Konzeption eines Vorgehensmodells zur Ableitung von Härtungsmaßnahmen für nicht-relationale Datenbanksysteme

- Motivation

- Grundlegende Konfigurations- und Konformitätsrichtlinien
- Entwicklung und Anwendung des Vorgehensmodells

- Live-Demonstration des InSpec Compliance-Profils für Redis

- Auswertung der Anwendung des Vorgehensmodells
- Zusammenfassung und Ausblick

Lukas Zorn

Fakultät für Ingenieurwissenschaften \ Bereich Elektrotechnik und Informatik

HOCHSCHULE WISMAR
UNIVERSITY OF APPLIED SCIENCES TECHNOLOGY, BUSINESS AND DESIGN

Motivation

- **Anstieg der Schäden um 97,09 % innerhalb von etwa 3 Jahren**
  - Bitkom 2022: „203 Mrd. EUR Schaden pro Jahr durch Cyberangriffe”
  - Bitkom 2018/19: „103 Mrd. EUR Schaden pro Jahr durch Cyberangriffe”

- **Anstieg der Cyberkriminalität bei zugleich rückläufiger Aufklärungsquote**
  - Jahr 2020: Zunahme um 6,3 % bei einer Aufklärungsquote von 32 %
  - Jahr 2021: Zunahme um 12,2 % bei einer Aufklärungsquote von 29,3 %
  - Jahr 2022: Keine Trendwende zu erwarten

Motivation

- **Herausforderungen durch die Corona-Pandemie seit 2020**
  - Zunehmende Vernetzung und Digitalisierung von Infrastrukturen
  - Zeitkritische Umsetzung ohne umfassende Berücksichtigung der IT-Sicherheit

- **Herausforderungen durch den Angriffskrieg auf die Ukraine seit 2022**
  - Wachsende Bedeutung staatlicher sowie geduldeter Cybercrime-Akteure
  - Politisch unabhängig geglaubte Gruppierungen greifen in den Konflikt ein

➢ **Folgen der Missachtung von IT-Sicherheit werden nun überdeutlich**

Motivation

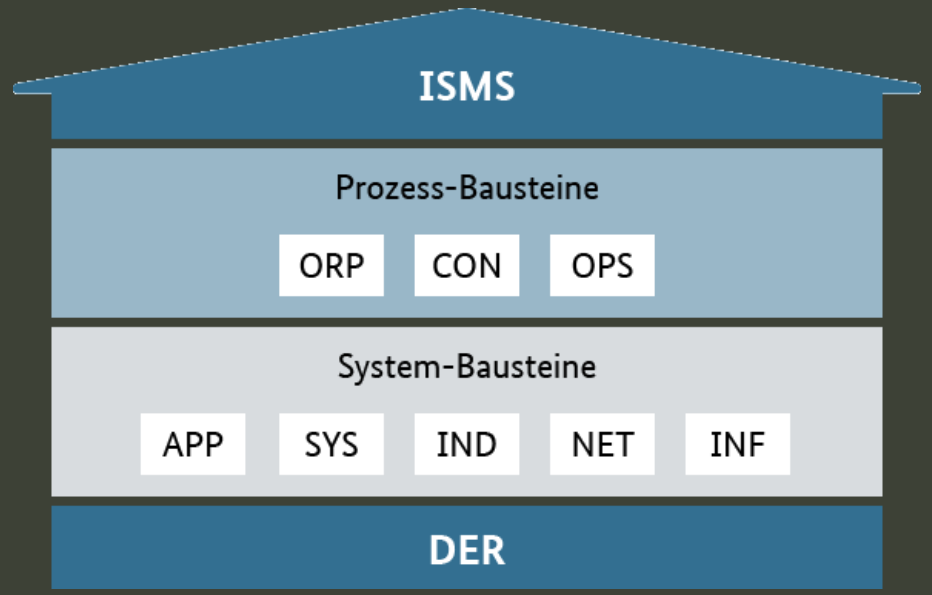
- **NoSQL-DBS im Zentrum moderner Anwendungen**
  - Anzahl an NoSQL-DBS ≈ 300
  - Hohe Relevanz: Steigende Datenmengen und Entwicklungsaufwand

- **Enormes Schadenspotenzial durch Kompromittierung von Datenbanken**
  - Sensible Mitarbeiterdaten bis hin zu kritischen Geschäftsdaten
  - Lediglich vereinzelte Absicherungs-/Härtungsstandards verfügbar

➢ **Vorgehensmodell zur Härtung von NoSQL-DBS von großer Bedeutung**

Grundlegende Konfigurations- und Konformitätsrichtlinien BSI IT-Grundschutz

- **Ganzheitlicher Ansatz zur IT-Sicherheit**
  - ISMS-Leitfaden
- **Vorgehensweisen**
  - BSI Standard 200-1 bis 200-3
  - BSI Standard 100-4 (bald 200-4)
- **Konkrete Anforderungen**
  - BSI IT-Grundschutz-Kompendium



Grundlegende Konfigurations- und Konformitätsrichtlinien
BSI Technische Richtlinien

- **Definierung von IT-Sicherheitsstandards**
  - Ergänzung der Prüfvorschriften des BSI
  - Kriterien und Methoden für Konformitätsprüfungen

- **BSI-TR-02102: Kryptographische Verfahren**
  - BSI TR-02102-1: Empfehlungen und Schlüssellängen
  - BSI TR-02102-2: Transport Layer Security (TLS)
- **BSI-TR-02103: X.509-Zertifikate**
- **BSI-TR-03111: ECC-Kryptographie**

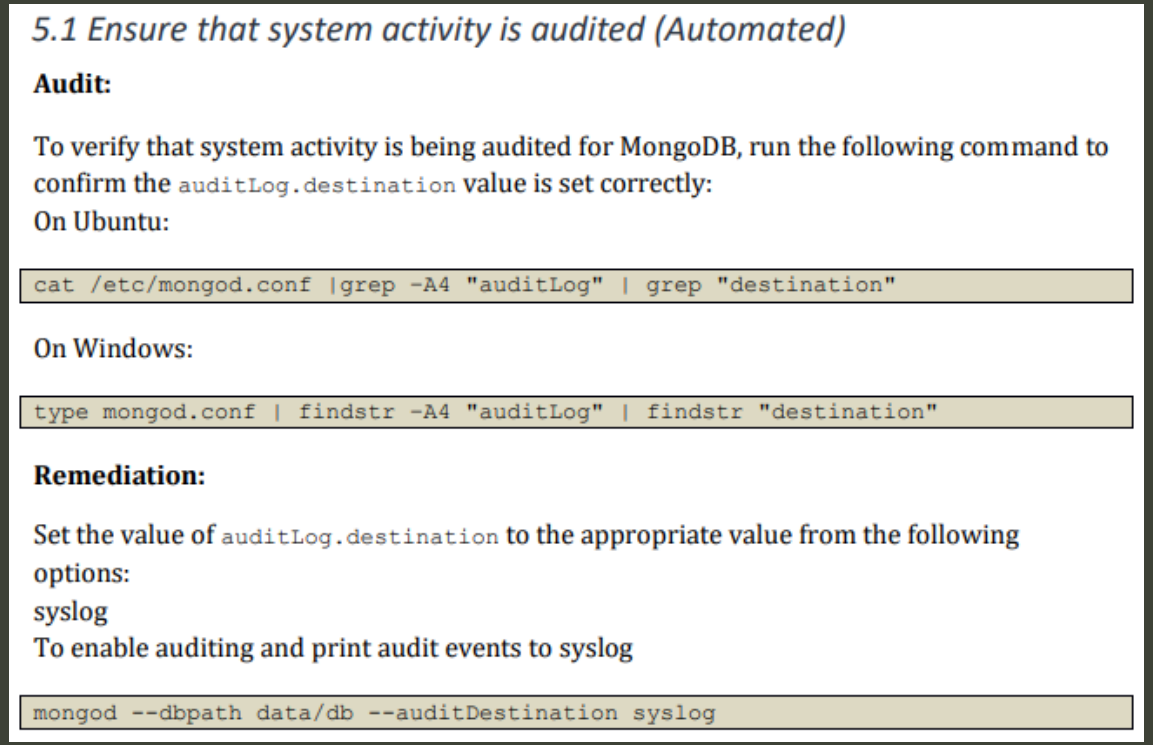
Grundlegende Konfigurations- und Konformitätsrichtlinien Center for Internet Security (CIS) Benchmarks und Controls

- **Center for Internet Security**
  - Non-Profit-Organisation
  - Gegründet Oktober 2000, New York
  - Bündelung von Kompetenzen

- **CIS-Controls**
  - Liste von 18 Schlüsselmaßnahmen
  - Vergleich BSI IT-Grundschutz-Kompendium

Grundlegende Konfigurations- und Konformitätsrichtlinien
Center for Internet Security Benchmarks und Controls

- **CIS-Benchmarks**
  - Konkrete technische Leitlinien
    - (Mobile) Betriebssysteme
    - Desktop- und Server-Anwendungen
    - Cloud-Anbieter
    - Netzwerkgeräte
    - Drucker
  - Konsensprozess
  - Für nicht-kommerzielle Zwecke kostenlos
  - Anzahl an Benchmarks ≈ 213



5.1 Ensure that system activity is audited (Automated)

Audit:

To verify that system activity is being audited for MongoDB, run the following command to confirm the `auditLog.destination` value is set correctly:
On Ubuntu:

```
cat /etc/mongod.conf |grep -A4 "auditLog" | grep "destination"
```

On Windows:

```
type mongod.conf | findstr -A4 "auditLog" | findstr "destination"
```

Remediation:

Set the value of `auditLog.destination` to the appropriate value from the following options:
syslog
To enable auditing and print audit events to syslog

```
mongod --dbpath data/db --auditDestination syslog
```

Grundlegende Konfigurations- und Konformitätsrichtlinien Security Technical Implementation Guides (STIGs)

- Konkrete technische Leitlinien
- Veröffentlicht von der Defense Information Systems Agency (DISA)
- Absicherung von IA-aktivierten Geräten/-Systemen
- Absicherung von Systemen des DoD
- Gesonderte CIS-STIG-Benchmarks für Betriebssysteme
  - Red Hat Enterprise Linux 7 & 8
  - Ubuntu Linux 20.04 LTS
  - Amazon Linux 2
  - Microsoft Windows Server 2016 & 2019

Entwicklung des Vorgehensmodells
Vorgehensweise und Geltungsbereich

- **Grundlage BSI-Bausteine, CIS-Benchmarks und STIGs-Leitfäden**
  - Untersuchung alle BSI IT-Grundschutz Bausteine
  - Untersuchung mehrerer CIS-Benchmarks
  - Untersuchung mehrerer STIGs-Leitfäden

- **Begrenzung auf ausgewählte CIS- und STIGs-Standards**

- **Begrenzung des Geltungsbereichs auf technische Maßnahmen**
  - Fokussierung auf Härtungsmaßnahmen, nicht auf deren Auswirkungen

Entwicklung des Vorgehensmodells
Untersuchung der BSI IT-Grundschutz Bausteine

ORP.4	Identitäts- und Berechtigungsmanagement	32 Maßnahmen
CON.1	Kryptokonzept	13 Maßnahmen
CON.8	Software-Entwicklung	9 Maßnahmen
CON.10	Entwicklung von Webanwendungen	2 Maßnahmen
OPS.1.1.3	Patch- und Änderungsmanagement	3 Maßnahmen
OPS.1.1.4	Schutz vor Schadprogrammen	1 Maßnahme
OPS.1.1.5	Protokollierung	7 Maßnahmen
APP.4.3	Relationale Datenbanksysteme	10 Maßnahmen
APP.6	Allgemeine Software	5 Maßnahmen

Entwicklung des Vorgehensmodells
Untersuchung der BSI IT-Grundschutz Bausteine

- Satzweise Untersuchung jeder Anforderung
- Begründung bei Nichtberücksichtigung
- Vergabe einer fortlaufenden Nummer mit Präfix „B“
- Identifikation von 82 BSI-Anforderungen

ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen [IT-Betrieb] (B)

× **„Es MUSS geregelt werden, wie Benutzerkennungen und Benutzergruppen einzurichten und zu löschen sind.“**
Entfällt, da die Verwaltung von Benutzerkennungen und Benutzergruppen nicht über eine technische Konfigurationsanpassung abgebildet werden kann, sondern durch organisatorische, prozessuale Maßnahmen umgesetzt werden muss.

× **„Jede Benutzerkennung MUSS eindeutig einem Benutzer zugeordnet werden können.“**
Entfällt, da die Zuordnung von Benutzerkennungen durch ein externes IT-System, wie z. B. ein IAM- oder Identity Management (IdM)-System, oder alternativ durch organisatorische, prozessuale Maßnahmen umgesetzt werden muss.

B1 **„Benutzerkennungen, die längere Zeit inaktiv sind, SOLLTEN deaktiviert werden.“**

B2 **„Alle Benutzer und Benutzergruppen DÜRFEN NUR über separate administrative Rollen eingerichtet und gelöscht werden.“**

B3 **„Nicht benötigte Benutzerkennungen, wie z. B. standardmäßig eingerichtete Gastkonten oder Standard-Administratorkennungen, MÜSSEN geeignet deaktiviert oder gelöscht werden.“**

Entwicklung des Vorgehensmodells
Untersuchung der CIS-Benchmarks

- CIS Apache Cassandra 3.11 Benchmark — 16 Maßnahmen
- CIS MongoDB 5 Benchmark — 22 Maßnahmen
- CIS PostgreSQL 14 Benchmark — 47 Maßnahmen

➢ Auslassung des CIS IBM Db2 11 Benchmarks

Entwicklung des Vorgehensmodells
Untersuchung der CIS-Benchmarks

- Untersuchung jeder Kontrolle
- Begründung bei Nichtberücksichtigung
- Vergabe einer fortlaufenden Nummer mit Präfix „C“
- Identifikation von 85 CIS-Anforderungen

PostgreSQL-Einstellungen

× **„Stellen Sie sicher, dass die Backend-Laufzeitparameter ordnungsgemäß konfiguriert sind.“**
Entfällt, da es sich um Konfigurationsanpassungen handelt, die nur speziell für PostgreSQL umgesetzt werden können.

× **„Stellen Sie sicher, dass die Postmaster-Laufzeitparameter ordnungsgemäß konfiguriert sind.“**
Entfällt, da es sich um Konfigurationsanpassungen handelt, die nur speziell für PostgreSQL umgesetzt werden können.

× **„Stellen Sie sicher, dass die SIGHUP-Laufzeitparameter ordnungsgemäß konfiguriert sind.“**
Entfällt, da es sich um Konfigurationsanpassungen handelt, die nur speziell für PostgreSQL umgesetzt werden können.

× **„Stellen Sie sicher, dass die Superuser-Laufzeitparameter ordnungsgemäß konfiguriert sind.“**
Entfällt, da es sich um Konfigurationsanpassungen handelt, die nur speziell für PostgreSQL umgesetzt werden können.

× **„Stellen Sie sicher, dass die User-Laufzeitparameter ordnungsgemäß konfiguriert sind.“**
Entfällt, da es sich um Konfigurationsanpassungen handelt, die nur speziell für PostgreSQL umgesetzt werden können.

C78 **„Stellen Sie sicher, dass FIPS 140-2 OpenSSL-Kryptographie verwendet wird.“**

Entwicklung des Vorgehensmodells
Untersuchung der Security Technical Implementation Guides

- MongoDB Enterprise Advanced 4.x STIG V1, R1 45 Maßnahmen

- Redis Enterprise 6.x STIG V1, R1 70 Maßnahmen

➢ Auslassung des IBM DB2 V10.5 STIG V1, R4

Entwicklung des Vorgehensmodells
Untersuchung der Security Technical Implementation Guides

- Untersuchung jeder Schwachstellen-ID
- Begründung bei Nichtberücksichtigung
- Vergabe einer fortlaufenden Nummer mit Präfix „S“
- Identifikation von 115 STIGs-Anforderungen

S26	**„MongoDB muss die Vertraulichkeit und Integrität aller Informationen im laufenden Betrieb schützen.“**
×	**„Der Datenbankinhalt muss durch die Durchsetzung einer Datenübertragungsrichtlinie vor unbefugter und unbeabsichtigter Informationsübertragung geschützt werden.“** Entfällt, da dies durch organisatorische, prozessuale Maßnahmen umgesetzt werden muss.
S27	**„MongoDB muss die Gültigkeit aller Dateneingaben prüfen, mit Ausnahme derjenigen, die von der Organisation speziell festgelegt wurden.“**
S28	**„MongoDB muss nicht-privilegierten Benutzern Fehlermeldungen zur Verfügung stellen, die Informationen für Korrekturmaßnahmen liefern, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten.“**
S29	**„MongoDB darf detaillierte Fehlermeldungen nur dem ISSO, ISSM, SA und DBA offenbaren.“**
S30	**„MongoDB muss eine Benutzersitzung automatisch beenden, wenn organisationsdefinierte Bedingungen oder Trigger-Ereignisse ein Trennen der Sitzung erfordern.“**
S31	**„MongoDB muss eine zentrale Verwaltung des Inhalts der von allen MongoDB-Komponenten erzeugten Audit-Datensätze nutzen.“**
S32	**„MongoDB muss die Speicherkapazität für Audit-Datensätze in Übereinstimmung mit den Speicheranforderungen für Audit-Datensätze am Standort zuweisen.“**

Entwicklung des Vorgehensmodells
Zusammenführung der BSI-, CIS- und STIGs-Anforderungen

- **Angabe der zugrundliegenden Einzelanforderungen**
- **Angabe einer Anforderungsbeschreibung**
  - Inhalt und Zweck der Anforderung
  - IT-Sicherheitstechnischer Hintergrund der Anforderung
  - Zugabe weiterer Anforderungen aus BSI-TR, Best-Practices
- **Angabe von Umsetzungshinweisen**
  - Was muss beachtet werden?
  - Sind Alternativansätze möglich?
  - Gibt es sonstige Einschränkungen?

Entwicklung des Vorgehensmodells
Beispiel der Anforderung A60

A59 Das für den Schlüsselaustausch verwendete Verfahren muss sicher sein.

BSI: B39 | **STIGs:** S25

Beschreibung Ein Schlüsselaustauschprotokoll dient dem Austausch eines gemeinsamen, geheimen Schlüssels zwischen mehreren Verbindungspartnern über einen unsicheren Kommunikationskanal. Zu diesem Zweck kann ein geeignetes sicheres kryptografisches Verfahren aus dem Bereich der asymmetrischen Kryptografie verwendet werden, um einen einmaligen Schlüssel im Rahmen des Verbindungsaufbaus zu vereinbaren. In BSI-TR-02102-2 werden die folgenden Schlüsselaustauschprotokolle empfohlen:

- Elliptic Curve Diffie-Hellman Ephemeral (ECDHE),
- Diffie-Hellman Ephemeral (DHE).

Alternativ kann auch ein zuvor vereinbarter statischer Schlüssel (Pre-Shared-Key) verwendet werden, z. B. im Rahmen des Cluster-Betriebs.

Umsetzung Das DBMS muss daraufhin untersucht werden, ob die Verwendung von ECDHE und/oder DHE konfiguriert und alle abweichenden Schlüsselaustauschprotokolle deaktiviert werden können. Sollte es nicht möglich sein, Perfect Forward Secrecy (PFS) als Grundbedingung für die Inanspruchnahme der ephemeren Protokollvarianten zu verwenden, ist alternativ auch die Verwendung der entsprechenden Schlüsselaustauschprotokolle ohne dieses Merkmal möglich. Diese müssen jedoch spätestens nach 2026 einer Sicherheitsbewertung unterzogen werden.

- Vergabe einer fortlaufenden Nummer mit Präfix „A“

➢ **Formulierung von 82 Anforderungen für NoSQL-DBS**

Entwicklung des Vorgehensmodells
Sonderstellung der Anforderung A1

A1 Die Standardwerte aller sicherheitsrelevanten Konfigurationsparameter müssen explizit festgelegt werden.

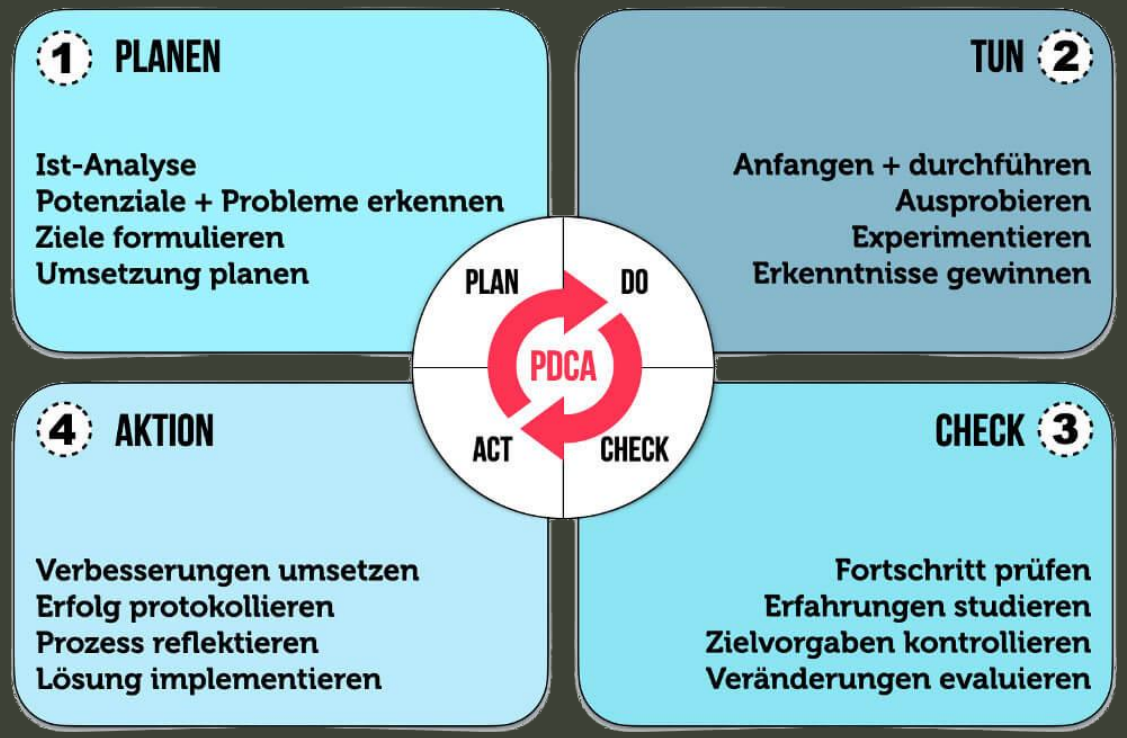
BSI: B47, B80 | **STIGs:** S45, S76

Beschreibung Zur Identifikation aller sicherheitsrelevanten Konfigurationsparameter ist grundsätzlich ein holistischer Ansatz zu verfolgen. Die vorliegenden Anforderungen, die auf einer komprimierten Zusammenfassung von 282 Einzelanforderungen aus 6 verschiedenen Leitfäden beruhen, decken nahezu alle Maßnahmen ab, die aus technischer Sicht im Zusammenhang mit dem sicheren Betrieb von nicht-relationalen Datenbanksystemen zu berücksichtigen sind. Dennoch müssen weiterhin sämtliche Konfigurationsparameter über die hier vorgenommene Klassifizierung hinaus auf ihre sicherheitstechnische Relevanz hin analysiert und gegebenenfalls mit einem sicheren Konfigurationswert versehen werden. Dies liegt zum einen an der großen Vielfalt nicht-relationaler Datenbanksysteme, die zum Teil auf die Ausschlussdefinition des Begriffs selbst zurückzuführen ist, und zum anderen an der hohen Geschwindigkeit der Weiterentwicklung, sodass eine Abdeckung aller sicherheitsrelevanten Aspekte in einem Vorgehensmodell nicht abschließend sichergestellt werden kann. Dies ist insbesondere auch dann von Bedeutung, wenn der Standardwert des jeweiligen Konfigurationsparameters bereits einer sicheren Konfiguration entspricht, da sich Standardwerte durch die Installation von Updates nachträglich negativ verändern können.

Umsetzung Die Dokumentation des DBMS ist auf sicherheitsrelevante Konfigurationsparameter zu untersuchen. Außerdem sollen die Inhalte der Standard-Konfiguration und die Empfehlungen aus Best-Practice-Ansätzen bei der Untersuchung berücksichtigt werden, da insbesondere bei Open-Source-Projekten neue Parameter und Funktionalitäten mitunter erst verzögert in der Dokumentation beschrieben werden.

➢ **Integration eines PDCA-Zyklus**

Entwicklung des Vorgehensmodells
Sonderstellung der Anforderung A1



- **Demingkreis-Implementierung**
  - Ausschlussdefinition „NoSQL“
  - Hoher Abdeckungsbedarf
  - Sammelbecken für nicht-zuordenbare Maßnahmen

➢ **Grundlage für Fortschreibung und Weiterentwicklung**

Anwendung des Vorgehensmodells
Auswahl der zu untersuchenden NoSQL-DBS

- **Neo4j 5.1.0 Community-Edition**
  - Veröffentlichung von Version 5.x erst im Oktober 2022
  - Noch keine Absicherungsstandards seitens CIS oder STIGs vorhanden
  - Hohe Popularität im Bereich der Graphdatenbanken

- **Redis 7.0.4 Community-Edition**
  - Noch keine Absicherungsstandards für Version 7 vorhanden
  - STIGs für Version 6 der Enterprise-Edition vorhanden
  - Hohe Popularität im Bereich der Schlüssel-Werte-Datenbanken

Anwendung des Vorgehensmodells
Vorgehensweise

- **Untersuchung mehrerer Quellen**
  - Hersteller-Dokumentationen
  - Hersteller-Guidelines
  - Mitgelieferter Standard-Konfigurationen
  - Best-Practice-Ansätze von Dritten

- **Ausarbeitung möglichst spezifischer Maßnahmen aus technischer Sicht**
  - Direkter Bezug zum jeweiligen DBS
  - Vorbereitung der Überführung in InSpec-Anwendungscode

Anwendung des Vorgehensmodells
Beispiel der Anforderung A1

A1 Die Standardwerte aller sicherheitsrelevanten Konfigurationsparameter müssen explizit festgelegt werden.

Neo4j Es konnten mehrere sicherheitsrelevante Konfigurationsoptionen für Neo4j identifiziert werden, die keiner der nachfolgenden Anforderungen zugeordnet werden konnten. Diese können in der Datei /etc/neo4j/neo4j.conf konfiguriert werden.

1. Der Zugriff auf Java Management Extensions, die eine der potenziellen Angriffsmöglichkeiten im Zusammenhang mit der Log4Shell-Schwachstelle (CVE-2021-44228) darstellten, sollte wie folgt deaktiviert werden:

```
# JMX-Endpoint deaktivieren (Standardwert false)
server.jvm.additional=-Dlog4j2.disable.jmx=true
```

2. Das OCSP-Stapling zur Überprüfung des Widerrufsstatus Zertifikaten kann wie folgt aktiviert werden:

```
# OCSP-Stapling für Bolt aktivieren (Standardwert false)
server.bolt.ocsp_stapling_enabled=true
```

3. HTTP Strict-Transport-Security kann wie folgt aktiviert werden:

```
# HSTS für HTTPS aktivieren (Standardwert <leer>)
dbms.security.http_strict_transport_security=max-age=15768000
```

Redis Es konnte eine sicherheitsrelevante Konfigurationsoption für Redis identifiziert werden, die keiner der nachfolgenden Anforderungen zugeordnet werden konnte.

Standardmäßig ändert Redis den Prozesstitel, um einige Laufzeitinformationen bereitzustellen. Dies kann wie folgt in der Datei /etc/redis/redis.conf deaktiviert werden:

```
# Laufzeitinformationen im Prozesstitel deaktivieren (Strandardwert
  ↪ yes)
set-proc-title no
```

➢ **Fortschreibung → PDCA-Zyklus**

Anwendung des Vorgehensmodells
Beispiel der Anforderung A31

A31 Eine rollenbasierte Zugriffskontrolle zur Trennung von Benutzer- und Datenbankverwaltungsfunktionen muss umgesetzt werden.

Neo4j In der Community-Edition von Neo4j wird jeder Benutzer einer ACL mit vordefinierten Standardberechtigungen zugewiesen. Diese Vorgehensweise kann nicht individuell angepasst oder anderweitig beeinflusst werden (siehe Umsetzung der Anforderung A32).

Redis In Redis kann dies in der ACL-Datei /etc/redis/users.acl durch die Definition eines administrativen Benutzers und eines Standardbenutzers mit minimalen Zugriffsrechten wie folgt realisiert werden:

```
1 # Administratives Benutzerkonto konfigurieren
2 user admin on ~* &* +@all
  ↪ #749f09bade8aca755660eeb17792da880218d4fbdc4e25fbec279d7fe9f65d70
```

```
3 # Minimales Benutzerkonto konfigurieren
4 user minimal on resetkeys -minimal:* resetchannels &minimal:* +@all
  ↪ -@admin -@dangerous -@scripting
  ↪ #21adaff8e0b936c51ed239be3935addd85f8e1c0f914dd087d6da10f2d956aab
```

Redis interpretiert die Berechtigungsanweisungen hierarchisch von links nach rechts. So wird dem Standardbenutzer zunächst der Zugriff auf alle Schlüssel und Kanäle entzogen und anschließend nur der Zugriff auf diejenigen mit dem Präfix `minimal:` gewährt. Das Gleiche gilt für die Befehlsgruppen, bei denen der Zugriff zunächst auf alle Befehle eingeräumt wird und anschließend alle administrativen und gefährlichen Befehle davon wieder ausgenommen werden.

- **Angabe von Interpretationshinweisen**
- **Angabe von Konfigurationswerten**

Anwendung des Vorgehensmodells
Beispiel der Anforderung A35

A35 Passwörter und kryptografische Schlüssel dürfen nur einen einzigen Einsatzzweck aufweisen und nicht mehrfach verwendet werden.

Neo4j Neo4j speichert immer alle Passwörter als SHA-256 mit Salt in der Neo4j-Systemdatenbank. Daher kann die Konformität mit dieser Anforderung nicht überprüft werden, ohne die mit den Hash-Werten assoziierten Klartext-Passwörter zu kennen.

Redis Redis speichert unter Berücksichtigung der hier angestrebten gehärteten Konfiguration alle Passwörter als SHA-256 ohne Salt in der ACL-Datei /etc/redis/users.acl. Um die Konformität mit dieser Anforderung zu überprüfen, können daher die Hash-Werte aller Benutzerkonten wie folgt auf Duplikate untersucht werden:

```
1 # Suche nach Passwort-Hash-Duplikaten
2 cat /etc/redis/users.acl | grep -e "^user" | grep -oe
  ↪ "[0-9a-f]\{64\}" | uniq -c
```

Der erwartete Rückgabewert für den Fall, dass zwei Duplikate vorliegen, entspricht folgendem Muster:

```
1 # Muster-Ausgabe von uniq -c für Passwort-Hash-Duplikate
2 2    68b77a946d17400f0cca8ddd86b145015e5d01cb89c8d953bb4067adebb91fbe
```

- **Angabe von Interpretationshinweisen**
- **Angabe von Systembefehlen**

Live-Demonstration

InSpec Redis Community-Edition Baseline

Lukas Zorn

Fakultät für Ingenieurwissenschaften \ Bereich Elektrotechnik und Informatik

Auswertung des Vorgehensmodells

	Punktwerte		Prozentwerte	
Anforderungskategorie	**Neo4j**	**Redis**	**Neo4j**	**Redis**
Grundprinzipien des Vorgehensmodells	2 / 2	2 / 2	100,00 %	100,00 %
Installation und Updates	11 / 14	10 / 14	≈ 78,57 %	≈ 71,43 %
Authentifizierung	14 / 26	17 / 26	≈ 53,85 %	≈ 65,38 %
Autorisierung	5 / 20	9 / 20	25,00 %	45,00 %
Passwortrichtlinien	9 / 16	10 / 16	56,25 %	62,50 %
Auditierung und Protokollierung	17 / 22	18 / 22	≈ 77,27 %	≈ 81,82 %

Auswertung des Vorgehensmodells

Monitoring	1 / 2	1 / 2	50,00 %	50,00 %
Fingerprinting	6 / 6	6 / 6	100,00 %	100,00 %
Verschlüsselung	14 / 18	13 / 18	≈ 77,78 %	≈ 72,22 %
Verzeichnis- und Dateiberechtigungen	6 / 6	6 / 6	100,00 %	100,00 %
Sicherer Betrieb der Datenbankanwendung	18 / 26	16 / 26	≈ 69,23 %	≈ 61,54 %
Backup und Replikation	1 / 4	0 / 4	25,00 %	0,00 %
Zusammenfassung	**104 / 162**	**108 / 162**	**≈ 64,20 %**	**≈ 66,67 %**

Fazit

- Das Vorgehensmodell bietet eine gute Arbeitsgrundlage für die Ableitung technischer Härtungsmaßnahmen
- Das Vorgehensmodell muss als fortlaufender PDCA-Zyklus verstanden und entsprechend weiterentwickelt werden
- Beide DBS konnten nur ≈ 2/3 der Anforderungen erfüllen
- Die Community-Editionen vieler NoSQL-DBS verfügen nicht über grundlegende Sicherheitsfunktionalitäten
- Fehlende Sicherheitsfunktionalitäten können kaum selbständig nachgerüstet werden

Ausblick

- **Einführung der Bewertung der Anforderungen hinsichtlich ihrer Kritikalität**
  - Auswirkungen auf Aussagekraft
  - Mögliche Orientierung am CVSS-System (Wert zwischen 0,0 und 1,0)

- **Fortschreibung**
  - Formulierung von Anforderungen aus der Umsetzung von A1
  - Anwendung auf weniger „fortschrittliche“ NoSQL-DBS

- **Weiterentwicklung der InSpec Redis Community-Edition Baseline**
  - Unterstützung weiterer Betriebssysteme und Redis-Versionen u. v. m.

Offene Diskussion und Rückfragen

Das Vorgehensmodell wird durch seine Anwendung und Fortschreibung geprägt!

Lukas Zorn

Fakultät für Ingenieurwissenschaften \ Bereich Elektrotechnik und Informatik