

# Identitäts und Berechtigungsmanagement

Maximilian Heim

10. Mai 2024

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>3</b>
1.1	Aufgabenstellung . . . . .	3
1.2	Forschungsfragen . . . . .	3
<b>2</b>	<b>Grundlagen</b>	<b>3</b>
2.1	Einordnung . . . . .	3
2.2	Identität . . . . .	3
2.3	Identitätsmanagement . . . . .	3
2.4	Berechtigung . . . . .	3
2.5	Berechtigungsmanagement . . . . .	4
2.6	Erkenntnisse im Kontext von IT-GRC . . . . .	4
<b>3</b>	<b>Methoden, Technologien und Tools</b>	<b>4</b>
3.1	Betriebliche Motivation . . . . .	4
3.2	Standards . . . . .	4
3.3	Methoden und Prozesse . . . . .	4
3.4	Technologien und Tools . . . . .	4
3.5	Erkenntnisse im Kontext von IT-GRC . . . . .	5
<b>4</b>	<b>Betriebliches Identitäts- und Berechtigungsmanagement</b>	<b>5</b>
4.1	Überblick . . . . .	5
4.2	Organisatorische Aspekte . . . . .	5
4.3	Technische Aspekte . . . . .	5
4.4	Wirtschaftliche Aspekte . . . . .	5
4.5	Erkenntnisse im Kontext von IT-GRC . . . . .	5
<b>5</b>	<b>Fazit</b>	<b>5</b>
5.1	Zusammenfassung . . . . .	5
5.2	Beantwortung der Forschungsfragen . . . . .	5
<b>6</b>	<b>Eidesstattliche Versicherung</b>	<b>5</b>
<b>7</b>	<b>Literaturverzeichnis</b>	<b>6</b>
<b>8</b>	<b>Quellenverzeichnis</b>	<b>7</b>

# **1 Einleitung**

## **1.1 Aufgabenstellung**

## **1.2 Forschungsfragen**

Diese Seminararbeit soll dem Leser eine gute Grundlage dafür geben, sich mit dem Thema Identitäts- und Berechtigungsmanagement auseinanderzusetzen.

- In Kapitel section 2 werden die Begriffe Identität, Berechtigung und Identitäts- und Berechtigungsmanagement eingeführt um eine Grundlage für die weitere Arbeit zu haben.
- In Kapitel section 3 werden die existierenden Methoden, Standards, Technologien und Tools zusammenfassend beschreiben.
- In Kapitel section 4 wird der Kontext von IAM im betrieblichen Kontext beschrieben.

# **2 Grundlagen**

## **2.1 Einordnung**

## **2.2 Identität**

Um den Begriff Identitätsmanagement zu definieren sollte zuerst der Begriff der Identität definiert werden. In der Philosophie wird Identität über die Ununterscheidbarkeit von Dingen definiert. Nach dem Identitätsprinzip sind zwei Dinge genau dann identisch wenn sich zwischen ihnen keine Unterschiede finden lassen.

## **2.3 Identitätsmanagement**

Identitätsmanagement beschreibt die Verwaltung von digitalen Identitäten. Hierbei werden Prozesse für die Provisionierung, Änderung und Deprovisionierung von digitalen Identitäten definiert und umgesetzt. [SDP16]

## **2.4 Berechtigung**

Berechtigungen beschreiben welche Identitäten auf welche Ressourcen zugreifen darf. Dieser Prozess findet nach der Feststellung der Identität statt.

## 2.5 Berechtigungsmanagement

## 2.6 Erkenntnisse im Kontext von IT-GRC

# 3 Methoden, Technologien und Tools

## 3.1 Betriebliche Motivation

## 3.2 Standards

**BSI** Das Bundesamt für Sicherheit der Informationstechnik (BSI) definiert mit BSI-Standard 200-3 einen Leitfaden zur Risikobewertung. In BSI-Standard 200-1 werden Sicherheitsmaßnahmen definiert die zur Behandlung der Risiken geeignet sind. In Bezug auf den BSI-Standard definiert das IT-Grundschutz-Kompodium des BSI's Prozessbausteine zur Umsetzung des ISMS. Hier wird im Prozessbaustein ÖRP.4 Identitäts- und Berechtigungsmanagement auf verschiedene Anforderungen für die Umsetzung von IAM eingegangen. Kapitel 3.1 definiert Basis-Anforderungen welche umgesetzt werden müssen. Kapitel 3.2 definiert Standard-Anforderungen welche umgesetzt werden sollten. Kapitel 3.3 definiert Anforderungen welche bei erhöhtem Schutzbedarf umgesetzt werden sollten. Das IT-Grundschutz-Kompodium definiert zusätzlich zu ÖRP.4 System-Bausteine wie SYS.1.3 und APP.2.1. Diese enthalten konkrete Maßnahmen zur Umsetzung des IAM für System-Komponenten wie Betriebssysteme und Verzeichnisdienste.

**ISO 27001 Annex A.9** ISO 27001 definiert mit Anhang A.9 die Zugangssteuerung.

## SO/IEC 29146

**NIST 800-53A** Das National Institute of Standards and Technology (NIST) publizierte die "NIST Special Publication 800-53A - Assessing Security and Privacy Controls in Information Systems and Organizations". Dieses Dokument stellt Prozesse und Methoden für die Bewertung von Sicherheits- und Datenschutzmaßnahmen vor. Im Kapitel "Security and Privacy Assessment Procedures" wird im Unterkapitel 4.1 "Access Control Family (AC)" auf Zugangskontrolle und im Unterkapitel 4.7 "Identification and Authentication Family (IA)" auf Identifizierung und Authentifizierung eingegangen.

## 3.3 Methoden und Prozesse

## 3.4 Technologien und Tools

IAM Tools ersetzen nicht die Einhaltung von Standards und die sorgfältige Planung von IAM Prozessen. Sie sind jedoch hilfreiche Werkzeuge zur technischen Umsetzung von IAM.

## Microsoft Active Directory

**Microsoft Entra ID** Das Unternehmen Microsoft bietet mit dem Produkt "Microsoft Entra ID" eine Cloud-basierte Lösung zum Identitäts- und Berechtigungsmanagement von Microsoft und Drittpartei-Diensten. Dieses Produkt bietet viele Vorteile. So z.B. eine Multi-Faktor-Authentifizierung mittels Microsoft Authenticator.

**SAP Cloud Identity Access Governance** Das Unternehmen SAP bietet mit dem Produkt SAP Cloud Identity Access Governance eine Cloud-basierte Lösung zum Identitäts- und Berechtigungsmanagement. SAP selbst schreibt dem Produkt eine intuitive Bedienung, hohe Anpassbarkeit und skalierbare Funktionen zu.

### 3.5 Erkenntnisse im Kontext von IT-GRC

## 4 Betriebliches Identitäts- und Berechtigungsmanagement

### 4.1 Überblick

### 4.2 Organisatorische Aspekte

Das Identitäts- und Berechtigungsmanagement fällt unter die Domäne der Informations- und IT-Sicherheit. Auf der Führungsebene ist im Unternehmen der Chief Information Security Officer (CISO) für die Umsetzung des Informationssicherheitsmanagementsystems (CISO) verantwortlich. Daher trägt der CISO in diesem Kontext eine führende Rolle. Im Fall von umfangreichen Anforderungen an das System kann die Umsetzung des IAM ein ganzes Team benötigen.

### 4.3 Technische Aspekte

### 4.4 Wirtschaftliche Aspekte

### 4.5 Erkenntnisse im Kontext von IT-GRC

## 5 Fazit

### 5.1 Zusammenfassung

### 5.2 Beantwortung der Forschungsfragen

## 6 Eidesstattliche Versicherung

## 7 Literaturverzeichnis

### Literatur

- [SDP16] Deepak H Sharma, CA Dhote und Manish M Potey. “Identity and access management as security-as-a-service from clouds”. In: *Procedia Computer Science* 79 (2016), S. 170–174.

## 8 Quellenverzeichnis