Identitäts und Berechtigungsmanagement

Maximilian Heim

26. Mai 2024

Inhaltsverzeichnis

1 Einleitung

1.1 Aufgabenstellung

Diese Seminararbeit wurde im Rahmen der Vorlesung IT-GRC angefertigt. Ziel der Arbeit ist es die in Kapitel 1.2 definierten Forschungsfragen zu beantworten. Die Forschungsfragen zielen darauf ab wichtige Aspekte des betrieblichen Identitäts- und Berechtigungsmanagements im Kontext der IT-GRC zu beleuchten.

1.2 Forschungsfragen

Im Rahmen der Seminararbeit wurden 7 Forschungsfragen definiert, diese sind im Folgenden aufgeführt.

- Was versteht man unter den Begriffen „Identität“ sowie „Identitätsmanagement“ und welche Zielstellung wird dabei verfolgt?
- Was versteht man unter den Begriffen „Berechtigung“ sowie „Berechtigungsmanagement“ und welche Zielstellung wird dabei verfolgt?
- Welche Standards, Methoden, Technologien und Tools lassen sich differenzieren?
- Welche Aufgaben und Prozesse sind im Kontext von Identitäts und Berechtigungsmanagement zu bearbeiten?
- Welche betrieblichen Anwendungsfälle zeigen die Bedeutung des Identitäts und Berechtigungsmanagements auf?
- Wie wird das Identitäts und Berechtigungsmanagement im Kontext der Sicherheit in der Informationstechnik eingesetzt?
- Wer hat im Unternehmen typischerweise die Zuständigkeit für Identitäts und Berechtigungsmanagemnt und wer führt diese Aufgaben operativ durch?

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. Identitätsmanagement und Berechtigungsmanagement sind zwei unterschiedliche Disziplinen, jedoch werden diese meist zusammen angewendet. [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 des Identitätsmanagements handelt es sich hier um digitale Identitäten, d.h. eine Menge an Attributen und Rollen die einer Person, einem IT-System oder einer Anwendung zugeordnet werden können, inklusive einem Bezeichner und Zugangsdaten die zur Nutzung der Identität notwendig sind. [TS17] Ein Subjekt (Person, System) kann mehreren digitalen Identitäten zugeordnet sein. Dieser Sachverhalt ist in Kapitel 2.2 dargestellt.

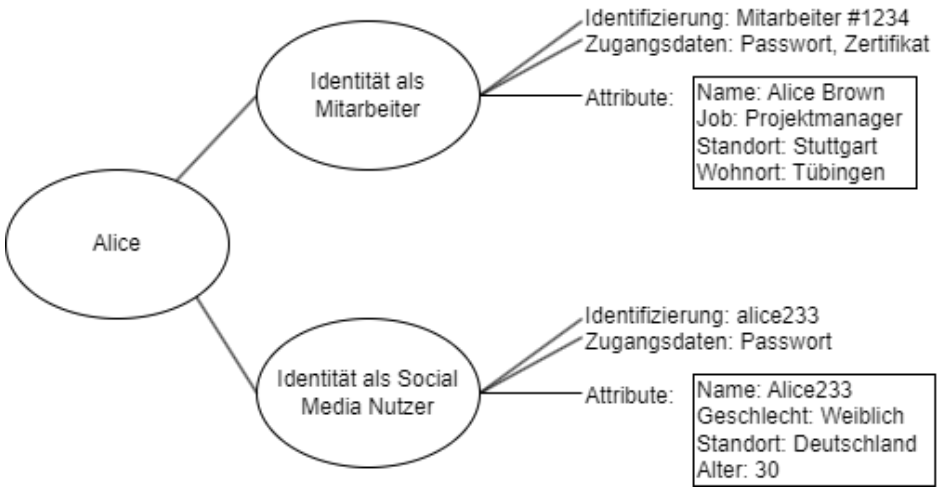

Abbildung 1: Digitale Identität - In Anlehnung an: Grafik 2.1 aus Identity Management Concepts, Technologies, and Systems von Elisa Bertino und Kenji Takahashi

In der Informationstechnik wird der Beweis über die eigene Identität, basierend auf Bezeichner und Zugangsdaten als Authentifizierung bezeichnet. Es haben sich verschiedenste Authentifizierungsverfahren durchgesetzt von denen im Folgenden einige vorgestellt werden.

Authentifizierungsverfahren

- 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 [TS17]

- Tokens sind eine andere Art der Authentifizierung die auf Besitz und Wissen basieren und daher sicherer sind wie rein wissensbasierte Verfahren wie Passwörter. Hierbei wird ein Gerät verwendet welches nach Entsperrung mittels Pin/Passwort ein Einmalpasswort ausgibt oder automatisch die Authentifizierung freigibt [TS17]

- 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 authentifizieren [TS17]

2.3 Identitätsmanagement

Identitätsmanagement ist die Verwaltung von digitalen Identitäten. Die Aufgaben im Bereich des Identitätsmanagements sind vielfältig. Es gibt unterschiedliche Definitionen von den Teilbereichen des Identitätsmanagements. Jedoch lassen sich aus den verschiedenen Quellen grundlegende Aufgaben extrahieren welche im Rahmen des Identitätsmanagements durchgeführt werden müssen. Die Aufgabenbereiche sind im Folgenden aufgelistet.

- Identity Lifecycle Management: Management von Prozessen für die Provisonierung, Änderung und Deprovisionierung von digitalen Identitäten [BT10]
- Technologie: Planung, Implementierung und Wartung der Infrastruktur zur Speicherung und Authentifizierung von digitalen Identitäten [BT10]
- Compliance: Identifikation von Standards und Gesetzen welche eingehalten werden müssen, Definition von Prozessen zur Einhaltung der Compliance Vorgaben [Con17][TS17]
- Audit: Auditierung der Compliance Vorgaben im Rahmen der Identifikation von Abweichungen zu den Vorgaben und Speicherung von Transaktionen zur Nachverfolgbarkeit [PDS07][Acc08][BT10]

2.4 Berechtigung

Berechtigungen oder auch Zugriffsberechtigungen beschreiben welche Identitäten auf welche Ressourcen zugreifen dürfen. 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 und die Kontrolle dieser

Berechtigungen. Das Ziel hierbei ist das Least-Privilege-Prinzip (PoLP) umzusetzen. Die Definitionen der Aufgabenbereiche im Berechtigungsmanagement divergieren wie auch beim Identitätsmanagement je nach Quelle. Jedoch lassen sich ebenso verschiedene Aufgabenbereiche identifizieren, diese sind im Folgenden vorgestellt.

- Berechtigungskonzeption: Management von Prozessen für die Provisonierung, Änderung und Deprovisionierung von Berechtigungen [BSI21] [TS17]
- Technologie: Planung, Implementierung und Wartung der Infrastruktur zur Berechtigungskontrolle [TS17]
- Compliance: Identifikation von Standards und Gesetzen welche eingehalten werden müssen, Definition von Prozessen zur Einhaltung der Compliance Vorgaben [Con17][TS17]
- Audit: Auditierung der Compliance Vorgaben im Rahmen der Identifikation von Abweichungen zu den Vorgaben und Speicherung von Transaktionen zur Nachverfolgbarkeit [Ben05]

2.6 Identitäts- und Berechtigungsmanagement

Eine systematisches Modell zu den provisionierenden und operativen Prozessen des Identitäts- und Berechtigungsmanagements findet sich in Kapitel 2.6

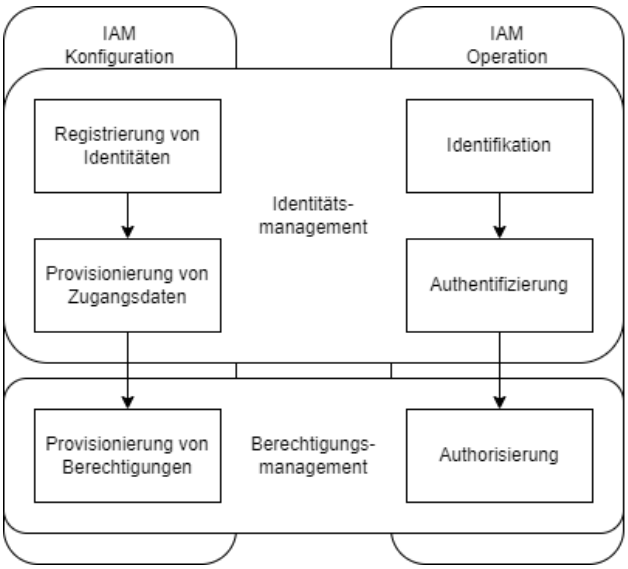

Abbildung 2: Phasen des Identitäts- und Berechtigungsmanagements - In Anlehnung an: A Multi-Layer Security System for Data Access Control, Authentication, and Authorization von Tamanna Kaiser und Rafa Siddiqua

2.7 Erkenntnisse im Kontext von IT-GRC

- Die Nutzung von Identitäts- und Berechtigungsmanagement spielt eine zentrale Rolle im unternehmensweiten Risikomanagement. Durch die Steuerung welche logischen Identitäten auf welche Ressourcen zugreifen kann können eine Vielzahl an beabsichtigter und unbeabsichtigter Sicherheitsrisiken minimiert werden.

3 Methoden, Technologien und Tools

3.1 Betriebliche Motivation

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. Mithilfe dieses Dokuments kann eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz umgesetzt werden. [BSI23]

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

3.3.1 Identitäts Lebenszyklus

Ein zentraler Prozess welcher im Rahmen des Identitätsmanagements definiert und umgesetzt werden muss ist der Identitäts Lebenszyklus. Dieser enthält die grundlegenden Elemente Geburt, Leben, Änderung, Tod und Governance. Der Prozess ist in Kapitel 3.3.1 dargestellt und wird nachfolgend genauer beschrieben. [BT10]

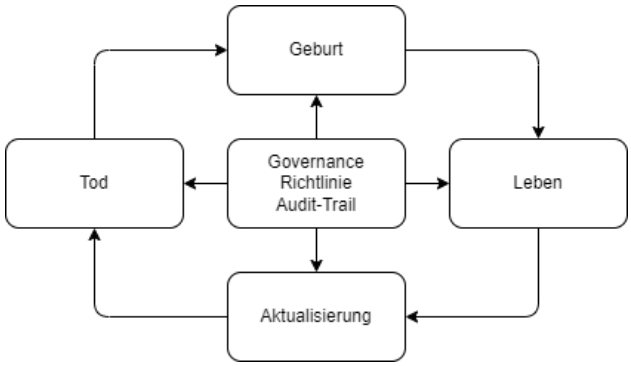

Abbildung 3: Identity Life Cycle - In Anlehnung an: Identity Management Concepts, Technologies, and Systems von Elisa Bertino und Kenji Takahashi

Geburt

Festlegung und Überprüfung von Attributen Der erste Schritt in der Geburt einer Identität ist die Sammlung relevanter Attribute wie Name, Geburtsdatum, Wohnsitz, Rolle im Unternehmen etc. und Überprüfung dieser. [BT10]

Festlegen von Anmeldeinformationen Um dem Subjekt Zugriff auf die provisionierte Identität zu geben müssen Bezeichner (z.B. E-Mail Addressen oder Nutzernamen) und geeignete Verfahren zur Authentifikation festgelegt werden. So werden in diesem Schritt z.B. Einmalpasswörter für die initiale Anmeldung vergeben oder der Fingerabdruck der zu authentifizierenden Person gespeichert. [BT10]

Abschließende Erstellung Nachdem alle relevanten Informationen zur Erstellung der Identität gesammelt wurden kann die Identität erstellt werden. [BT10]

Leben

Authentifizierung Die Authentifizierung der eignenen Identität ermöglicht die gesicherte Nutzung von Ressourcen. [BT10]

Weitergabe von Informationen Verfahren zur Weitergabe von Informationen sind ein zentraler Aspekt beim Ausleben einer digitalen Identität. [BT10]

Aktualisierung

Änderungen Bei Änderung von Attributen wie z.B. Rollen im Unternehmen, Wohnort oder Namensänderung müssen die Attribute schnellstmöglich aktualisiert werden um die Integrität dieser zu gewährleisten. Zugangsdaten wie neu ausgestellte Zertifikate oder geänderte Passwörter müssen ebenso aktualisiert werden um die Authentifizierung zu gewährleisten. [BT10]

Tod

Entzug von Zugangsrechten Bei der Kündigung oder Beurlaubung von Mitarbeitern oder bei der Dekommisionierung von Systemen muss der Zugriff auf Ressourcen aufgehoben werden um Sicherheitsrisiken zu verhindern. In diesem Szenario ist es jedoch auch wichtig die Identitätsinformationen weiterhin zu persistieren um für zukünftige Untersuchungen wie z.B. des Audit-Trails eine Zuordnung zu haben. [BT10]

Governance

Richtlinien Die Administration, Nutzung und Weitergabe von Identitätsinformationen muss klar durch Richtlinien definiert sein. [BT10]

Audit Trail Jegliche Transaktionen bezüglich Zugriff, Änderung oder Weitergabe von Identitätsinformationen sollten aufgezeichnet werden um die Rückverfolgbarkeit zu gewährleisten. [BT10]

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. So gibt es einige standarisierte Technologien die bei der Implementierung von Identitäts- und Berechtigungsmanagement angewendet werden können. Zur konkreten Umsetzung in Organisationen gibt einige quelloffene Lösungen und von den großen Technologiekonzernen wie Microsoft, SAP, IBM, Oracle werden kommerzielle Lösungen angeboten. Im Folgenden werden einige standartisierte Technologien und Produkte vorgestellt welche bei der Umsetzung von CIAM und IAM 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. [HM05]

- 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.

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 Kapitel 3.4.1 abgebildet. [Har12]

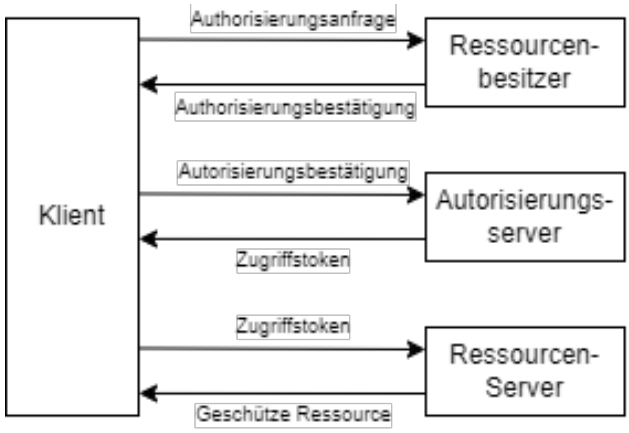

Abbildung 4: Protokoll OAuth 2.0 - [Basierend auf RFC 6749]

OpenID OpenID Connect (OIDC) ist ein Standard für Föderierte Authentifizierung welches die veraltete OpenID 2.0 Spezifikation ablößt.

3.4.2 IAM Lösungen

Shibboleth Shibboleth ist eine quelloffene Lösung zur Umsetzung von SSO. Shibboleth basiert auf SAML und setzt daher das Prinzip der Föderierten Identität mittels IdP und SP um. Die Technologie setzt sich aus 3 Software

Paketen zusammen. IdP, SP und Embedded Discovery Service. Der Embedded Discovery Service erlaubt einem SP mehrere IdP's zur Verfügung zu stellen.

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.

3.5 Erkenntnisse im Kontext von IT-GRC

- Im Rahmen von Normen wie der ISO 27001 spielt die Umsetzung von IAM eine zentrale Rolle.

- Professionelle IAM Lösungen können durch eine Vielzahl an Funktionalitäten dazu beitragen Identitäts- und Berechtigungsmanagement effizient umzusetzen.

4 Betriebliches Identitäts- und Berechtigungsmanagement

4.1 Überblick

4.2 Organisatorische Aspekte

Im Rahmen der Ausarbeitung eines IAM Konzepts im Unternehmen müssen hierbei klare Verantwortlichkeiten, Prozesse und Technologien definiert werden. Die relevanten Organisationseinheiten zum Identitäts- und Berechtigungsmanagement werden im Folgenden vorgestellt.

Führungebene IAM fällt unter die Domäne der Informationssicherheit, benötigt jedoch gegebenfalls umfangreiche IT Infrastruktur und Produkte. Auf der Führungsebene 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]

Helpdesk Der Helpdesk ist im Unternehmen eine zentrale Anlaufstelle für Probleme mit der Authentifizierung wie vergessener Passwörter oder fehlender Berechtigungen. So wurde bei Umfragen festgestellt dass je nach Unternehmen 10-66 % aller Helpdesk Tickets aufgrund von vergessener Passwörter erstellt werden. [Yle+04][TS17] Ein wichtiger Aspekt hierbei ist die Einhaltung fester Prozesse welche mögliche Angriffe durch Social Engineering verhindern. [Woo05]

Personalmanagement Eine Zentrale Rolle in der Provisionierung und Änderung von Identitäten spielt das Personalmanagement. Dieses ist für die erstmalige Erstellung der Identitäten, der Ausgabe von Authentifizierungsinformationen, der Vergabe von Rollen für rollenbasierte Zugriffskontrolle und der Deprovisionierung bei Beurlaubung und Kündigung zuständig. [You04][Moh17]

4.3 Technische Aspekte

Für die Umsetzung von Identitäts- und Berechtigungsmanagement im Betrieb bieten sich die Lösungen der namhaften Hersteller wie Microsoft, SAP oder Okta an. Dies sind ausgereifte Lösungen mit einer Vielzahl an Funktionalitäten die die Umsetzung des Identitäts- und Berechtigungsmanagements unterstützen. Während der traditionelle Ansatz die Nutzung von On-Premise Services war bewegt sich die IAM Industrie in Richtung von SaaS Modellen. Im Kontext von IAM werden diese Lösungen als IDaaS bezeichnet. [Kun+14]

4.4 Wirtschaftliche Aspekte

Die Signifikanz von Identitäts- und Berechtigungsmanagement in Unternehmen tiefgreifend. Es lassen sich 4 Aspekte identifizieren. Security, Produktivität, Compliance und Kundenerlebnis. [Mon+10][Azh14] Diese 4 Aspekte sind im Folgenden aufgeführt.

Security Der wirtschaftliche Schaden der durch Datendiebstahl und unautorisierter Kontrolle entstehen kann ist immens. [Azh14] Wenn ein Mitarbeiter eine Vielzahl an Passwörtern für die unternehmensinternen/unternehmensexternen Dienste verwalten muss kann dies zur unsachgemäßen Handhabung führen - so z.B. Notizen mit Passwörtern oder die Verwendung von schwachen Passwörtern, dies erhöht die Wahrscheinlichkeit von Sicherheitrisiken. [HS12] [Azh14] Im Jahr 2017 fiel Deloitte einem Cyberangriff zum Opfer. Hierbei wurden Nutzernamen, Passwörter, IP Addressen und sensible Unternehmensinformationen von 244.000 Mitarbeitern und Kunden geklaut. Grund für den Cyberangriff war ein Administratoraccount ohne Zugriffsbeschränkungen welcher nur mittels Passwort, ohne MFA geschützt war. [Del17] Mittels fest definierter Prozesse des Identity Management Life Cycles und Audit dieses können Risiken für ähnliche Angriffe minimiert werden.

Produktivität Im vorherigen Abschnitt wurde die wirtschaftliche Signifikanz von Identitäts- und Berechtigungsmanagement aufgezeigt. Dies kann jedoch einen negativen Einfluss auf die Produktivität von Mitarbeitern haben. So führt z.B. die Verwendung von mehreren verschiedenen Systemen, alle mit unterschiedlichen Authentifizierungsverfahren dazu dass Mitarbeiter verschiedene Passwörter verwalten müssen oder sich in jedem System separat authentifizieren müssen. Mit der Anwendung von SSO Verfahren lässt

sich dieser Aufwand auf ein Minimum reduzieren. [RR12] [HS12] Während die Umsetzung des Principle of Least Privilege wünscheswert ist können schlecht konfigurierte Zugriffsberechtigungen dazu führen dass Mitarbeiter ihre Arbeit unterbrechen müssen um neue Rechte anzufordern. Dies kann unter Umständen zu teuren Verzögerungen im direkten Arbeitsablauf adminstrativer oder operativer Aufgaben führen. [Wei+15]

Kundenerlebnis Im Kontext des Customer IAM führen ungeeignete IAM Lösungen zu erhöhter Komplexität für den Nutzer. Eine strikte Umsetzung von starken Passwörtern oder die Nutzung einer weiteren MFA-App kann für den Kunden abschreckend sein. Somit steigt der Kunde möglicherweise zur Konkurrenz um. [Azh14] Durch das Anbieten von SSO mittels externer Dienste lässt sich die Komplexität und das Risiko von Sicherheitsproblemen reduzieren.

Compliance

EuroSOX Die Richtlinie 2006/43/EG, durch den direkten Bezug zum Sarbanes Oxley Act auch EuroSOX genannt fordert im Rahmen des Internen Kontrollsystems nach einer Berechtigungsvergabe und Funktionstrennung im Unternehmen. Dies stellt eine direkte Forderung für Identitäts- und Berechtigungsmanagement dar. [Con17]

KonTraG Das KonTraG fordert Unternehmen auf ein Risikomanagementsystem zu implementieren. Unauthorisierter Zugriff auf sensible Daten und Geschäftsprozesse kann in diesem Kontext als Risiko aufgefasst werden. D.h. es besteht eine indirekte Forderung nach Identitäts- und Berechtigungsmanagement. [Con17]

BDSG Im BDSG nimmt Identitäts- und Berechtigungsmanagement eine zentrale Rolle ein.

- Zutrittskontrolle, Zugriffskontrolle: Systeme die personenbezogene Daten verarbeiten müssen vor unauthorisiertem Zutritt und Zugriff geschützt werden. [Con17] Dies stellt eine direkte Forderung für physische und logische Berechtigungskontrollen dar.

- Weitergabekontrolle: Beim Transport von personenbezogenen Daten die Vertraulichkeit und Integrität der Daten gewährleistet wird und dass jegliche Transaktionen protokolliert werden müssen. [Con17] Dies stellt eine direkte Forderung für Audit-Trails und Berechtigungskontrollen dar.

- Eingabekontrolle: Bei der Erfassung von personenbezogenen Daten muss die Nachvollziehbarkeit des Ursprungs gewährleistet sein. [Con17] Dies stellt eine direkte Forderung für Audit-Trails dar.

EU-DSGVO Die DSGVO stellt verschiedenste Forderungen für die sichere Erhebung, Speicherung und Verarbeitung von personenbezogener Daten. [Hin20]

- Artikel 5 - Grundsätze für die Verarbeitung personenbezogener Daten - Paragraph 1.f: Die Integrität und Vertraulichkeit personenbezogene Daten muss gewährleistet sein. [Uni16] Somit müssen geeignete Verfahren zur Zutritts und Zugriffskontrolle vorhanden sein.

- Artikel 15 - Auskunftsrecht der betroffenen Person - Paragraph 3: Das betroffene Person über die Daten erhoben wurde hat das Recht Auskunft über alle personenbezogenen Daten anzufordern. [Uni16] Hierbei sind geeignete Prozesse im Rahmen des Identitätsmanagements zu definieren. Diese müssen durch geeignete Authentifizierungsverfahren geschützt werden um die Vertraulichkeit der Weitergabe zu gewährleisten.

- Artikel 17 - Recht auf Löschung - Paragraph 1: Die betroffene Person hat das Recht eine Forderung für die unverzügliche Löschung der Daten einzureichen. [Uni16] Hierbei sind geeignete Prozesse im Rahmen des Identitätsmanagements zu definieren.

4.5 Erkenntnisse im Kontext von IT-GRC

- Die Umsetzung von IAM kann kostspielig sein denn das Management und die eingesetzten Technologien sind teuer. Rechtlichen Vorgaben sind jedoch nicht optional und die Risiken von fehlendem IAM können enorm sein.

5 Fazit

5.1 Zusammenfassung

5.2 Beantwortung der Forschungsfragen

Identität und Identitätsmanagement Eine (digitale) Identität ist eine Menge von Attributen und Rollen, inklusive Bezeichner und Zugangsdaten zur Authorisierung. So kann eine Identität eine Person, ein IT-System oder eine Anwendung darstellen. Eine Identität kann einer Entität, also einer Person oder einer Organisation zugeordnet werden. Das Identitätsmanagement ist zuständig für die Festlegung von Prozessen zur Verwaltung, Authentifizierung und Überwachung von Identitäten.

Berechtigung und Berechtigungsmanagement Eine Berechtigung ist eine Kombination aus zu berechtigender Ressource und zu berechtigender Operation auf diese Ressource. Berechtigungsmanagement bezeichnet die Prozesse für die Zuweisung, Kontrolle, Überwachung und Entzug von Berechtigungen sowie der Überwachung dieser Prozesse.

Welche Standards, Methoden, Technologien und Tools lassen sich differenzieren? Die ISO 27001 Norm in Kombination mit dem IT-Grundschutz des BSI's stellt einen Goldstandard in der Informationssicherheit in Organisationen dar. Ein wichtiger Aspekt einer ISO 27001 Zertifizierung ist die Zugriffskontrolle. Es haben sich einige standardisierte Verfahren zur Umsetzung von Identitäts- und Berechtigungsmanagement etabliert, so z.B. SAML, OAuth, OpenID Connect. Es gibt eine Vielzahl an Anbietern welche IAM Lösungen anbieten. Beispiele für große Hersteller sind Microsoft, IBM, SAP und Okta.

Welche Aufgaben und Prozesse sind im Kontext von Identitäts- und Berechtigungsmanagement zu bearbeiten? Die grundlegenden Aufgaben und Prozesse des Identitäts- und Berechtigungsmanagements sind:

- Provisionierung, Änderung und Deprovisionierung von digitalen Identitäten und Berechtigungen
- Technische Umsetzung der Infrastruktur zur Speicherung der relevanten Informationen, der Authentifizierung und der Authorisierung

- Identifikation von rechtlichen Aspekten und Standards, Planung von Prozessen zur Einhaltung dieser
- Auditierung aller Prozesse zur Identifikation von Abweichungen und Speicherung von Informationen im Rahmen der Rückverfolgbarkeit von Transaktionen

Welche betrieblichen Anwendungsfälle zeigen die Bedeutung des Identitäts und Berechtigungsmanagements auf?

Wie wird das Identitäts und Berechtigungsmanagement im Kontext der Sicherheit in der Informationstechnik eingesetzt? Das Identitäts- und Berechtigungsmanagement wird eingesetzt um Zugriffe auf schützenswerte Ressourcen einzuschränken. Dies geschieht durch geeignete Authentifizierungs und Authorisierungsverfahren.

Zuständigkeit für Identitäts- und Berechtigungsmanagement Für die Planung und Umsetzung der Prozessen des Identitäts- und Berechtigungsmanagements ist im Unternehmen der CIO verantwortlich. Dieser wird ggf. durch den CISO unterstützt denn Identitäts- und Berechtigungsmanagement ist ein sicherheitskritischer Prozess. Operativ involviert sind die Personalverwaltung und der Helpdesk. Die Personalverwaltung ist zuständig für die Erstellung, Änderung und Löschung von Identitäten und Rollen. Der Helpdesk ist die Anlaufstelle für Probleme bei der Nutzung von Identitäts- und Berechtigungsmanagement-Systemen und bei Incidents.

6 Eidesstattliche Versicherung

Literaturverzeichnis

[Yle+04] Mikko Ylen u. a. “Centralized password management in a global enterprise”. Magisterarb. 2004.

[You04] Dale Young. “Human Resources have a vital role to play within employee identity and access management”. In: *Network Security* 2004.11 (2004), S. 5–7. ISSN: 1353-4858. DOI: https://doi.org/10.1016/S1353-4858(04)00154-0. URL: https://www.sciencedirect.com/science/article/pii/S1353485804001540.

[Ben05] Messaoud Benantar. *Access control systems: security, identity management and trust models*. Springer Science & Business Media, 2005.

[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.

[Woo05] Peter Wood. “Implementing identity management security-an ethical hacker's view”. In: *Network Security* 2005.9 (2005), S. 12–15.

[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.

[BT10] Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

[Mon+10] M Casassa Mont u. a. “Economics of identity and access management: a case study on enterprise business services”. In: *HP Laboratories, Technical Report HPL-2010-11* (2010).

[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.

[HS12] Peter Haag und Marco Spruit. “Selecting and implementing Identity and Access Management technologies: The IAM Services Assessment Model”. In: *Digital Identity and Access Management: Technologies and Frameworks*. IGI Global, 2012, S. 348–365.

[RR12] V Radha und D Hitha Reddy. “A survey on single sign-on techniques”. In: *Procedia Technology* 4 (2012), S. 134–139.

[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.

[Kun+14] Michael Kunz u. a. “Analyzing Recent Trends in Enterprise Identity Management”. In: *2014 25th International Workshop on Database and Expert Systems Applications*. 2014, S. 273–277. DOI: 10.1109/DEXA.2014.62.

[Wei+15] Eva Weishäupl u. a. “Towards an economic approach to identity and access management systems using decision theory”. In: (2015).

[Con17] Daniel Conta. “Leitfaden eines mandantenunabhängigen Identity Access Management”. Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

[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.

[Hin20] Andrew Hindle. März 2020. URL: https://bok.idpro.org/article/id/24/print/.

[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.

[Uni16] Europäische Union. Mai 2016. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE.

[Del17] Deloitte. 2017. URL: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-FactsSheetforGlobalWebsite-cyber-attack.pdf.

[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.

[BSI23] BSI. Sep. 2023. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/iso-27001-basis-it-grundschutz_node.html.

[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