Identitäts und Berechtigungsmanagement

Maximilian Heim

15. 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 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. Hierbei geht es um die Fragestellung „wer 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 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 Life Cycle bezeichnet [SDP16]
- Management der Compliance mit internen und externen Vorgaben zum Datenschutz und Risikomanagement [Azh14]
- Auditieren des Identity Life Cycles und der Einhaltung von Compliance Vorgaben [PDS07] [Acc08]

2.4 Berechtigung

Berechtigungen oder auch Zugriffsberechtigungen beschreiben welche Identitäten auf welche Ressourcen zugreifen darf. 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. Beispiele hierfür sind der Zugriff auf eine Datenbank, der Zugriff auf Dokumente oder der Konfiguration von Systemen. Das Ziel ist hierbei ist das Least-Privilege-Prinzip (PoLP) umzusetzen. Das Berechtigungsmanagement besteht aus verschiedenen Aspekten. So z.B. der Provisionierung von Rechten, der Compliance mit Standards und der konkreten technischen Umsetzung der Authorisierung.

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 die Compliance mit internen und externen Vorgaben zu gewährleisten.

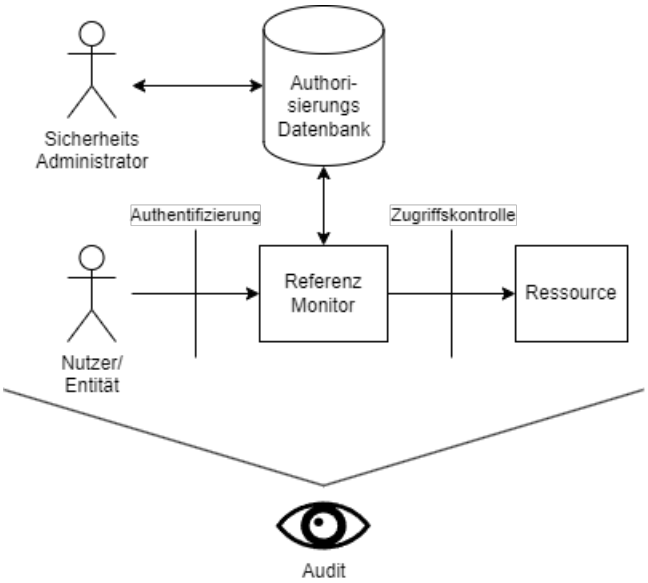

Abbildung 1: Abstrakte Einordnung der Zugriffskontrolle [Basiert auf Access Control: Principles and Practice von Ravi S. Sandhu and Pierangela Samarati]

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. Die Einhaltung von rechtlichen Vorgaben gesetzlich vorgegeben, die Einhaltung von S

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-Kompendium des BSI's Prozessbausteine zur Umsetzung des ISMS. Hier wird im Prozessbaustein „ORP.4 Identitäts- und Berechtigungsmanagent“ 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-Grundschuztz-Kompendium definiert zusätzlich zu ORP.4 System-Bausteine wie SYS.1.3 und APP.2.1. Diese enthalten konkrete Maßnah-

men 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.

ISO/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.

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

OpenID

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 Active Directory

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.

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, 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. Im Fall von umfangreichen Anforderungen an das System kann die Umsetzung des IAM ein ganzes Team benötigen.

7 Literaturverzeichnis

Literatur

[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.

[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.

[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.

8 Quellenverzeichnis

Abbildungsverzeichnis