallzeit	**X**	**Konsistenz der Daten**		**Geringes Verlustrisiko**	

Auswertung Härtungsanalysen

- **Festlegung der Bewertungskriterien**
  - Angelehnt an Checkliste BSI zum Baustein „APP4.3. - Relationale Datenbanksysteme“
- **Auswertung techn. Anforderungen je untersuchtem Baustein**
- **Zusammenfassung der Ergebnisse je Baustein zu Gesamtauswertung**

Erfüllung	Beschreibung	Zahlenwert
„Ja“	Vollständige Umsetzung im DBS möglich	2
„teilw.“	Teilweise Umsetzung im DBS möglich	1
„nein“	Keine Umsetzung im DBS möglich	0

Anf.	Titel	Orient DB	Mongo DB	Redis	Art
ORP.4.A8	Regelungen Passwort	2	1	1	Techn.
ORP.4.A15	Konzeption der Prozesse	0	0	0	Org.
ORP.4.A16	Richtlinien Zugriff u. Zugang	2	2	1	Techn.

Auswertung Härtungsanalysen

DBMS	Gesamterfüllung Abs.	Gesamterfüllung Rel. [%]
OrientDB	17	61
MongoDB	17	61
Redis	15	54

Diskussion/Fazit

- **Keines der untersuchten DBMS konnte mehr als 61% der Bewertungspunkte erreichen**

DBMS	Gesamter-füllung Abs.	Gesamter-füllung Rel. [%]
OrientDB	17	61
MongoDB	17	61
Redis	15	54

- **Alle drei betrachteten DBMS besitzen z.T. unsichere Standard-Konfigurationen**
  - Bsp: Deaktivierte Authentifizierung-smechanismen (MongoDB, Redis)

- **Wichtige Sicherheitsfunktionen, z.B. Auditing- und erweiterte Logging-Funktionen nicht in Community Versionen NoSQL-DBMS abgebildet**
  - Einsatz in Produktivumgebungen nahezu ausgeschlossen

Diskussion/Fazit

- **Das IT-Grundschutz-Kompendium bietet Unternehmen Handlungshilfen zur Etablierung eines ISMS**
  - Neue Technologien müssen zeitgerecht berücksichtigt werden, z.B. NoSQL-DBMS
  - Erweiterung durch neue Bausteine notwendig
- **DB-Administratoren benötigen spezielles Fachwissen hinsichtlich NoSQL-Datenbanken**
- **Organisatorische Maßnahmen: Prozesse**

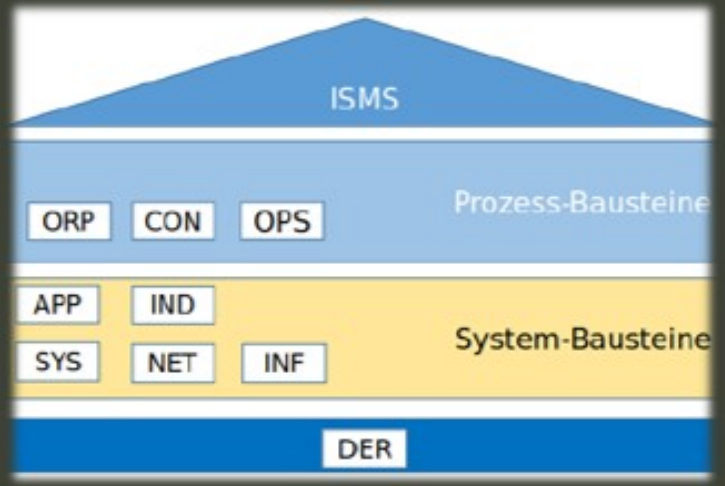


Abb: Schichtenmodell des BSI [3]

Quellen:
[3] Bundesamt für Sicherheit in der Informationstechnik: „IT-Grundschutz-Kompendium“

Diskussion/Fazit

Vielen Dank für Ihre Aufmerksamkeit!