Identitäts und Berechtigungsmanagement

Maximilian Heim

19. Mai 2024

Inhaltsverzeichnis

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 bilden.
- 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

Das Identitäts- und Berechtigungsmanagent ist eine zentrale Disziplin in der Informationssicherheit. Das Identitäts- und Berechtigungsmanagement besteht aus Richtlinien, Prozessen und Technologien welche das Risiko von unberechtigten Zugriffen minimieren sollen. [Moh17] Es wird häufig zwischen Identitäts- und Berechtigungsmanagement (IAM) und Customer Identitäts- und Berechtigungsmanagement (CIAM) unterschieden. Bei IAM geht es um die Authentifikation und Zugriffskontrolle im Unternehmen. Im Kontrast behandelt das CIAM die Authentifikation und Zugriffskontrolle von Nutzern außerhalb vom Unternehmen. [Moh17] [LD22]

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. Hierbei geht es um die Fragestellung „wer/was bist du?“. Im Kontext der IT wird dies durch Authentifizierungsverfahren umgesetzt.

Authentifizierung In der IT haben sich eine Vielzahl an Authentifizierungsverfahren durchgesetzt. Für einen kurzen Überblick sind einige Authentifizierungsverfahren im folgenden aufgelistet.

- Passwörter und Pins sind die wohl bekanntesten Arten der Authentifizierung. Jedoch ist es auch eine der unsichersten Arten da diese gerne mehrfach verwendet werden oder bei unzureichender Länge geknackt werden können
- Tokens sind eine andere Art der Authentifizierung die auf Besitz und Wissen basieren und daher sicherer sind wie rein wissensbasierte Verfahren. Hierbei wird ein Gerät verwendet welches nach Entsperrung mittels Pin/Passwort ein Einmalpasswort ausgibt oder automatisch die Authentifizierung freigibt
- Eine weiteres Beispiel für Authentifizierung ist die Biometrie. Hierbei werden z.B. der Fingerabdruck, die Retina oder die Stimme einer Person verwendet um diese zu identifizieren

[TS17]

2.3 Identitätsmanagement

Identitätsmanagement ist die Verwaltung von digitalen Identitäten. Die Aufgaben im Bereich des Identitätsmanagements sind vielfältig. Beispiele für Aufgaben sind.

- Planung und Umsetzung einer passenden Identity Management Architektur [Win05]
- Management von Prozessen für die Provisonierung, Änderung und Deprovisionierung von digitalen Identitäten. Dies wird zusammengefasst als Identity Lifecycle Management bezeichnet [SDP16]
- Identifikation von Standards und Gesetzen welche eingehalten werden müssen, Einbringung dieser in den Identitätsmanagement Prozess [Azh14]
- Auditieren des Identity Life Cycles und der Einhaltung von IT-GRC Vorgaben [PDS07] [Acc08]

2.4 Berechtigung

Berechtigungen oder auch Zugriffsberechtigungen beschreiben welche Identitäten auf welche Ressourcen zugreifen darf. Eine Berechtigung besteht aus einer zu berechtigenden Ressource und aus einer zu berechtigenden Operation für diese Ressource. Beispiele hierfür sind der Schreibzugriff auf eine Datenbank, der Lesezugriff auf Dokumente oder der Konfiguration von Rechnersystemen. Dieser Prozess findet nach der Authentifizierung statt. Hierbei geht es um die Fragestellung „was darf er/sie/es?“. Die Kontrolle der Berechtigungen basierend auf einer Identität wird Zugriffskontrolle oder auch Autorisierung genannt. [TS17]

2.5 Berechtigungsmanagement

Berechtigungsmanagement ist verantwortlich für die Festlegung welche Nutzer/Entitäten auf welche Ressourcen Zugriff haben. Das Ziel hierbei ist das Least-Privilege-Prinzip (PoLP) umzusetzen. Das Berechtigungsmanagement besteht wie auch das Identitätsmanagement aus verschiedenen Aspekten welche größtenteils Isomorph sind, jedoch der vollständigkeit halber separat erläutert und differenziert werden.

- Auswahl und Implementierung einer passenden Methode zur Berechtigungssteuerung. Hierbei gibt es verschiedenste Ansätze welche basierend auf dem Kontext analysiert werden sollten. Beispiele hierfür sind die Rollenbasierte Berechtigungssteuerung (RBAC), die Attributsbasierte Berechtiungssteuerung (ABAC) oder die Gruppenbasierte Berechtigungssteuerung (GBAC).
- Auswahl geeigneter Technologien und Tools und Implementierung dieser.
- Provisionierung und Änderung von Rechten
- Identifikation von Standards und Gesetzen welche eingehalten werden müssen, Umsetzung dieser im Berechtigungsmanagement Prozess
- Auditierung des Berechtigungsmanagement-Prozesses um Abweichungen im Kontext der IT-GRC zu identifizieren

2.6 Erkenntnisse im Kontext von IT-GRC

Das Identitäts und Berechtigungsmanagement ist eine zentrale Disziplin im Kontext der IT-GRC. Die sorgfältige Umsetzung von Identitäts- und Berechtigungsmanagement hilft dabei IT-Sicherheits-Risiken zu minimieren und Compliance mit Standards und Gesetzlichen Vorgaben zu gewährleisten.

3 Methoden, Technologien und Tools

3.1 Betriebliche Motivation

Die Motivationen für die korrekte Umsetzung IAM im Unternehmen sind vielfältig. Die Umsetzung von IAM kann kostspielig sein denn das Management und die eingesetzten Technologien sind teuer. Rechtlichen Vorgaben wie das Bundesdatenschutzgesetzes oder das KonTraG sind jedoch nicht optional. Standards zum Informations- und Risikomanagement wie die ISO 27001 oder die BSI-Standards zur IT-Sicherheit sind eine gute Grundlage für rechtliche und ökonomische Sicherheit. [TS17]

3.2 Standards

BSI Das Bundesamt für Sicherheit der Informationstechnik (BSI) definiert den IT-Grundschutz. Dieser besteht aus den BSI-Standards und dem IT-Grundschutz-Kompendium. In BSI-Standard 200-1 werden Sicherheitsmaßnahmen definiert die zur Behandlung der Risiken geeignet sind, in diesen Sicherheitsmaßnahmen wird das Identitäts- und Berechtigungsmanagement als Sicherheitsmaßnahme aufgeführt. In Bezug auf den BSI-Standard definiert das IT-Grundschutz-Kompendium Prozessbausteine zur Umsetzung des ISMS. Hier wird im Prozessbaustein „ORP.4 Identitäts- und Berechtigungsmanagent“ auf verschiedene Anforderungen für die Umsetzung von Identitäts- und Berechtigungsmanagement 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. Zusätzlich zu ORP.4 gibt es das Dokument „Umsetzungshinweise zum Baustein: ORP.4. Identitäts- und Berechtigungsmanagement“ welches spezifische Maßnahmen definiert. [BSI21]

ISO 27001 Annex A.9 ISO 27001 definiert mit Anhang A.9 Kontrollen für das Identitäts- und Berechtigungsmanagement. Das Kapitel ist in die Unterkapitel „9.1 Geschäftsanforderungen an die Zugangssteuerung“, „9.2 Benutzerzugangsverwaltung“, „9.3 Benutzerverantwortlichkeiten“ und „9.4 Zugangssteuerung für Systeme und Anwendungen“ unterteilt. Die Maßnahmen des oben erwähnten IT-Grundschutz-Kompendiums eignen sich zur Umsetzung der ISO 27001 Kontrollen. Eine Gegenüberstellung des Anhangs A.9 zu den Prozessbausteinen lässt sich im Dokument „Zuordnungstabelle: Zuordnung ISO/IEC 27001 zum IT-Grundschutz“ finden.

ISO/IEC 24760 Eine speziell für Identitätsmanagement erstellte Norm ist ISO/IEC 24760. Hierbei werden Konzepte und operative Strukturen zur korrekten Umsetzung von Identitätsmanagement definiert. [ISO23]

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. Im folgenden werden einige Technologien und Produkte vorgestellt welche bei der Umsetzung von Identitäts- und Berechtigungsmanagement verwendet werden.

3.4.1 Standardisierte Technologien

SAML SAML ist ein weit verbreiteter Standard zur Umsetzung von Sicherheits-Assertationen. Mit SAML wird ein XML Format definiert welches zur Authentifizierung und Authorisierung von Nutzern verwendet werden kann. Im Kontext von SAML werden verschiedene Begrifflichkeiten definiert.

- Assertation - Eine Assertation über die Charakteristiken und Attribute eines Subjekts. So z.B. die Zugehörigkeit zu einer Gruppe oder der Besitz eines Attributs.
- Identity Provider (IdP) - Der Server der für die eigentliche Bearbeitung der Assertation zuständig ist. Er erhält die Anfrage und leitet die Antwort an den Service Provider weiter.
- Service Provider (SP) - Das Ziel der Authentifizierung/Authorisierung, dieser stellt eine Ressource/Service zur Verfügung.

[HM05]

OAuth OAuth ist eine verbreiteter Standard zur delegierten Zugriffskontrolle welcher in RFC 6749 definiert wird. OAuth ist ein Framework welches das Problem der Autorisierung Dritter lößt. Somit müssen keine sensiblen Informationen wie Passwörter mit Dritten geteilt werden um ihnen Zugriff auf eine Ressource zu geben. Im Kontext des Standards werden folgende Begriffe definiert.

- Ressourcenbesitzer - Eine Entität welche die Ressource besitzt und Zugriff gewähren kann
- Ressourcenserver - Ein Server welcher die Ressource hostet und auf Anfragen mittel Zugriffstokens reagieren kann
- Klient - Eine Anwendung welcher für Ressourcen authorisiert ist und Anfragen an den Ressourcenserver senden kann
- Authorisierungsserver - Ein Server welcher Zugriffstokens im Name des Ressourcenbesitzers an den Klient ausstellen kann

Der Ablauf des Protokolls ist in Grafik section 3.4.1 abgebildet. [Har12]

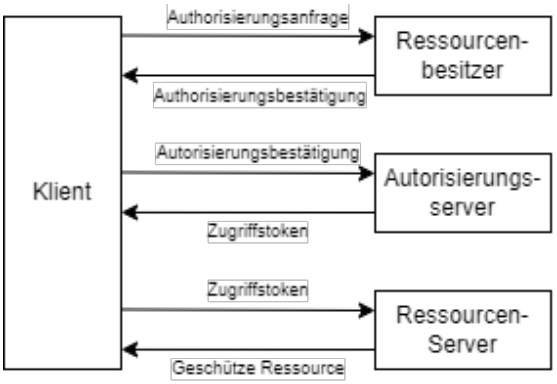

Abbildung 1: Protokoll OAuth 2.0 - [Basierend auf RFC 6749]

OpenID OpenID Connect (OIDC) ist ein Standard für federatedlößt die veraltete OpenID 2.0 Spezifikation ab. Es ist ein weit verbreiteter Standard von `https://www.openid.net/developers/libraries-for-obsolete-specifications/`

3.4.2 IAM Lösungen

IBM Security Verify IBM bietet mit dem Produkt „IBM Security Verify“ eine Cloud basierte Lösung zum Identitäts- und Berechtigungsmanagement an. Dieses Produkt bietet umfangreiche Funktionalitäten wie SSO, MFA, KI gestütze Risikobewertung von Zugriffen und Identitätsanalyse, d.h. die Analyse von Identitäten und Berechtigungen zum Zweck der Identifizierung von Abweichungen.

Microsoft Entra ID Microsoft bietet mit dem Produkt „Microsoft Entra ID“ eine Cloud basierte Lösung zum Identitäts- und Berechtigungsmanagement von Microsoft und drittpartei Diensten an. Dieses Produkt bietet Funktionen wie z.B. Multi-Faktor-Authentifizierung mittels Microsoft Authenticator.

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

Okta Inc. Das Unternehmen Okta Inc. ist ein in den USA ansässiges Unternehmen welches sich auf IAM spezialisiert hat. Mit rund 6000 Mitarbeitern und mehr als einer Milliarde US-Dollar an Umsatz ist es ein führender Hersteller von IAM Produkten. Vom Unternehmen werden 2 Produkte angeboten. Customer Identity Cloud und Workforce Identity Cloud. Customer Identity Cloud ist eine Lösung zum Customer Identity Management, d.h. es ermöglicht die sichere Verwaltung und Authentifizierung von Kunden-Identitäten. Workforce Identity Cloud ist eine Lösung zum Unternehmensinternen Identitätsmanagement.

Oracle Oracle ist mit 132000 Mitarbeitern und mehr als 40 Milliarden US-Dollar Umsatz eine bekannte größe in der Technologiebranche. Oracle bietet eine vielzahl an Produkten zum Identitäts- und Berechtigungsmanagement an. Die wichtigsten werden im folgenden vorgestellt.

- Oracle Cloud Infrastructure Identity and Access Management - On Premise und Cloud IAM Lösung für Unternehmen. Unterstützt die Einbindung von Programmen mittels eines SDK's

SailPoint SailPoint ist ein auf IAM spezialisiertes Unternehmen. Es werden verschiedenste Produkte zum Identitäts- und Berechtigungsmanagement angeboten.

- IdentityIQ - Identits Lifecycle und Compliance Management Lösung

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 Informationssicherheit, benötigt jedoch gegebenfalls umfangreiche IT Infrastruktur und Produkte. Auf der Führungsebene ist im Unternehmen sind daher der Chief Information Security Officer (CISO) und der Chief Information Officer (CIO) für die Umsetzung des Identitäts- und Berechtigungsmanagement verantwortlich. [Azh14][BMS09] Im Fall von umfangreichen Anforderungen an das System kann die Umsetzung des IAM ein ganzes Team benötigen. [MHY11]. Ein weiterer

4.3 Technische Aspekte

4.4 Wirtschaftliche Aspekte

Die wirtschaftliche Signifikanz von Identitäts- und Berechtigungsmanagement ist unumstreitbar. Es lassen sich 3 Aspekte identifizieren.

Produktivität Für die Mitarbeiter im Unternehmen stellt schlecht umgesetztes IAM eine Hürde dar. Wenn ein Mitarbeiter eine vielzahl an Passwörtern für die unternehmensinternen Dienste verwalten muss kann dies zur unsachgemäßen Handhabung führen, dies erhöht die Wahrscheinlichkeit von Sicherheit Risiken und verringert die Produktivität im Vergleich zu SSO mittels MFA. [Azh14]

Security Der wirtschaftliche Schaden der durch nichteinhaltung von Gesetzen, Datendiebstahl und unautorisierter Kontrolle entstehen kann ist immens. [Azh14]

Kundenerlebnis Im Kontext des Customer IAM führen ungeeignete IAM Lösungen zu erhöhter Komplexität für den Nutzer. Eine Folge hiervon ist dass Kunden möglicherweise schwache Passwörter verwenden oder auf mehreren Plattformen das gleiche Passwort verwenden, dies kann zur kompromittierung von Kundenkonten führen. Im Kontrast kann die strikte Umsetzung von starken Passwörtern oder die Nutzung einer weiteren MFA-App für den Kunden abschreckend sein. Somit steigt der Kunde möglicherweise zur Konkurrenz um. [Azh14]

4.5 Erkenntnisse im Kontext von IT-GRC

5 Fazit

5.1 Zusammenfassung

5.2 Beantwortung der Forschungsfragen

6 Eidesstattliche Versicherung

Literaturverzeichnis

[HM05] John Hughes und Eve Maler. "Security assertion markup language (saml) v2. 0 technical overview". In: *OASIS SSTC Working Draft sstc-saml-tech-overview-2.0-draft-08* 13 (2005), S. 12.

[Win05] Phillip J Windley. *Digital Identity: Unmasking identity management architecture (IMA)*. Ö'Reilly Media, Inc.", 2005.

[PDS07] Liam Peyton, Chintan Doshi und Pierre Seguin. "An audit trail service to enhance privacy compliance in federated identity management". In: *Proceedings of the 2007 conference of the center for advanced studies on Collaborative research*. 2007, S. 175–187.

[Acc08] Rafael Accorsi. "Automated privacy audits to complement the notion of control for identity management". In: *Policies and Research in Identity Management: First IFIP WG11. 6 Working Conference on Policies and Research in Identity Management (IDMAN'07), RSM Erasmus University, Rotterdam, The Netherlands, October 11-12, 2007*. Springer. 2008, S. 39–48.

[BMS09] Adrian Baldwin, Marco Casassa Mont und Simon Shiu. "Using modelling and simulation for policy decision support in identity management". In: *2009 IEEE International Symposium on Policies for Distributed Systems and Networks*. IEEE. 2009, S. 17–24.

[MHY11] Ishaq Azhar Mohammed, Abubakar Hassan und DM Yusuf. "Identity and access management system: a web-based approach for an enterprise". In: *International Journal of Advanced and Innovative Research* 1.4 (2011), S. 1–7.

[Azh14] Ishaq Azhar. "Economics of Identity and Access Management: Providing decision support for investments". In: *Ishaq Azhar Mohammed.(2014). Economics of Identity and Access Management: Providing decision support for investments. International Journal of Managment, IT and Engineering (IJMIE)* 4.2 (2014), S. 540–549.

[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.

[Moh17] Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.

[TS17] Alexander Tsolkas und Klaus Schmidt. "Zugriffskontrolle über Authentifizierung". In: *Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen*. Wiesbaden: Springer Fachmedien Wiesbaden, 2017, S. 129–160. ISBN: 978-3-658-17987-8. DOI: 10.1007/978-3-658-17987-8_7. URL: https://doi.org/10.1007/978-3-658-17987-8_7.

[LD22] Anastasios Liveretos und Ivo Draganov. “Customer Identity and Access Management (CIAM): An overview of the main technology vendors”. In: *International Journal of Economics and Management Systems* 7 (2022).

Quellenverzeichnis

[Har12] Dick Hardt. *RFC 6749: The oauth 2.0 authorization framework*. 2012. URL: https://datatracker.ietf.org/doc/html/rfc6749.

[BSI21] BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2021.pdf?__blob=publicationFile&v=2.

[ISO23] ISO. *ISO/IEC 24760-1:2019 IT Security and Privacy - A framework for identity management 2023*. 2023. URL: https://www.iso.org/standard/77582.html.

Abbildungsverzeichnis