h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Hochschule Darmstadt

– Fachbereich Informatik –

Modernisierung einer Berechtigungsstruktur im Hostbereich für die Helvetia Schweizerische Versicherungsgesellschaft AG mittels Konzeptionen und Umsetzungsvorschlag

vorgelegt von

Lucas Stumm

Matrikelnummer: 764915

Referent	:	Professor Stephan Karczewski
Korreferent	:	Professor Dr. Urs Andelfinger

ERKLÄRUNG

Ich versichere hiermit, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die im Literaturverzeichnis angegebenen Quellen benutzt habe.

Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder noch nicht veröffentlichten Quellen entnommen sind, sind als solche kenntlich gemacht.

Die Zeichnungen oder Abbildungen in dieser Arbeit sind von mir selbst erstellt worden oder mit einem entsprechenden Quellennachweis versehen.

Diese Arbeit ist in gleicher oder ähnlicher Form noch bei keiner anderen Prüfungsbehörde eingereicht worden.

Darmstadt, 23.03.2023

Lucas Stumm

SPERRVERMERK

Diese Abschlussarbeit darf nur von der Referentin/ dem Referenten, der Korreferentin / dem Korreferenten sowie den vom Prüfungsausschuss dazu beauftragten Hochschulangehörigen eingesehen werden. Sie darf ohne ausdrückliche Zustimmung des Autors weder vollständig noch auszugsweise vervielfältigt, veröffentlicht oder Dritten zugänglich gemacht werden. Die Durchführung des Kolloquiums bleibt von der Geheimhaltung unberührt. Die Geheimhaltungsverpflichtung erlischt fünf Jahre nach Einreichung automatisch.

ZUSAMMENFASSUNG

Kurze Zusammenfassung des Inhaltes in deutscher Sprache von ca. einer Seite länge. Dabei sollte vor allem auf die folgenden Punkte eingegangen werden:

- Motivation: Wieso ist diese Arbeit entstanden? Warum ist das Thema der Arbeit (für die Allgemeinheit) interessant? Dabei sollte die Motivation von der konkreten Aufgabenstellung, z.B. durch eine Firma, weitestgehend abstrahiert werden.
- Inhalt: Was ist Inhalt der Arbeit? Was genau wird in der Arbeit behandelt? Hier sollte kurz auf Methodik und Arbeitsweise eingegangen werden.
- Ergebnisse: Was sind die Ergebnisse der Arbeit? Ein kurzer Überblick über die wichtigsten Ergebnisse als Teaser, um die Arbeit vollständig zu lesen.

Eine großartige Anleitung von Kent Beck, wie man gute Abstracts schreibt, finden Sie hier:

https://plg.uwaterloo.ca/~migod/research/beckOOPSLA.html

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

PRC Pew Research Center

FuT Führungskräfte und Teamleiter

VAIT Versicherungsaufsichtliche Anforderungen an die IT

BaFin Bundesanstalt für Finanzdienstleistungsaufsicht

NIST National Institute of Standards and Technology

IAM Identity & Access Management

K/W Konventionen/Wartbarkeit

Zf Zielerfüllungsfaktor

Gf Gewichtsfaktoren

TN Teilnutzwert

GN Gesamtnutzwert

RACF Resource Access Control Facility

CICS Customer Information Control System

API Application Programming Interface

DSGVO Datenschutz-Grundverordnung

Teil I

THESIS

1 EINLEITUNG

1.1 MOTIVATION

Viele Unternehmen verfügen über sensible Informationen, sei es zum Beispiel Versicherungen oder Krankenhäuser. Sensibel Informationen können dabei Telefonnummern oder auch Namen und Adressen sein. Diese Informationen werden auf gesicherten Servern gelagert, auf welche nur bestimmte Personen Berechtigungen haben. Diese Personen verfügen über Profile, die ihnen diese Berechtigungen zur Verfügung stellen. Jedoch kann es passieren, dass solche Profile gestohlen oder Personen gegeben werden, welche diese nicht haben sollten. Berechtigungsstrukturen sollen genau diese Szenarien verhindern. Wird aber eine Berechtigungsstruktur lange genutzt und werden nicht alle Richtlinien und Normen eingehalten, so wird diese im Laufe der Zeit unsicherer und unübersichtlicher. Das hat zur Folge, dass das Risiko, dass die sensitiven Informationen in nicht autorisierten Händen kommen, steigt. Dadurch können sogenannte „Super Accounts“ entstehen. „Super Accounts“ verfügen über zu viele, bis zu allen Berechtigungen im System. Sollte diese Person durch einen Angriff diesen „Super Account“ verlieren, wäre die gesamte Struktur kompromittiert. Dasselbe ist der Fall, wenn ein Mitarbeiter mit einem solchen Account dem Unternehmen schaden will.

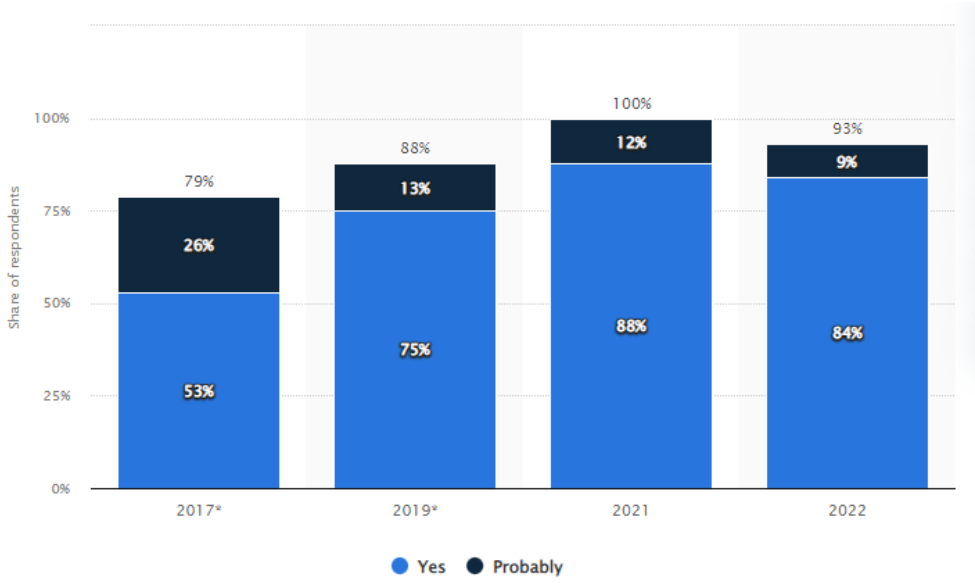

Abbildung 1.1: Eine Umfrage von deutschen Unternehmen, die von Daten Diebstahl, Espionage oder Sabotage betroffen waren. [Sta22]

Wie man in der Grafik (1.1) erkennen kann, waren 88% der befragten Unternehmen in Deutschland von Datendiebstahl, Espionage oder Sabotage in

2021 betroffen. In 2022 lag die Zahl bei 84%. Wobei man berücksichtigen muss, dass diese Befragung zwischen Januar und März stattgefunden hat und dies daher nur das erste Quartal von 2022 abdeckt. Aufgrund dessen, dass solche Angriffe wahrscheinlich sind, darf es keine „Super Accounts“ geben, da diese ansonsten in solchen Angriffen als Schwachstelle ausgenutzt werden könnten. Genauso müssen die Strukturen übersichtlich sein, damit bei einer Überprüfung es keine Probleme darstellt, festzustellen, welcher Nutzer welche Berechtigungen hat. Wenn dies nicht der Fall ist, kann es passieren, dass die jeweiligen Nutzer zu viele Berechtigungen haben und dies wäre wieder ein Problem bei Espionage oder Sabotage. Um dies zu erreichen, gibt es verschiedene Methoden und Konzepte, die die Berechtigungsstrukturen sicher und übersichtlich gestalten.

1.2 ZIEL DER ARBEIT

Diese Arbeit ist eine Vergleichsarbeit, bei der verschiedene Konzepte verglichen werden. Dabei wird auf die folgende Fragestellung in dieser Arbeit eingegangen, *inwieweit kann man bestehende Berechtigungsstrukturen im Hostbereich verändern und optimieren kann*. Dazu gibt es drei Unterfragen, welche verwendet werden, um die Problemstellung systematisch zu beantworten.

- *Welche Konzepte werden derzeit für Berechtigungsstrukturen verwendet, um diese sicher und übersichtlich zu gestalten?*
- *Wie unterscheiden sich die verschiedenen Konzepte?*
- *Womit kann man die verschiedenen Konzepte vergleichen?*

Die erste Unterfrage wird durch eine Recherche mit verschiedenen Arbeiten im Bereich der Berechtigungsstruktur beantwortet. Dies soll einen Überblick zum Stand der Technik geben. Anschließend wurden mehrere Befragungen durchgeführt, um die bestehenden Konzepten nach den Wünschen der Befragten anzupassen. Darauf basierend werden die bestehenden Methoden geranked und verglichen. Dies beantwortet die zweite Unterfrage mittels des erstellten Vergleiches.
Um die dritte Frage zu beantworten, wird ein Schema verwendet, welches als eine Hilfestellung zur Konzeptauswahl dienen wird. Zum Schluss wird eine Alternative zum bestehenden System vorgestellt. Dies ist die Arbeit in visueller Form.

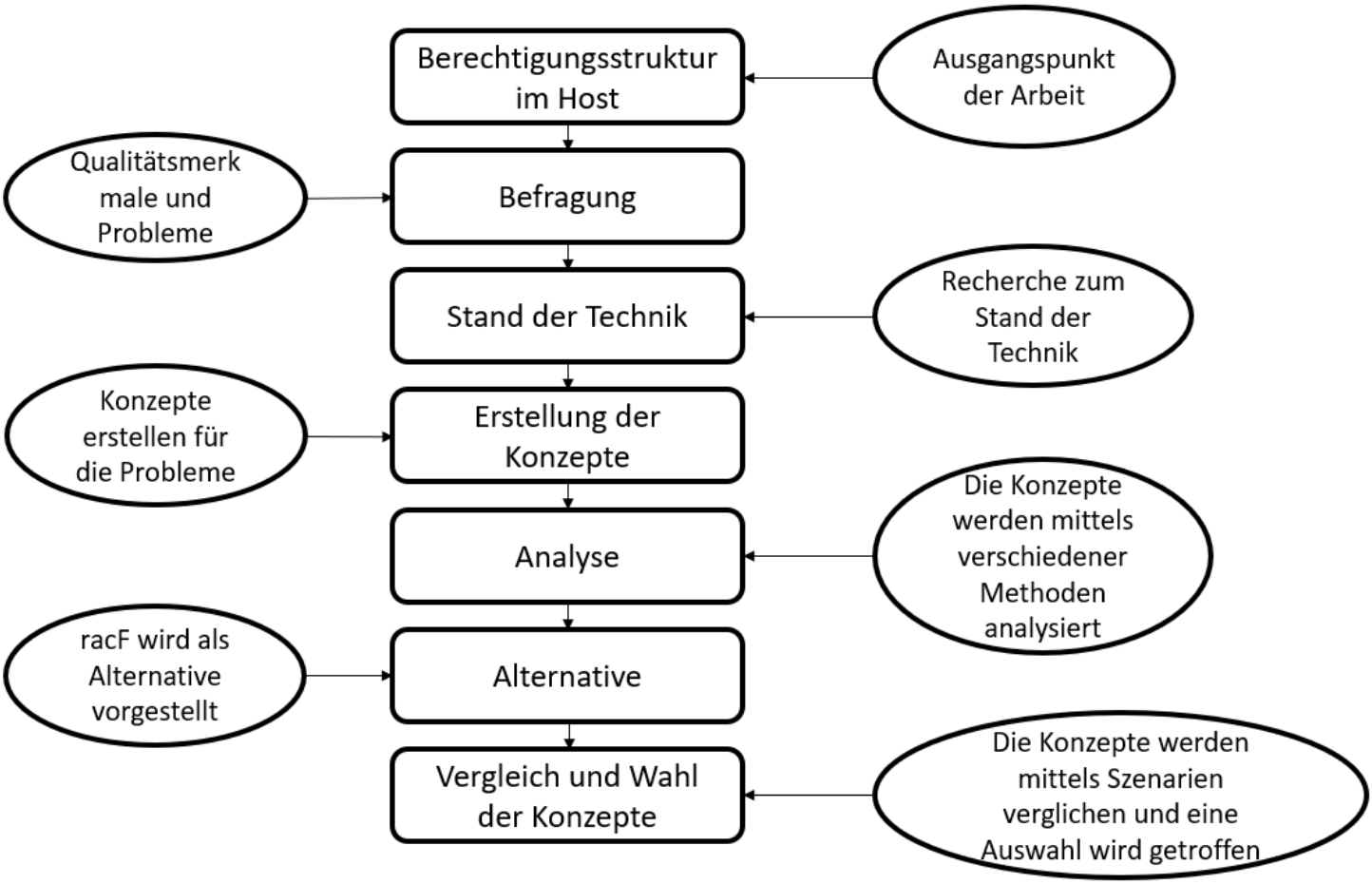

Abbildung 1.2: Aufbau der Arbeit

1.3 URSACHE-WIRKUNGS-DIAGRAMM

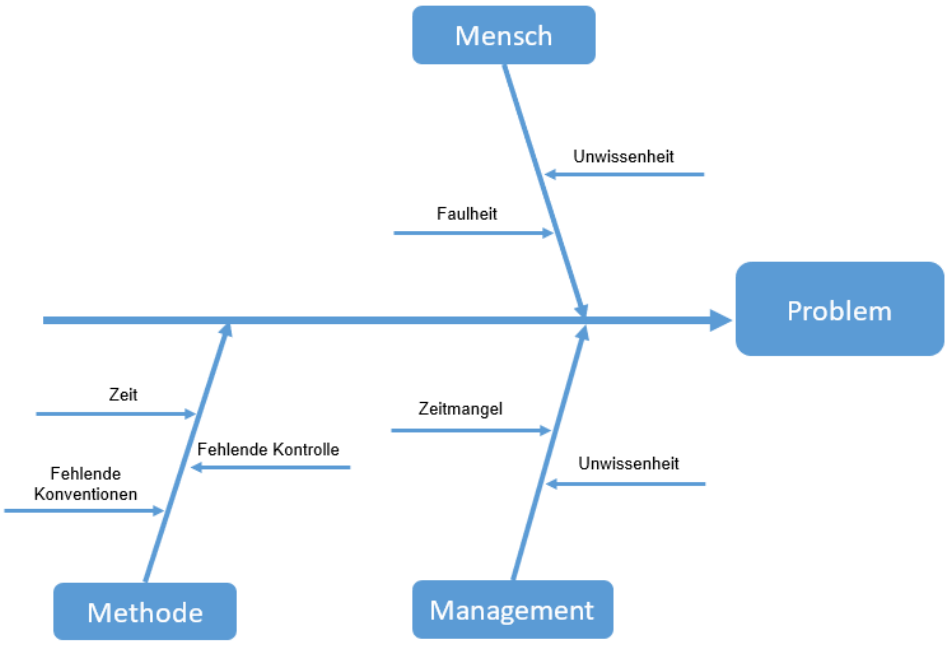

Abbildung 1.3: Ursache-Wirkungs-Diagramm (Fischgrätenmodell)

Im Ursache-Wirkungs-Diagramm wurden dabei die folgenden drei Punkte als Hauptursache für das Problem der bestehenden Berechtigungsstruktur erkannt.

- Mensch
- Management
- Methode

Bei Mensch sind die Mitarbeiter genannt, die die Berechtigungsstruktur verwalten und hegen. Dort wurden die Punkte Faulheit und Unwissenheit genannt. Dies liegt daran, dass es nicht unüblich ist, dass diese gewisse Formalien ignorieren, um einfacher das Problem zu beheben. Auf der anderen Seite ist auch die Unwissenheit ein Problem, da die gesamte Struktur so gewachsten ist, ist es unmöglich für jemand diese komplett nachzuvollziehen.
Das Management hat nicht die Zeit, sich genau mit dem Problem zu beschäftigen. Dies hat zur Folge, dass das Management wie die Mitarbeiter unwissend sind.
Bei der Methode steht die Zeit, fehlende Kontrolle und fehlende Konventionen als Problem dar. Mit der Zeit ist gemeint, dass die aktuelle Problemstellung schon so lange der Fall ist, dass dies ein Problem ist. An vielen Stellen fehlt bei der bestehenden Berechtigungsstruktur Kontrollen. Dies ist zum Beispiel der Fall, wenn ein Account wieder aktiviert wird oder die Überprüfung von Profilen. Denn wenn es diese gäbe, dürfte es keine rekursiven Beziehungen geben. Es fehlt auch eine allgemeine Konvention, wie die Profile

in den verschiedenen Fachbereichen funktionieren. Dies sorgt dafür, dass es die Mitarbeiter schwerer haben alle Verbindungen zu verstehen und macht die gesamte Struktur komplexer.

2 DEFINITIONEN

Dieses Kapitel erklärt und beschreibt einige der zentralen Begriffe zum Thema des Hosts und der Berechtigungsstrukturen. Dadurch soll der Leser ein Grundverständnis erhalten, um die folgenden Kapitel zu verstehen.

2.1 HOST/MAINFRAME

Der Host bzw. Mainframe ist ein Komplex aus verschiedenen Hochleistungscomputern. Der Anbieter „IBM“ definiert diesen dabei wie folgt:

„At their core, mainframes are high-performance computers with large amounts of memory and processors that process billions of simple calculations and transactions in real time.“ [IBM]

Oder übersetzt:

„Im Kern besteht der Mainframe aus Hochleistungsrechnern, welche über einen großen Speicher verfügen, und in der Lage sind, Milliarden von einfachen Prozessen und Transaktion in Echtzeit durchzuführen.“ [IBM]

Dabei spielt der Mainframe eine wichtige Rolle in der Finanzindustrie, welche widerstandsfähige, sichere und agile Server benötigt. Dies ist der Fall, weil die Finanzindustrie über viele sensible Daten verfügt. Daher müssen die Server sicher und widerstandsfähig sein, damit diese Daten nicht verloren gehen oder gestohlen werden. Zudem müssen die Server agil sein, da die Technologie und die Regulierungen für den Mainframe sich stetig ändern und dieser daher immer auf dem neuesten Stand sein muss. Der Mainframe muss die Regularien vom Versicherungsaufsichtliche Anforderungen an die IT (VAIT) erfüllen, die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) aufgestellt werden. Die BaFin soll eine konsistente IT-Strategie vorgeben, an die sich die Unternehmen halten müssen. [BaF]

2.2 BERECHTIGUNG

Dabei definiert die National Institute of Standards and Technology (NIST), welche eine Institution von amerikanischer Regierung ist, Berechtigungen wie folgt:

„The right or a permission that is granted to a system entity to access a system resource.“ [ST]

Dies bedeutet:

„Das Recht oder die Erlaubnis haben, um auf System Ressourcen einer Systemeinheit zu zugreifen.“ [IBM]

Im Kontext des Mainframebereiches betrifft dies bei Helvetia hauptsächlich das Betrachten und Zugreifen über Dialogmasken auf Daten. Die Grafik (2.1)

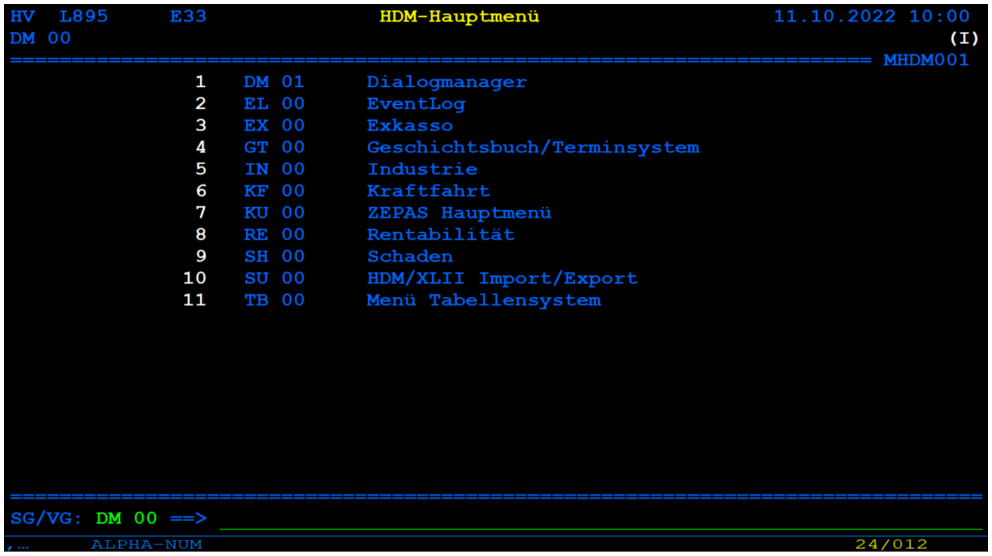

Abbildung 2.1: Beispiel Dialogmaske

zeigt eine solche Dialogmaske. Anhand dieser Dialogmaske kann man erkennen, dass der Nutzer L895 für die aufgezählten weiteren Dialogmasken (EL 00, EX 00, ...) zumindest die Leseberechtigung hat. Zudem hat dieser die Schreibberechtigungen auf die Dialogmaske DM 00, da dieser sich in dieser Maske aufhält.

In dieser Grafik (2.2) kann man die Profile und individuellen Berechtigun-

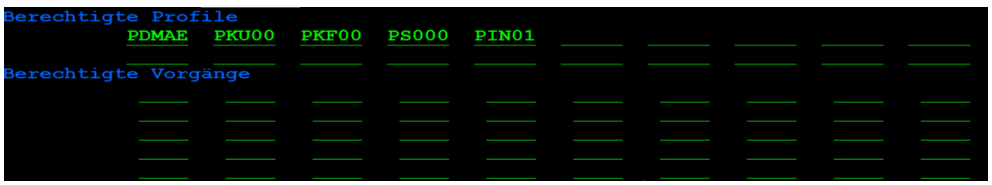

Abbildung 2.2: Berechtigungsdialogmaske

gen sehen, die der Nutzer L895 besitzt. Dabei sind Profile eine Ansammlung von Berechtigungen.

2.3 BERECHTIGUNGSSTRUKTUR

Eine Berechtigungsstruktur besteht aus den Berechtigungen, die im Unterkapitel (2.2) definiert werden, und aus der Struktur. Dabei definiert Oxford

Struktur wie folgt:

„the way in which the parts of something are connected together, arranged or organized; a particular arrangement of parts“ [Dic]

Dies bedeutet, dass die Teile miteinander verknüpft, angeordnet oder organisiert sind. [Dic]
In diesem Zusammenhang bedeutet Berechtigungsstruktur die Verknüpfung, Anordnung oder Organisation von Berechtigungen. Wie man in der Grafik

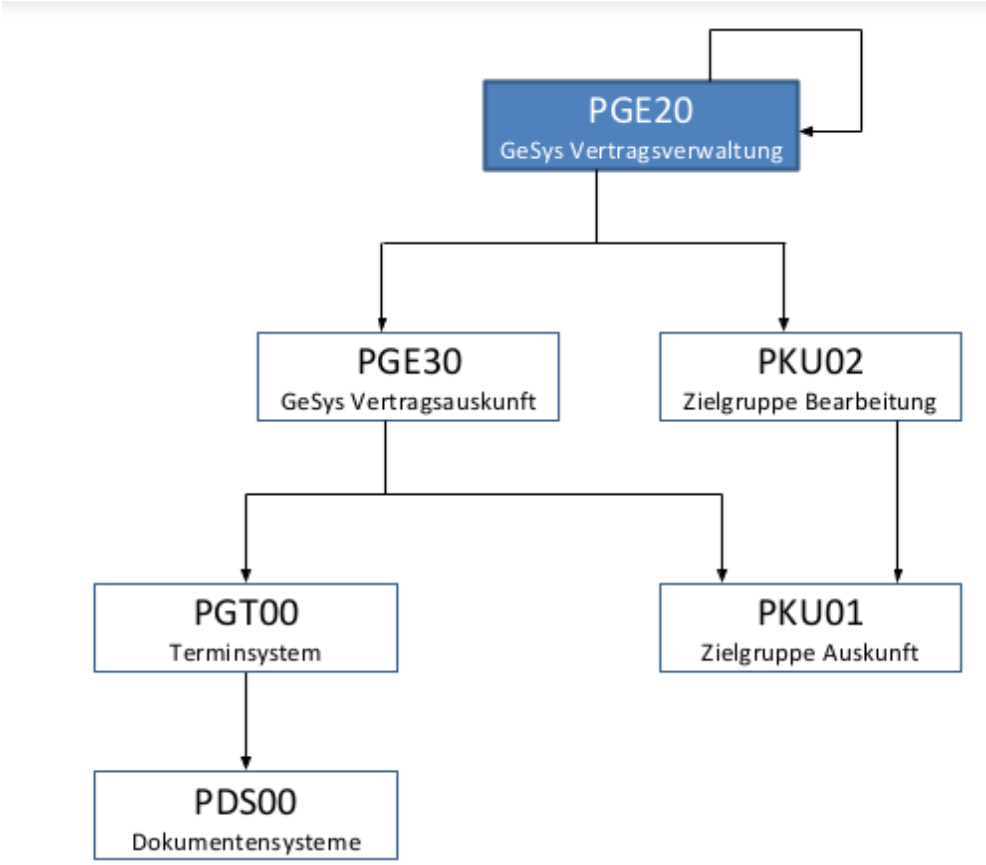

Abbildung 2.3: Teilausschnitt der Berechtigungsstruktur der Helvetia

(2.3) erkennen kann, sind die Profile hierarchisch aufgebaut. Diese Profile beinhalten die Berechtigungen.

PGE00	Gewerbe Bea	PGT10		PZIST	PNE20	PGE20						GE00					
PGE01	Gewerbe Auskunft											GE00	GEPA	GETA			
PGE20	GeSys Vertra	PGE20	PGE30	PKU02								GENA	GEEA	GEVA	GEAS	GEER	GEEU
PGE21	GeSys Vertra	PGE20															
PGE30	GeSys Vertra	PKU01	PGT00									DM00	GE00	GE20	GEB1		

Abbildung 2.4: Berechtigungen für die Profile PGE20 und PGE30

Die Grafik (2.4) zeigt, dass die Profile PGE20 und PGE30 zum Beispiel über die folgenden Berechtigungen verfügen:

- DM00
- GEEA
- GEVA
- GE20

Daher ist die aktuelle Berechtigungsstruktur hierarchisch bei der Helvetia.

2.4 IAM

Die Virginia IT Agency beschreibt IAM wie folgt: Das Identity & Access Management (IAM) ist eine Möglichkeit, sämtliche Nutzer und Profile, welche man zu den jeweiligen Personen über die IT-Umgebung über Nutzerrollen und Businessregeln zu ordnen kann, zu handhaben. Dabei ist die Zugriffverwaltung die Möglichkeit die Zugriffskontrolle über Regeln auf verschiedenen Plattformen einzuhalten. Ein wichtiger Teil von IAM ist sicherzustellen, dass die Nutzer einen sicheren Zugriff auf die Ressourcen haben und auch nur auf die Ressourcen, die sie benötigen, um ihre Arbeit zu erledigen. [Polo7] Im Bild (2.5) kann man erkennen, dass wenn ein Nutzer oder

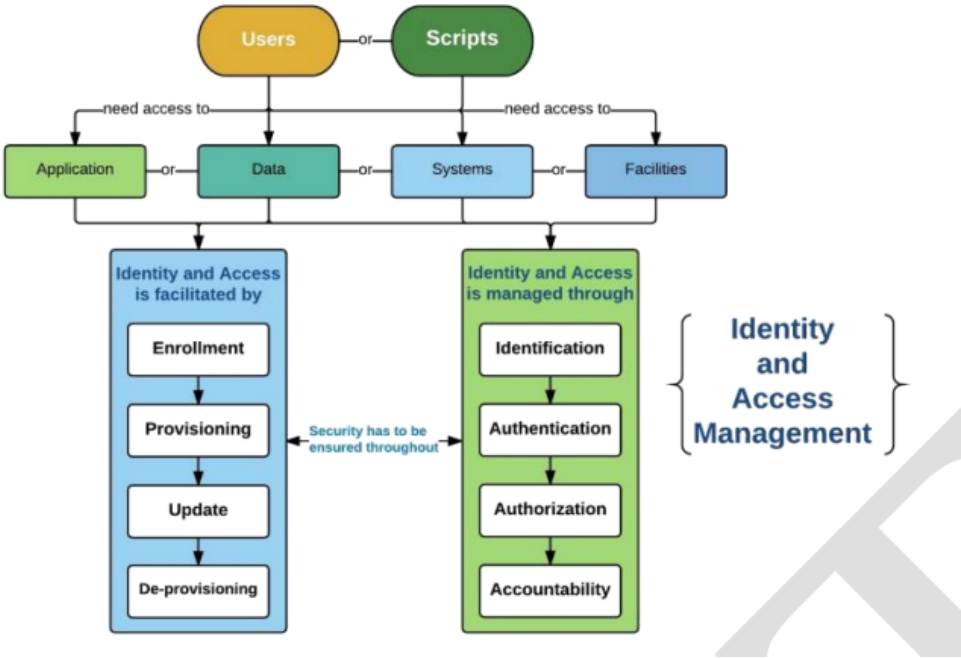

Abbildung 2.5: Übersicht von IAM [Moh19]

Programm Zugriff auf eine Ressource möchte, dieser die Identifizierung, Authentifizierung, Autorisierung, sowie Rechtschaffenheit vorlegen und einhalten muss. [Moh19] Beispielsweise wenn der Nutzer Lucas Stumm Daten vom

Host haben möchte, muss dieser durch verschiedene Schritte gehen. Als Erstes muss sich dieser Identifizieren mittels eines Nutzernamens und Passwort. Während dieser sich durch die Menüs manövriert hat, wird überprüft, ob Lucas Stumm überhaupt die Berechtigungen hat, diese Menüs sehen und auswählen zu können. Wenn dies der Fall ist, kann der Nutzer auf die Daten zugreifen.
Im Rahmen dieser Ausarbeitung handelt es sich bei den Ressourcen, um die Berechtigungen (2.2).

3 RECHERCHE

In diesem Kapitel geht es um mehrere selbstdurchgeführte Befragungen zur Berechtigungsstruktur und der jährlichen Rezertifizierung. Die jährliche Rezertifizierung ist die Überprüfung, ob die Mitarbeiter ihre Berechtigungen benötigen oder nicht. Diese wird von den Teamleitern und Führungskräften durchgeführt, welche die Berechtigungsstruktur nutzen, um dies zu tun. Dafür wurden drei verschiedene Gruppen befragt. Die Ergebnisse sind die Grundlage für die Notwendigkeit einer sicheren und übersichtlichen Struktur sowie die Feststellung der Hauptprobleme der bestehenden Struktur. Dabei wurde die Quelle [ML19] als primäres Grundgerüst verwendet, um die Befragung strukturiert und erfolgreich abzuschließen. Ebenso wurde die Quelle [Cen] genutzt.

3.1 VORGEHENSWEISE

Für die Befragung wurde zuerst analysiert, welche Stakeholder es gibt. Bei der Analyse wurden die folgenden drei Stakeholder-Gruppen identifiziert:

- FuT
- IT-Systemspezialist
- Mitarbeiter

Die FuT entsprechen den Stakeholdern, die die Berechtigungsstruktur für die jährliche Rezertifizierung nutzen. Diese haben eine hohe Priorität, da sie die Berechtigungsstruktur direkt verwenden und die Sicherheit der Struktur gewähren.
Die IT-Systemspezialisten sind die Stakeholder, die an der Berechtigungsstruktur gearbeitet haben. Ebenso wie die Teamleiter und Führungskräfte haben die IT-Systemspezialisten auch eine hohe Priorität, weil sie die Struktur warten und verändern.
Die Mitarbeiter umfassen das restlichen Arbeitspersonal. Im Gegensatz zu den anderen beiden Stakeholdern haben die Mitarbeiter eine geringe Priorität, da diese weder die Struktur nutzen noch einen anderen Kontakt haben.

Nachdem diese drei Stakeholder festgestellt worden sind, wurde spezifisch für diese drei Gruppen Fragenkataloge entwickelt. Dabei ist das Ziel festzustellen, welche die größten Probleme, aus der Sicht der Teamleiter und Führungskräfte sowie IT-Systemspezialisten, haben. Die Mitarbeiter wurden befragt, über wie viele Berechtigungen sie verfügen, die sie eigentlich nicht mehr benötigen. Die große Herausforderung besteht dabei, die richtigen Fragen für die Fragenkataloge zu entwerfen. Die Institution Pew Research Cen-

ter (PRC) hat festgestellt, dass bei geschlossenen Fragen die Befragten zu einem großen Teil (über 90%) eine der vorgeschlagenen Antworten gewählt haben. [Cen] Dies stellt ein Problem dar. Wenn die Fragen geschlossen sind, dann kann es dazu führen, dass die befragten nicht die Probleme angeben, die sie sehen. Auf der anderen Seite sind offene Fragen auch eine Herausforderung, da es schwierig wird, die verschiedenen Antworten zu quantifizieren und auswerten zu können. Ebenso ist die Wortwahl ein entscheidender Faktor. In einer Studie von PRC in 2003 wurden die Personen befragt, ob diese für oder den Krieg in Irak sind, um Saddam Hussein's Herrschaft zu beenden. 68% haben ja gesagt und 25% für nein. Darauf wurde die Frage geändert zu, ob diese für oder den Krieg in Irak sind, um Saddam Hussein's Herrschaft zu beenden, selbst wenn es Tausende Verluste gibt. Mit dieser Änderung haben nur noch 43% dafür gestimmt und 48% dagegen. [Cen]
Dies ist relevant, da zum Beispiel bei der Befragung der Mitarbeiter bei einer falschen Formulierung der Gedanke bekommen könnte, dass dieser mit der Beantwortung der Frage seine Zustimmung gibt, dass ich ihm die genannten Berechtigungen entferne. Dies kann zu fehlerhaften Ergebnissen führen. Deshalb müssen die Fragen gut überlegt sein.

Für die FuT wurden die folgenden Fragen formuliert:

- Wie handhabbar ist für Sie der aktuelle Prozess der jährlichen Rezertifizierung der Vorgangsberechtigung Ihrer Mitarbeiter?
- Was finden Sie im aktuellen Rezertifizierungsprozess gut?
- Was finden Sie im aktuellen Rezertifizierungsprozess schlecht?
- Was würden Sie gerne am aktuellen Rezertifizierungsprozess ändern?
- Was halten Sie von der Idee das Profile entweder nur noch (Unter-)Profile oder Profile ausschließlich Berechtigungen beinhalten?
- Soll es eine einheitliche Strukturierung für die Berechtigungsstruktur innerhalb der Bereiche geben?
- Haben Sie weitere Anmerkungen?

Die Fragen wurden größtenteils offen formuliert, um am besten die Probleme am bestehenden System zu finden. Dabei umfassen die ersten drei Fragen den Ist-Zustand der Berechtigungsstruktur und wie dies die FuT finden. Fragen vier, fünf und sechs fragen nach dem Soll-Zustand der Berechtigungsstruktur. Dabei wurden auch konkrete Vorschläge in den Fragen unterbreitet, um einen ersten Eindruck von den FuT zu erhalten. Zum Schluss gab es noch die offene Frage, ob es weitere Anmerkungen gibt, um eventuelle Antworten und Anmerkung zu erhalten, die durch die vorherigen Fragen nicht abgedeckt wurden.

Für die IT-Systemspezialisten wurden die folgenden Fragen formuliert:

- Welche Erfahrung haben Sie mit der Berechtigungsstruktur gehabt?
- Auf welche Probleme sind Sie im Zusammenhang mit der Berechtigungsstruktur gestoßen?
- Gibt es Sachen, die man bei der Berechtigungsstruktur beachten muss?
- Haben Sie Vorschläge, wie man die Berechtigungsstruktur besser gestalten könnte?
- Haben Sie weitere Anmerkungen?

Die erste Frage soll dazu anregen sich über das Thema Gedanken zu bilden, damit die folgenden Fragen einfacher zu beantworten sind. Dabei soll die zweite Frage klarstellen, welche Herausforderungen die befragte Person mit der Struktur hatte. Dies ermöglicht es, dann präventiv gegen diese vorzugehen und dies direkt mit in die neuen Konzepte zu integrieren. Bei der dritten Frage sollen mögliche Ausnahme Fälle genannt werden, die bei einem Konzept mitberücksichtigt werden müssten. Anschließend wird gefragt, ob die Person eventuell sich selbst Gedanken gemacht hat, welche Möglichkeiten es gibt, um die aktuelle Struktur zu verbessern. Zum Abschluss wird gefragt, ob es weitere Anmerkung gibt, welche nicht von den vorherigen Fragen abgedeckt wurden.

Die Mitarbeiter haben die Frage bekommen:

Wie viele Vorgangsberechtigungen Sie in der Produktion von Hoblink haben, die Sie nicht mehr nutzen?

Bei dieser Frage war es wichtig diese so zu formulieren, dass die befragte Person nicht den Eindruck bekommt, dass ich ihr die Berechtigungen wegnehmen möchte. Dies würde ansonsten zu fehlerhaften Ergebnissen führen. Die Befragung der Mitarbeiter dient dazu, um die Problematik der nicht optimalen Berechtigungsstruktur darzustellen und auch um feste Zahlen zu haben.

Dabei wurden die FuT in der Informatikabteilung befragt, da diese am ehesten Kontakt mit der Berechtigungsstruktur haben. Andere FuT außerhalb der Informatik wurden nicht befragt, weil die Wahrscheinlichkeit zum zeitlichen Aufwand zu gering ist, hier nützliche Informationen zu erhalten. Bei den IT-Systemspezialisten wurden alle Personen befragt, die mir bekannt waren. Von den Mitarbeitern wurden zufällig von jedem Team von jeder Abteilung eine Person befragt. Dies soll dazu dienen, dass man das Ergebnis skalieren kann.

3.2 AUSWERTUNG

Die folgenden Grafiken zeigen die Antworten der jeweiligen Befragungen.

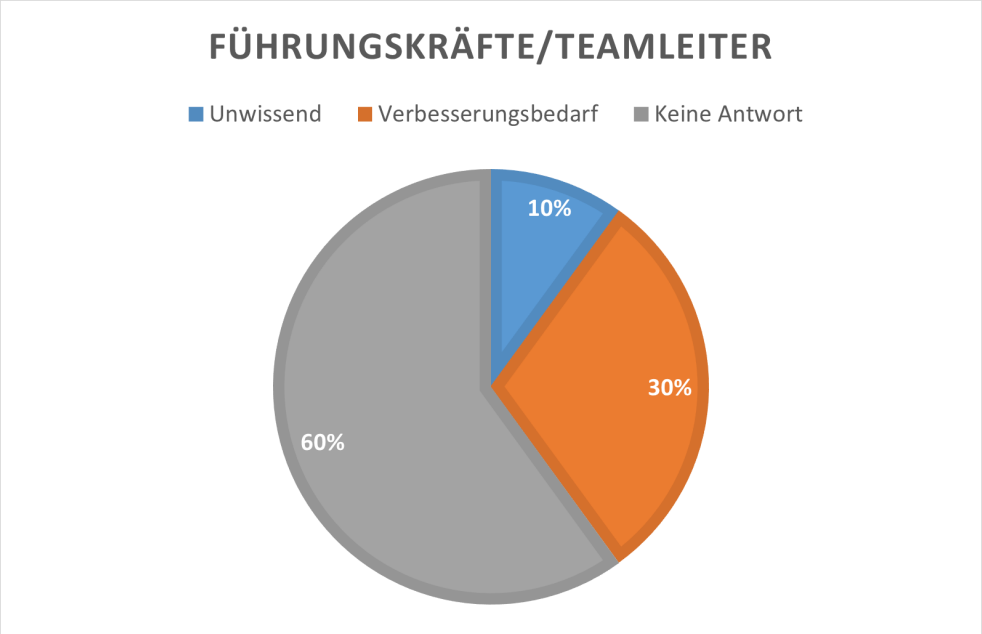

Abbildung 3.1: Auswertung der Ergebnisse von den FuT

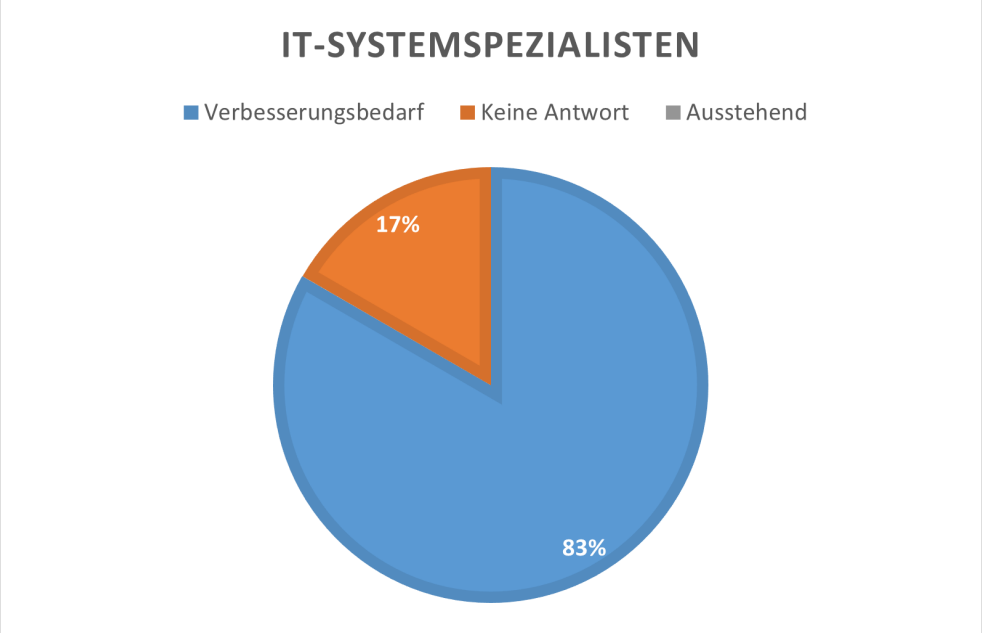

Abbildung 3.2: Auswertung der Ergebnisse von den IT-Systemspezialisten

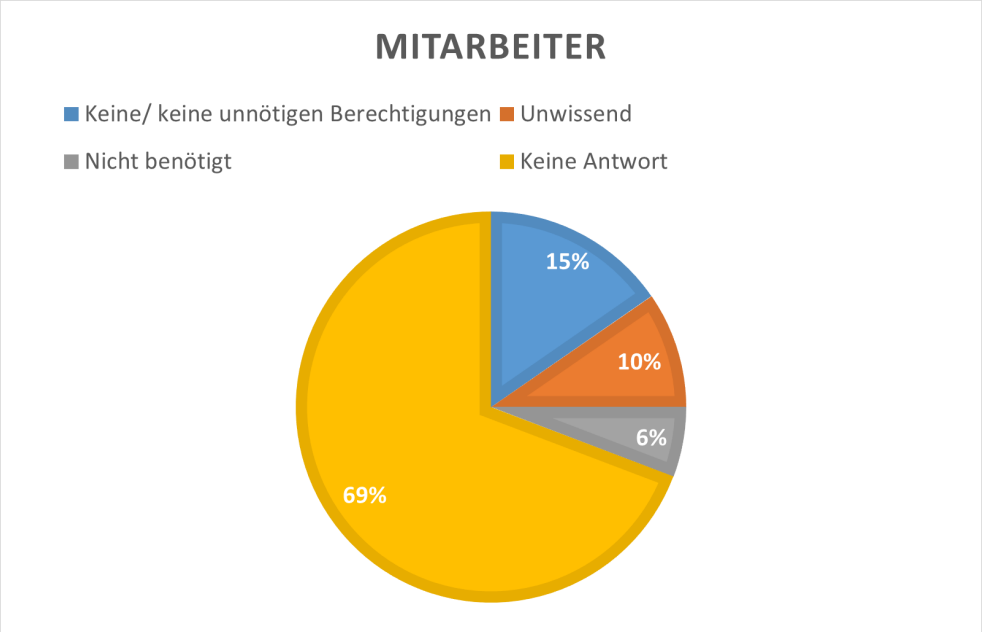

Abbildung 3.3: Auswertung der Ergebnisse von den Mitarbeitern

Von den zehn befragten Teamleitern (Grafik 3.1) haben vier an der Umfrage teilgenommen. Von diesen vier haben drei angegeben, dass sie mit der aktuellen Struktur und Vorgehen umgehen können, es aber Verbesserungsbedarf besteht. Dabei haben sie folgende Vorschläge gemacht:

- Veraltete Vorgänge entfernen
- Helvetia Leben braucht keine HV/HI Mandanten
- Nur Änderung zum Vorjahr vergleichen
- Überprüfung von Sachgebieten anstelle von Profilen/Vorgängen

Der erste Punkt wird aktuell sukzessive umgesetzt, ist jedoch nicht einfach und dauert lange. Die Helvetia Versicherung ist aufgrund von gesetzlichen Regelungen in die Helvetia Leben und Helvetia Komposit aufgeteilt. Dabei umfasst Helvetia Leben alle Versicherungen für die Person. Dazu verfügt die Helvetia über drei Mandanten (HV, HI und HL). Der HV-Mandant wird für den Zugriff von deutschen Daten verwendet. HI im Gegensatz ist der Mandant für internationale Informationen. Helvetia Leben hat explizit den HL-Mandanten. Deswegen wurde vorgeschlagen, dass die Helvetia Leben Mitarbeiter nicht die anderen beiden benötigen. Jedoch ist dies nicht umsetzbar, da es Fälle gibt, bei denen diese auf die anderen Daten zugreifen müssen. Zum Beispiel, wenn ein Vermittler nach Daten fragt, die nur über den HV-Mandanten verfügbar sind, muss der Mitarbeiter in der Lage sein, auf diese zu zugreifen.
Der Vorschlag, dass man nur Änderung zum Vorjahr vergleicht, würde den Aufwand massiv reduzieren, würde aber nicht mehr den Sinn der jährlichen Rezertifizierung erfüllen. Das Problem dabei besteht, dass ein Mitarbeiter

nach mehreren Jahren eine Berechtigung nicht mehr benötigt. Wenn man dann nur den Vergleich zum Vorjahr betrachtet, würden dieser Person nie die älteren Berechtigungen entzogen werden können.
Die Überprüfung mittels Sachgebiete, anstelle von Profilen/Vorgängen, findet aktuell schon statt, da der Aufwand bei der Überprüfung der individuellen Profile/Vorgänge zu groß wäre. Zudem bestände dann auch die große Wahrscheinlichkeit, dass versehentlich gewisse Profile/Vorgänge übersehen werden, welche eigentlich entfernt werden müssten.

Von den IT-Systemspezialisten haben sechs von sieben an der Befragung (3.2) teilgenommen. Im Interview mit den Befragten Personen haben diese verschiedene Anmerkung zum bestehenden System geäußert:

- Chaotische Organisation
- Intransparent
- Schreckliches durcheinander

Wie man an den Bemerkungen erkennen kann, sehen die IT-Systemspezialisten das größte Problem bei der Hierarchie und dem Aufbau der Struktur. Dabei haben sie verschiedene Vorschläge gemacht, wie man die Struktur aus ihrer Sicht verbessern kann.

- Transparenter gestalten
- Baumstruktur „verdammen“
- Profile in Profile abschaffen
- Eindeutige Struktur
- Konventionen

Auch wurde angesprochen, ob man das bestehende System nicht in RACF auslagern könnte. Dabei wurde erwähnt, dass man sich darüber schon mal Gedanken gemacht hat. Hierauf wird im Kapitel (5.4) näher eingegangen. Zudem haben sie auch eine eigene Lösungsidee vorgeschlagen. Diese wird in (4.5) erläutert.

Bei der Umfrage (3.3) von den Mitarbeitern haben 16 von 52 geantwortet. Dabei haben sechs Personen angegeben, dass diese über gar keine oder keine unnötigen Berechtigungen verfügen. Fünf haben geschrieben, dass sie nicht sicher sind, und weitere fünf haben angegeben, dass diese über Berechtigungen verfügen, die sie eigentlich nicht bräuchten. Nachdem ich die Ergebnisse der Personen ausgewertet habe, habe ich mir von ein paar Personen, die Berechtigungen angesehen und habe dies mit ihren Aussagen verglichen. Dabei habe festgestellt, dass zwei Personen die angegeben haben, dass diese über gar keine Berechtigungen verfügen und den Host nicht verwenden, über Berechtigungen verfügen. Bei Nachfrage hat es sich herausgestellt, dass

es sich um alte Accounts handelt, die sie für eine ehemalige Aufgabe benötigt hatten. Wenn man dies berücksichtigt, ändert sich der Graphen (3.3) wie folgt. Wenn man jetzt die Grafik betrachtet kann man erkennen, dass von

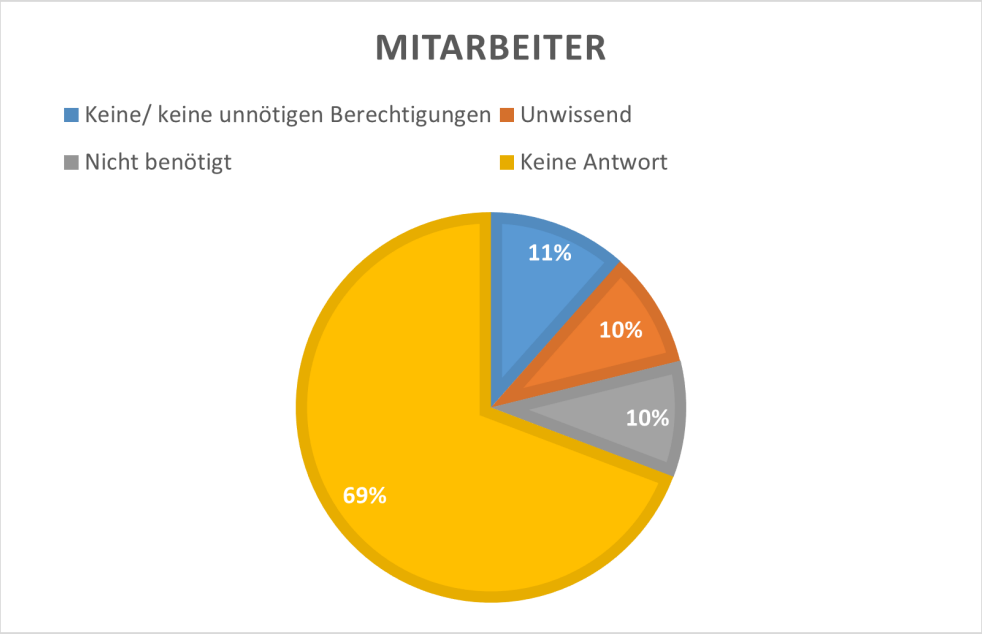

Abbildung 3.4: Auswertung der Ergebnisse von den Mitarbeitern nach der Überprüfung

den Personen die geantwortet haben 33% zu viele Berechtigungen haben.

3.3 ERGEBNIS

Wie man aus der letzten Grafik (3.4) erkennen kann, besteht aktuell ein Problem. Sollte einer dieser Mitarbeiter sein Passwort für diese Berechtigungen durch beispielsweise einen Phishingangriff weitergeben oder gegen das Unternehmen vorgehen wollen, könnte dies einen größeren, aber vermeidbaren Schaden anrichten. Außerdem existiert eine mögliche Dunkelziffer bei der Befragung der Mitarbeiter, die nicht ehrlich geantwortet haben, weil diese eventuelle Angst haben, dass das Resultat der Befragung dafür sorgt, dass ihnen Berechtigungen entfernt werden. Deswegen stelle ich die Annahme, dass 33% der Mitarbeiter über Berechtigungen verfügen, die diese nicht benötigen. Daher stellt die 33% lediglich das Minimum dar. Die Helvetia versendet jährlich Phishing Mails, um die Mitarbeit zu trainieren, diese zu erkennen. Dabei haben 10% der Mitarbeiter ihre persönlichen Informationen preisgegeben (3.5). Wäre dies kein Testfall, sondern ein echter Phishing-Angriff und einer der 33% Mitarbeiter würde dem Angreifer diese Informationen geben, hätte der Angreifer es einfacher das gesamte System zu kompromittieren.

Genauso stellen deaktivierte Accounts ein Problem dar, da diese nicht mehr überprüft werden und bei der Reaktivierung keine Rezertifizierung stattfin-

det, ob diese Person noch sämtliche Berechtigungen benötigt. Wodurch die Person Wahrscheinlichkeit besteht, dass diese zu viele Berechtigungen hat. Zudem hat die Befragung der FuT gezeigt, dass diese über kein tieferes Verständnis zur Struktur oder des Vorgehens verfügen, da diese nicht logische Vorschläge gemacht haben sowie Vorgehensweisen, die bereits verwendet werden. Die Entwickler, die bisher an der Berechtigungsstruktur gearbeitet haben, haben verschiedene Ansätze und Probleme aufgezeigt, die im nächsten Kapitel ausführlicher behandelt werden.

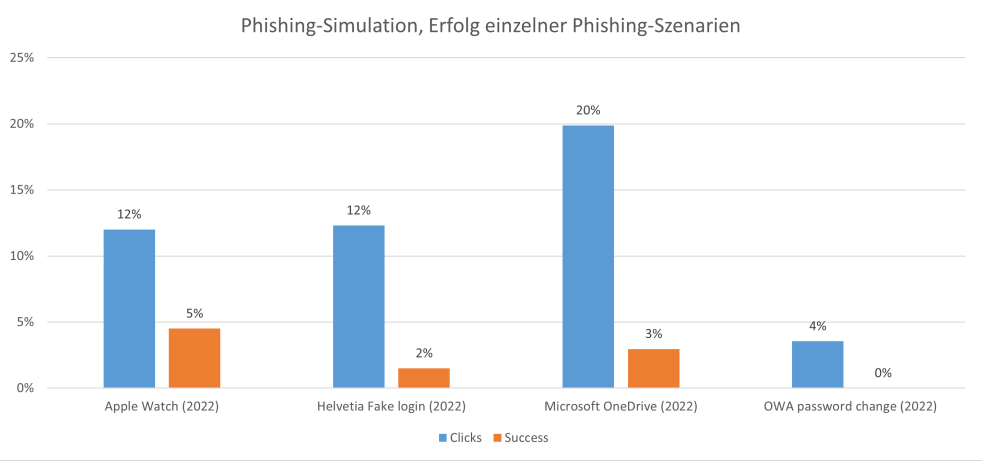

Abbildung 3.5: Phishing versuche der Helvetia an den eigenen Mitarbeitern [Hel]

3.4 IST-ZUSTAND

Der Ist-Zustand der Berechtigungsstruktur der Helvetia ist eine chaotische Organisation. Zum Beispiel kann man im Bild 2.3 erkennen, dass das Profil PGE20 eine rekursive Beziehung hat. Außerdem gibt es viele redundante Profile innerhalb eines Profils. Das Profil Azub enthält zum Beispiel die Berechtigung PNE10 welche zwölfmal vergeben wird. Dies macht es schwierig festzustellen, wer alles eine spezifische Berechtigung/Profil hat, da diese an verschiedenen Stellen vorkommt.
Zusätzlich gibt es Profile mit aufsteigenden Nummern wie zum Beispiel PNE10 und PNE20. Dabei besteht das Problem, dass diese manchmal einen Bezug zueinander und manchmal gar keinen haben. Wie man im Graphen

TD000032	PPV00	Privas Anwen	PPV10	PPV30	PPV40	PNE20
TD000032	PPV10	Privas Produk	PTD30			
TD000032	PPV20	Privas Produk	PPV10			
TD000032	PPV30	Privas Vertrag	PTD30			
TD000032	PPV40	Privas Vertrag	PGT00	PZIST	PNE20	PVP05
TD000032	PPV42	Privas Orgam	PNE20			
TD000032	PPV50	Privas f.Verm	PKU02			
TD000032	PPV51	Privas Puntob	PKU01			
TD000032	PPV54	TierKranken	PKU01			

Abbildung 3.6: Ausschnitt der Berechtigungsstruktur

erkennen kann, hat das Profil PPV00 einen Bezug zu PPV10, PPV30 und PPV40, aber PPV54 hat gar keinen Bezug dazu. Zudem sind dort Profile von anderen Fachbereichen vorhanden, welches das Risiko auf rekursive Beziehung erhöht und es schwierig macht, die Struktur zu verstehen. In diesem Fall fehlt es an einer Richtlinie, welche vorgibt, wie die Beziehung zwischen diesen Profilen sein soll. Diese wäre notwendig, da es ansonsten für jemanden, der nicht ein perfektes Wissen hat, welches Profil welche Berechtigungen enthält, es nicht möglich ist, dies nachzuvollziehen.

4 KONZEPT

In diesem Kapitel wird darauf eingegangen, wie vorgegangen wurde, um verschiedene Konzepte zu entwickeln. Dabei werden die vorher erwähnten Befragungen (3) verwendet, um eine Lösung für die individuellen Probleme zu entwickeln. Zudem wird der Stand der Technik betrachtet und ein Vergleich mit den Datenbankstrukturen gezogen. Dies wird getan, da Datenbanken eine ähnliche Struktur, wie die Berechtigungsstruktur der Helvetia, haben. Anschließend werden die Probleme aus den Befragungen quantifiziert, um daraus die verschiedenen Konzepte zu entwickeln.

4.1 KONZEPTENTWICKLUNG

4.1.1 *Stand der Technik*

In der Welt von Cloud Computing wird IAM als Sicherheitsmaßnahme verwendet. Dabei wird mittels IAM die Identität und der Zugriff reguliert. IAM kann daher in die folgende fünf Punkte gegliedert werden.

1. Authentifizierung der Person
Dabei wird überprüft, ob die Person auch wirklich die ist, als welche diese sich ausgibt. Um dies sicherzustellen, gibt es verschiedene Methoden. Ein Nutzername mit einem Passwort ist die gängigste Methode, um dies zu tun. Dies wird von den meisten Webseiten und Computern verwendet. Um die Authentifizierung sicherer zu gestalten, werden mehrere Faktoren berücksichtigt, um eine Person zu identifizieren. Dies kann zum Beispiel durch einen Fingerabdruck stattfinden. [SSD15] (S.1482)

2. Berechtigungsvergabe
Die Berechtigungsvergabe beschäftigt sich damit, welche Berechtigungen jeder Nutzer bekommt. Dies wird mittels Autorisierungsrichtlinien gesichert, damit die Nutzer nur Zugriff auf die Ressourcen und Dienste haben, welche diese benötigen. Dies wird mithilfe von Profilen erreicht, welche von der Organisation zugewiesen werden. [SSD15] (S.1482)

3. Identitätsvergabe
Die Identitätsvergabe sorgt dafür, dass der Nutzer eine digitale ID oder Account erhält. Wenn ein Mitarbeiter bei einem Unternehmen arbeitet, erhält dieser eine digitale Identität, um auf die Ressourcen des Unternehmens zugreifen zu können. Dabei ist auch wichtig, dass der Mitarbeiter diese digitale Identität wieder verliert, wenn dieser das Unternehmen verlässt oder an einer anderen Stelle im Unternehmen arbeitet und nicht mehr seine alte

digitale Identität benötigt.

4. Föderierte Identität
Dabei handelt es sich darum, dass die digitalen Identitäten über verschiedene Anwendungen und Organisationen gültig sind. Dadurch werden die Informationen der digitalen Identität gespeichert. Dies hat den Vorteil, dass der Nutzer sich nur einmal anmelden muss, um auf sämtliche seiner Ressourcen zugreifen zu können. Dabei werden Protokolle wie SAML, OAuth oder OpenID verwendet. Die Folge dadurch ist, dass der Nutzer sich nicht mehrere Passwörter sowie Accounts merken muss. [SSD15] (S.1482)

5. Compliance Verwaltung
Die Compliance Verwaltung überprüft die Authentifizierung- und Zugriffaufzeichnungen, um sicher zu stellen, dass die Richtlinien und Sicherheitsstandards eingehalten wurden. Diese Überprüfung ist notwendig für effektive Zugriffsregeln. Zudem werden diese für Audits benötigt. [SSD15] (S.1482)

Dies ist ein Beispiel, wie die oben genannten Punkte umgesetzt werden

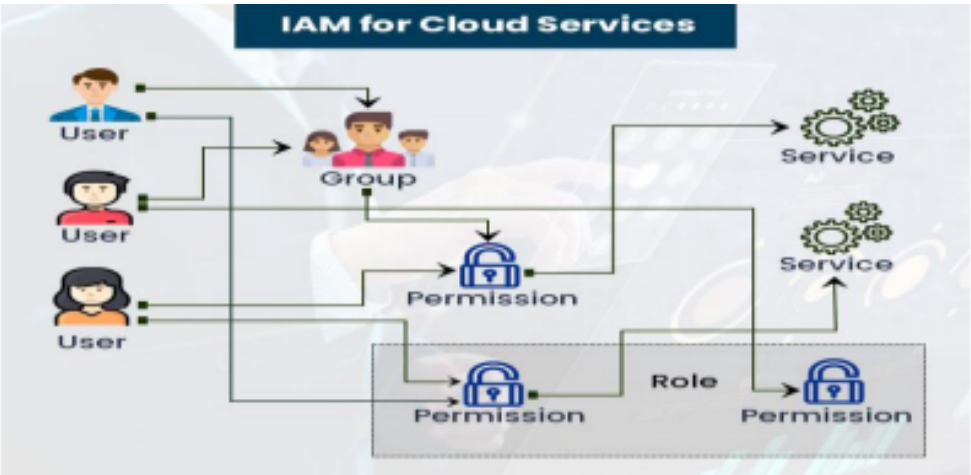

Abbildung 4.1: IAM für Cloud Dienste [Moh19] (Seite 3)

können. Dabei haben die Accounts der Personen entweder direkte Berechtigung oder diese werden mittels Gruppen verteilt. Sobald der Account die Berechtigung hat, kann dieser auf die dahinter steckende Ressource zugreifen. Die Berechtigungen können dabei auch mittels Profile zusammengefasst werden.
Dabei kann dies auf verschiedenen Wegen umgesetzt werden, da dieselbe Lösung für gewisse Fälle nicht funktioniert. Zum Beispiel die Quelle [Cal+17](S.208) beschreibt das Problem, wie die United States of America am besten mit ihren Verbündeten kooperieren soll. Da es sich dabei um sensitive Informationen handelt, welche an verschiedene Partner vermittelt werden, muss der Zugriff reguliert werden. Auch haben die verschiedenen Länder unterschiedliche Gesetzte, worauf geachtet werden muss. Deswegen

gibt es nicht die eine Lösung, um eine solche Herausforderung zu lösen. [Cal+17] (S.208)

4.1.2 *Vergleich mit Datenbanken*

Die Helvetia verwendet zum Speichern der Informationen für die Berechtigungsstruktur sogenannte HV-Tabellen. Bei diesen HV-Tabellen handelt es sich, um DB2-Tabellen. Zudem besteht eine Ähnlichkeit zwischen dem Nutzer und dem Profil in der Berechtigungsstruktur im Vergleich zum Account und der Gruppe in Datenbanken. Deswegen wird betrachtet, wie der Standard von Accounts und Gruppen innerhalb von Datenbanken ist.
Berechtigungen für Rollen werden mittels GRANT...ON...TO...[GRANT OPTION] vergeben. Dabei wird für die spezifische Berechtigung, zum Beispiel eine View und Account oder Gruppen angegeben. Zudem kann auch hinzugefügt werden, ob die Rolle die Berechtigung hat, anderen Accounts die Berechtigungen zu geben.[RAE09] (S.474-475)
Wenn man sich zum Beispiel das Bild (2.2) ansieht, könnte der Befehl wie folgt aussehen:

GRANT UPDATE ON PKU00 TO L895.

Das würde in diesem Beispiel bedeuten, dass der Nutzer L895 die Bearbeitungsberechtigung für die Ressource PKU00 erhalten hat. Dabei kommt auch die Frage, was man eher verwenden sollte. Individuelle Berechtigungsvergabe oder Gruppenvergabe für die Accounts. Microsoft hat folgendes als Best Practice definiert:

„To simplify administration, create groups and assign each group permission to functional areas and model objects. You can then add and remove users from the groups without accessing the Master Data Manager UI.

Do not assign additional permissions to an individual user, and do not include a user in multiple groups that have access to Master Data Manager. In addition, do not use hierarchy member permissions unless you want a group to have limited access to specific members.“ [Mic22]

Microsoft gibt an, dass man Gruppen erstellen soll. Die individuellen Nutzer sollen dabei keine zusätzlichen Berechtigungen bekommen. Ebenso ist es wichtig, dass diese nicht in mehreren Gruppen sind, welche Zugriff auf den Master Data Manager haben. Und auch IBM gibt in seiner Best Practice an, dass Angestellte in einem Unternehmen mittels Gruppen organisiert werden sollten. [IBM21]
Dies ist jedoch in der Praxis schwierig umzusetzen. Im Idealfall benötigt jeder Mitarbeiter ein oder zwei Standardprofile, welche dem Nutzer alle Berechtigungen geben. Dies ist aber selten der Fall, da die Nutzer nach Beispielsweise einem halben Jahr an einem anderen Projekt arbeiten und daher

andere Berechtigungen benötigen. Wenn man für jeden solchen Fall ein neues Standardprofil erstellt, werden diese unübersichtlich. Ebenso würde das Konzept der Standardprofile in Frage gestellt werden, wenn die Anzahl dieser Standardprofile der Anzahl der Berechtigungen gleicht. Dennoch sollte es versucht werden, dass Nutzer so wenig zusätzliche Berechtigungen wie möglich bekommen, um Best Practice Standards einzuhalten.

4.2 DSGVO

Neben den technische Herausforderunge und Anforderungen muss die Struktur neben dem VAIT auch den Standards vom Datenschutz-Grundverordnung (DSGVO) erfüllen. Bei Verstoß dieser kann es zur Verwarnung bis zum endgültigen Verbot zum Verarbeiten von den Daten kommen. [Koma] Dies würde die Helvetia sehr viel Geld kosten.
Eine sichere Berechtigungsstruktur ist daher nötig, um diese Anforderung von der DSGVO zu befriedigen. Diese ist nämlich verletzt, wenn Daten, für die das Unternehmen verantwortlich ist, von ihrer Vertraulichkeit, Verfügbarkeit oder Integrität verletzt werden. Deswegen sind Mitarbeiter, die mehr Berechtigungen, als die sie benötigen eine Risikostelle. [Komb]
Daher sollte die neue Berechtigungsstruktur so gestaltet werden, dass die Wahrscheinlichkeit, dass die Daten Vertraulichkeit, Verfügbarkeit oder Integrität nicht verletzt werden können.

4.3 HERAUSFORDERUNG UND ANFORDERUNGEN

Bei der Recherche (3) sind verschiedene Herausforderungen und Anforderungen aufgetreten. Um qualitativ ein Konzept entwickeln zu können, müssen diese Herausforderungen und Anforderungen aufgelistet und analysiert werden. Neben den genannten Punkten wurde der Punkte Implementierung hinzugefügt, da diese bei der Entscheidung der Konzepte elementar ist, da dass Unternehmen sich im Klaren sein muss, wie viele Ressourcen das neue Konzept kostet sowie der Punkt der Performance, da eine bessere Performance immer gut.

- Performance der Tabellen erhöhen
- Übersichtlicher gestalten (effizientere Verifizierung der Mitarbeiter)
- Rekursive Beziehungen verhindern
- Hierarchie verringern
- Konventionen/Wartbarkeit (K/W)
- Implementierung

Um diese zu quantifizieren zu können, wird eine Prioritätsanalyse (4.2) verwendet, um festzustellen, wie die Priorität für die Konzepte sein muss. [Hei]
Bei der Prioritätsanalyse wurde sich für ein vier Punktesystem entschieden.

Im Vergleich zwischen der Performance und der Übersichtlichkeit, wurden Performance drei Punkte gegeben und die Übersichtlichkeit hat nur einen Punkt erhalten, da die Performance eine der Grundanforderungen ist, weswegen die Berechtigungsstruktur geändert werden soll. Die Übersichtlichkeit dazu ist weniger wichtig. Die Performance und die Rekursion haben jeweils zwei Punkte bekommen, da eine performante Struktur keine rekursiven Beziehungen enthält. Die Performance hat vier Punkte zur Hierarchie und die Hierarchie zur Performance null Punkten erhalten, weil die Verringerung der Hierarchie kaum einen Einfluss auf die jährliche Rezertifizierung hat. K/W sowie Performance haben jeweils zwei Punkte bekommen. Dies liegt daran, dass neben der Performance die K/W elementar sind, da eine Struktur, die sich kaum warten lässt, mehr Ressourcen in der Zukunft kosten wird. Zwischen der Übersichtlichkeit und der Rekursion wurden der Rekursion drei Punkte gegeben und der Übersichtlichkeit nur einen, weil rekursive Strukturen unübersichtlicher sind und es daher wichtiger ist, dass es keine gibt. Übersichtlichkeit und Hierarchie haben beide zwei Punkte erhalten, da beide eine gleiche Rolle bei der Lesbarkeit der Struktur spielen. Übersichtlichkeit, sowie Rekursion und Hierarchie bekommen einen Punkt im Vergleich zu K/W, weil dieser Punkt langfristig eine wichtige Rolle spielt, und die anderen drei Punkte sollten keine Probleme sein, sofern sich an die Konventionen gehalten wird, damit die Struktur wartbar bleibt. Die Rekursion bekommt zur Hierarchie vier Punkte und die Hierarchie zur Rekursion null Punkte, da eine rekursive Beziehung die Hierarchie automatisch unendlich macht.

Wenn man dies auswertet, bekommt die Performance einen Gewichtsfaktor von 16,66667%, die Übersichtlichkeit 20%, die Rekursion 18,33333%, die Hierarchie 6,66667%, die K/W 18,33333% und Implementierung 20%. Dadurch sieht die Rangfolge wie folgt aus:

1. Implementierung | Übersichtlichkeit
2. Rekursion | K/W
3. Performance
4. Hierarchie

Anhand dieser Reihenfolge werden die folgenden Konzepte entwickelt.

Kriterien	Performance	Übersichtlich	Rekursive	Hierarchie	K/W	Implementierung	Summe je Krierium	Gewichtu	Rang
Performance		1	2	2	2	3	10	16,66667	3
Übersichtlich	3		2	3	2	2	12	20	1
Rekursive	2	2		4	2	1	11	18,33333	2
Hierarchie	0	1	2		1	0	4	6,666667	4
K/W	2	2	2	3		2	11	18,33333	2
Implementierung	1	2	3	4	2		12	20	1
Summe							60	100	

Abbildung 4.2: Prioritätsanalyse der Kriterien

4.4 KONZEPT HIERARCHISCHE STRUKTUR

Das erste Konzept für die Struktur ist wie folgt aufgebaut. Wie man in der

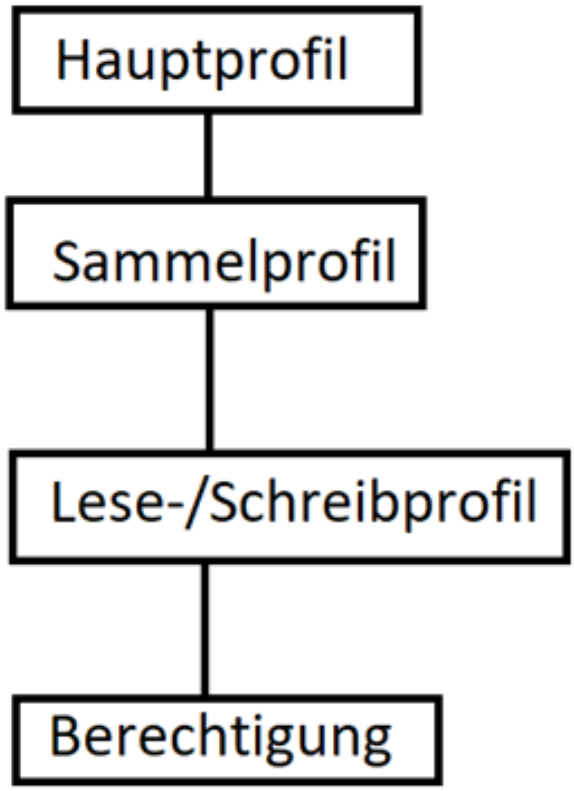

Abbildung 4.3: Hierarchie für Konzept Struktur

Grafik (2.3) aus dem zweiten Kapitel erkennen kann, gibt es bei der aktuellen Berechtigungsstruktur keine Struktur. Um dementsprechend die genannten Problem zu beheben, wurde die neue Struktur (4.3) entwickelt. Um die K/W zu verbessern, wurden die folgenden Konventionen für dieses Konzept entwickelt. Anzumerken dabei ist, dass es trotzdem ein Aufwand ist, diese durchzusetzen und zu implementieren.

- Profile enthalten nur noch Profile oder Berechtigungen.
- Die Berechtigungsstruktur soll nur noch eine Hierarchietiefe von maximal vier haben.
- Die erste Hierarchiestufe enthält das Standardprofil, welche dem Nutzer gegeben wird.
- Die zweite Hierarchiestufe enthält die jeweiligen Sammellese- und -schreibprofile, die jeweils in die Fachbereiche getrennt sind.
- Die dritte Hierarchiestufe enthält die individuellen Lese- und Schreibprofile.

- Die vierte Stufe enthält die Berechtigungen.
- Manche der bestehenden Profile beinhalten aktuell, was zukünftig Hauptprofile wären. In solchen Fällen würden diese Profile zu Hauptprofilen werden und vom vorherigen Hauptprofil separiert werden.
- Manche Fachbereiche haben aufzählende Profile (3.6). Diese Profile sollen nur noch über die Berechtigungen für den eigenen Vorgang enthalten, sodass ein Privas Profil nur Privas Berechtigungen enthält. Die Berechtigung die verloren gehen würden eigene Profile bekommen und würden über ein anderes Sammelprofil dem Hauptprofil hinzugefügt werden.
- Sollte ein Nutzer weitere Berechtigungen benötigen, würden diese direkt ihm zugewiesen werden.
- Wenn ein Account reaktiviert wird, muss dieser rezertifiziert werden.

Diese Konventionen sollen verhindern, dass die Struktur weiter wächst und das man ohne Probleme feststellen kann, was für Berechtigungen ein Profil hat. Zudem hat es den Vorteil, dass rekursive Beziehungen, sowie redundante Berechtigungsvergabe nicht möglich sind, da die Profile nur noch Profile oder Berechtigungen enthalten, die nicht mehr auf sich gegenseitig zeigen. Dadurch soll auch die Übersichtlichkeit verbessert und das Hierarchieproblem auf ein Minimum gebracht werden. Außerdem sollte die Performance verbessert werden. Dies durch die fehlenden rekursiven Beziehungen, sowie die Vereinfachung der Struktur, mit der Reduktion der Berechtigungen. Das Bild (4.4) zeigt eine bestehende Berechtigungsstruktur. (4.5) hingegen bildet die Struktur nach den neuen Konventionen dar. Diese beide Bilder wurden den IT-Spezialisten gezeigt, die befragt wurden. Einheitlich haben alle befragten IT-Spezialisten angegeben, dass Sie die neue Struktur übersichtlicher finden und diese einfacher zu verstehen ist. Zudem kann auch erkannt werden, dass die Hierarchie verringert wurde.
Das aktuelle Verfahren, das verwendet wird, um die Berechtigung zu überprüfen, gleicht einem Insertion-Sort. Dabei wird jedes einzelne Profil durchgegangen, bis die gewünschte Berechtigung gefunden wurde. Dies weißt eine Komplexität von n im Optimalfall und n^2 im schlimmsten Falle auf. n beschreibt dabei, die Anzahl von Profilen/Berechtigungen, die der Algorithmus durchlaufen muss. [Wol20a; Cor+09] (S. 12)
Bei der neuen Struktur kann ein Merge-Sort genutzt werden. Dabei achtet der Algorithmus auf bestimmte Eigenschaften der Profile. Würde zum Beispiel verlangt werden, dass der Nutzer eine Berechtigung für PNE10 hat, würde nur der Baum von PNE durchsucht werden und in diesem Falle direkt PNE10 ausgewählt werden. Dieser Suchalgorithmus ist komplexer als der Insertion-Sort. Er ist jedoch deutlich effizienter bei einer größeren Menge von Profilen und Berechtigungen. Die Komplexität beläuft bei ihm auf n*log(n) im besten, wie auch im schlechtesten Fall. [Wol20b; Cor+09] (S. 12)
Wenn beispielsweise n = 100 wäre, würden die Ergebnisse wie folgt aussehen:

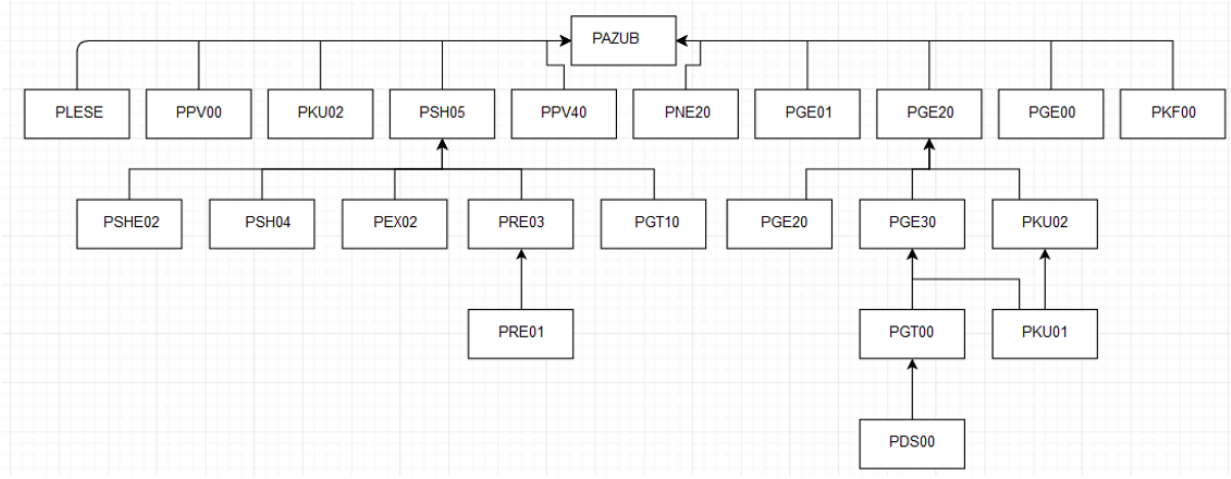

Abbildung 4.4: Beispiel der bestehenden Berechtigungsstruktur

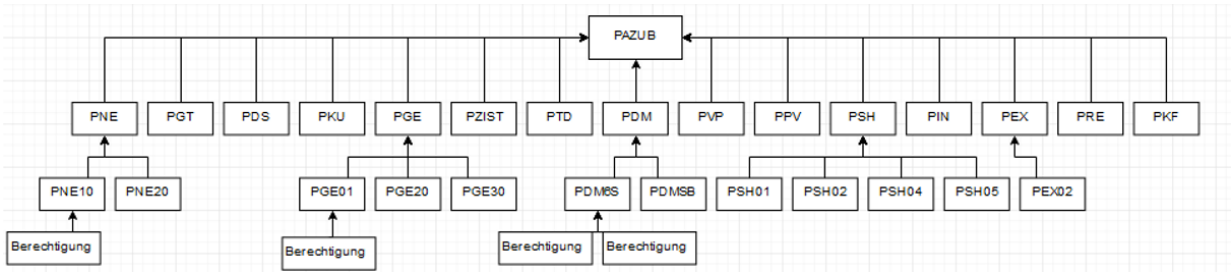

Abbildung 4.5: Beispiel der neuen Berechtigungsstruktur

Best-Case(Insert) = 100
Worst-Case(Insert) = $100^2 = 10.000$

Best-Case(Merge) = $100 * log(100) = 200$
Worst-Case(Merge) = $100 * log(100) = 200$

Wie man erkennen kann, ist der neue Algorithmus im Best-Case langsamer, aber im Worst-Case deutlich schneller und bietet allgemeinen eine konsistente Zeit, welche für eine Versicherung wichtig ist. Der Insertion-Sort sowie der Merge-Sort haben auch eine average Formel: [Wol20b; Wol20a]

Average(Insert) = $100^2 = 10.000$

Average(Merge) = $100 * log(100) = 200$

Man kann erkennen, dass im normalen Falle die neue Struktur mit dem Merge-Sort deutlich effektiver ist als die bestehende Struktur. Diese würde durchschnittlich 50 mal effektiver sein.

Die Entwicklung dieses Konzeptes ist aufwendig und komplex. Es gibt dabei zwei Möglichkeiten wie dieses umgesetzt werden kann. Die erste Möglich-

keit besteht dabei, dass sich eine Gruppe von Entwicklern an die bestehende Struktur setzen, eine Kopie davon erstellen und anhand der Kopie die neue Struktur erstellen. Dies ist jedoch Zeit aufwendig und es besteht ein hohes Potenzial, dass Fehler geschehen durch nachlässiges Arbeiten.
Die zweite Möglichkeit wäre eine Algorithmus zu schreiben, welcher dies automatisiert. Da weder die Zeit besteht noch die entsprechende Umgebung zum Testen eines Prototypen, kann die Entwicklung des Algorithmus innerhalb dieser Arbeit nur mittels von Pseudocode stattfinden. Dabei würde die Automatisierung wie folgt aussehen.

Algorithmus conversionToNewStructure(DB2 T)

Input Eine DB2 Tabelle T, welche die Struktur enthält

Output Neu DB2 Tabelle T, welches die neue Struktur von Profilen enthält.

Der Algorithmus muss dabei die Profile in zwei Kategorien aufteilen:

- Standardprofil
- Lese-/Schreibeprofil

Für die Standardprofile werden die Profile überprüft, die viele Unterprofile haben. Wenn ein Profil X Y viele Unterprofile hat, wird dieses zu einem Standardprofil. Die restlichen Profile werden zu Lese-/Schreibeprofile. Die individuellen Sammelprofile werden basierend auf den Lese-/Schreibeprofile generiert. Die Verbindungen zwischen den bisherigen Profilen wird aufgebrochen und zu den neuen Sammelprofilen zu gewiesen, welche mit dem Standardprofil verbunden sind. Anschließend werden auf redundante Profile und Berechtigungen überprüft, welche dann entfernt werden. Dabei muss man aber zum Schluss begutachten, ob alle generierten Standardprofile wirklich Standardprofile sein sollten sowie ob die bestehende Anzahl ausreichend ist. Die Grafik (4.6) stellt dies als ein Ablaufdiagram dar.

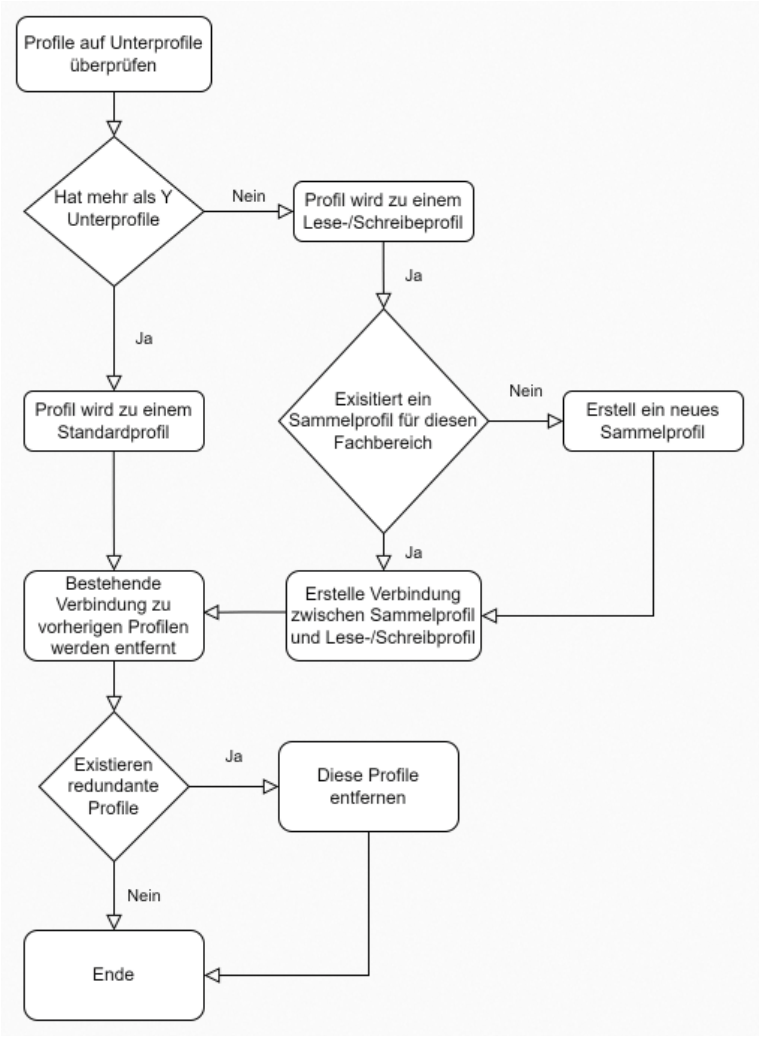

Abbildung 4.6: Ablaufdiagram für das hierarchische Struktur Konzept

4.5 KONZEPT MINIMALISTISCH

Im Gespräch der IT-Spezialisten kam der Vorschlag auf, dass man einen minimalistischen Ansatz nutzen könnte. Dabei haben die IT-Spezialisten folgende Vorschläge für die Konventionen gemacht:

- Profile enthalten nur noch Profile oder Berechtigungen.
- Es werden Standardprofile für die jeweiligen Abteilungen entwickelt.
- Nutzer, die in verschiedenen Abteilungen operieren erhalten, die jeweiligen Standardprofile.
- Zusätzliche Berechtigungen werden dem Nutzer direkt zu geordnet.
- Wenn ein Account reaktiviert wird, muss dieser rezertifiziert werden.

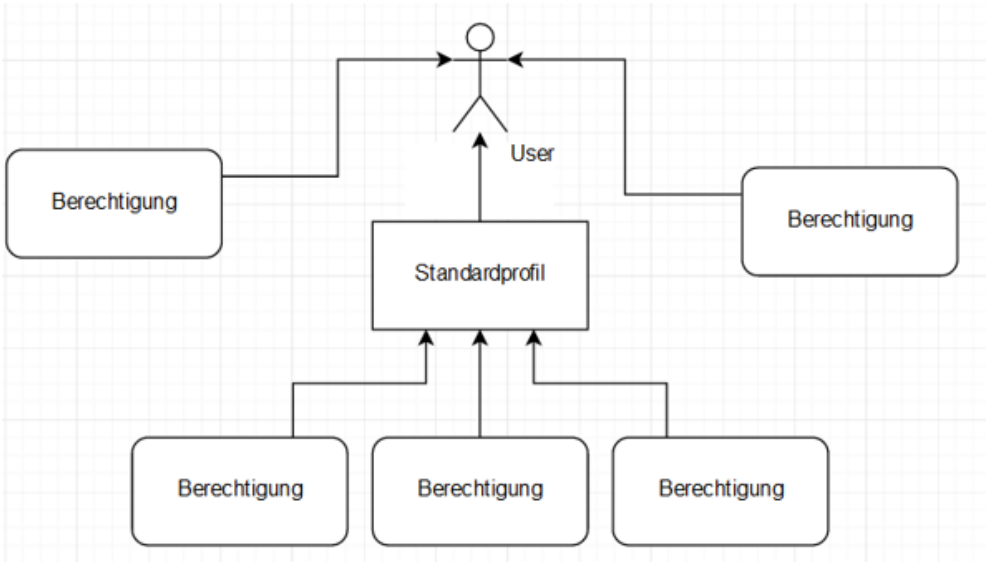

Abbildung 4.7: Beispiel für das Konzept Minimalistisch

Die IT-Spezialisten fanden auch, dass dies übersichtlicher als die bestehende Struktur ist. Dieses Konzept hat den Vorteil, dass es kaum noch eine Hierarchie gibt. Dadurch entfällt das Problem der Rekursion sowie redundante Berechtigungsvergabe. Die K/W ist einfacher in diesem Sinne, da nur überprüft werden muss, ob die Standardprofile über die notwendigen Berechtigungen verfügen. Auf der anderen Seite ist die Entwicklung aufwendig, da erst einmal bestimmt werden muss, welche Berechtigungen für einen Fachbereich notwendig sind. Ebenso muss sichergestellt werden, dass alle Nutzer ihre Berechtigungen beibehalten. Es besteht nämlich die Gefahr, dass bei dem Wechsel Berechtigungen verloren gehen.

Wenn man (4.7) betrachtet, kann für diese Struktur nur ein Insertion-Sort verwendet werden. Dies liegt daran, dass der Sort die individuellen Einträge durchlesen muss, da es keine Information gibt, wo welche Berechtigung ist. Die aktuelle Struktur verwendet auch einen Insertion-Sort, aufgrund des gleichen Problems. Jedoch ist zu bemerken, dass die Anzahl der n bei diesem Konzept geringer ist, da es nicht die verschiedenen Profile mit Redundanzen gibt.

Ein Hauptprofil hatte zum Beispiel 110 Profile mit enthalten Berechtigungen. Von diesen 110 waren 78 redundante Profile. Da Profile eine Ansammlung von Berechtigungen sind, ist die Anzahl von redundanten Berechtigungen deutlich höher. Wenn man nur den Unterschied zwischen der bestehenden Struktur mit der minimalistischen Struktur macht, erhält man folgenden Vergleich:

Best-Case(Alte Struktur) = 110
Worst-Case(Insert) = $110^2 = 12.100$
Average(Insert) = $110^2 = 12.100$

Best-Case(Neue Struktur) = 32
Worst-Case(Neue Struktur) = $32^2 = 1.024$
Average(Neue Struktur) = $32^2 = 1.024$

Man kann feststellen, dass obwohl die neue Struktur nicht über einen effizienteren Algorithmus verfügt, dieser trotzdem eine bessere Performance hat. Die neue Struktur wäre in diesem Beispiel ca. 12 mal performanter als die bestehende Struktur.

Ebenso kann für dieses Konzept eine manuelle Lösung verwendet werden sowie eine automatische. Wie im vorherigen Fall kann eine Kopie vom vorherigen Konzept erstellt werden, welches dann in das neue Konzept modeliert wird. Jedoch wird der Prozess der individuellen Berechtigungsvergabe zu den einzelnen Nutzern zeitaufwendig sein. Dabei können auch Berechtigungen verloren gehen und dies wäre ein Problem.
Als Alternative kann ein Algorithmus verwendet werden. Dieser ist dem vorherigen in der Grundstruktur gleich:

Algorithmus conversionToNewStructure(DB2 T)

Input Eine DB2 Tabelle T, welche die Struktur enthält

Output Neu DB2 Tabelle T, welches die neue Struktur von Profilen enthält.

Der Algorithmus würde die komplette bisherige Struktur auseinanderbrechen. Anschließend werden die Standardprofile anhand der Fachbereiche neu geformt und den Nutzern der jeweiligen Bereiche zugewiesen. Die bisherigen Berechtigungen werden anschließend den Nutzern direkt angehängt. Redundate Berechtigungen werden entfernt. Die Grafik (4.8) stellt dies als ein Ablaufdiagram dar.

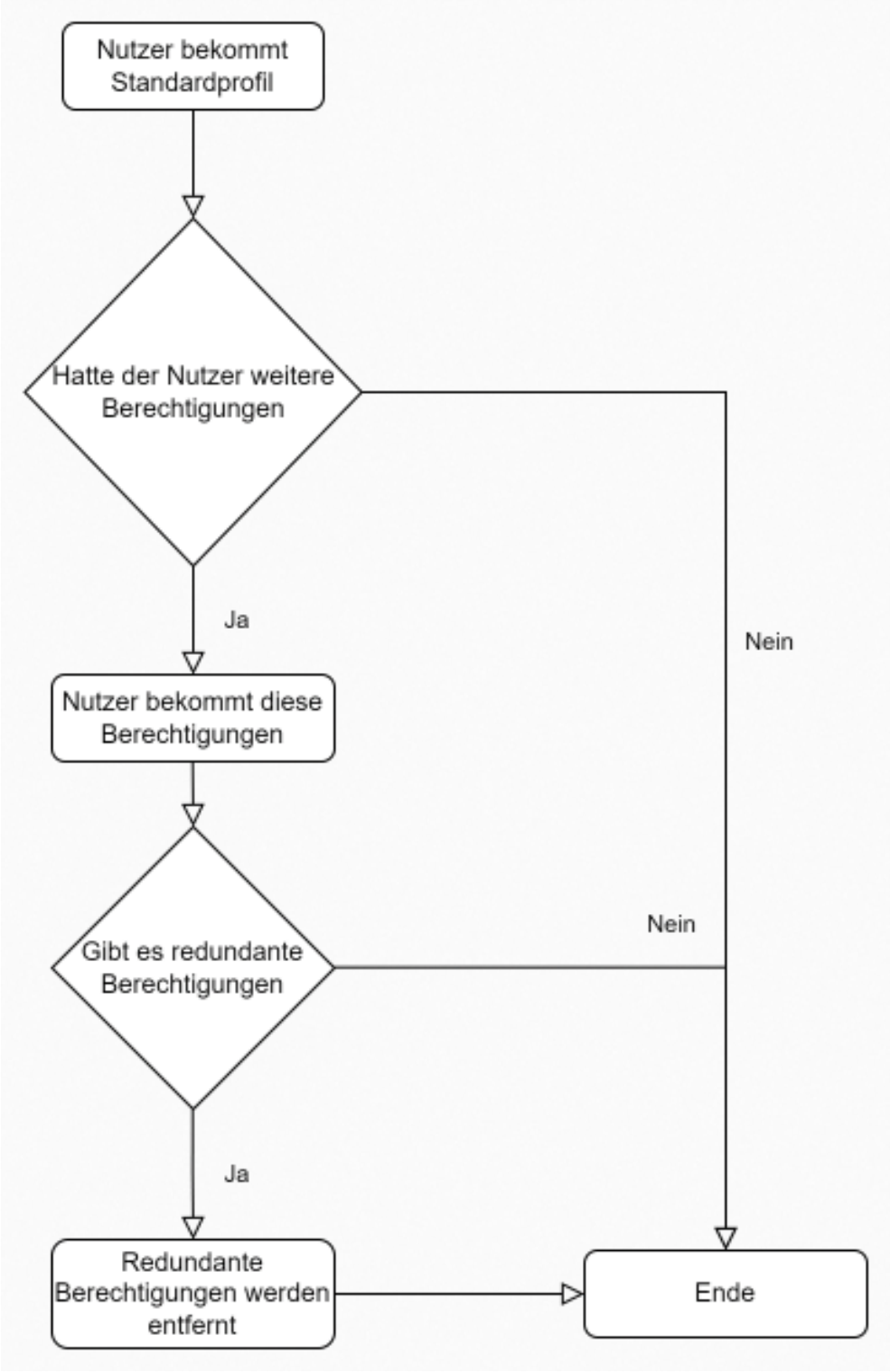

Abbildung 4.8: Ablaufdiagram für das Minimalistisch Konzept

5 VERGLEICH

In diesem Kapitel werden die beiden Konzepte „hierarchische Struktur“ und „minimalistisch“ mittels einer Nutzwertanalyse betrachtet. Diese sollen helfen herauszufinden, welches der beiden Konzepte die vorher genannten Kriterien am besten erfüllt. Dabei werden die Ergebnisse der Prioritätsanalyse verwendet und basierend auf dem Erfolg, welches das Konzept für das jeweilige Kriterium hat, verrechnet und addiert. Das Konzept mit einem höheren Wert erfüllt mehr die Kriterien als das andere. Zum Abschluss wird die alternative racF begutachtet auf ihre Vor- und Nachteile.

5.1 NUTZWERTANALYSE

Für die Nutzwertanalyse müssen die jeweiligen Teilnutzwert (TN) bestimmt werden. Dies wird mittels Gewichtsfaktoren (Gf) mal der Zielerfüllungsfaktor (Zf) gemacht. Daraus bildet sich der TN und die Summe davon generiert den Gesamtnutzwert (GN). Der höhere GN zeigt, dass dieses Konzept einen höheren Nutzen hat. Anzumerken dabei ist, dass wenn die GN zu ähnlich sind, weitere Schritte vorgenommen werden sollen, um ein eindeutiges Rank zu erschaffen. Für die Zf wurde wieder ein vier Punktesystem ausgewählt. Die Tabelle (5.3) zeigt, was die verschiedenen Zahlen bedeuten. [Hei]

Erfüllung des Kriteriums	Zielerfüllungsfaktor
nicht erfüllt	0
ausreichend	1
befriedigend	2
gut	3
sehr gut	4

Abbildung 5.1: Die Zf Tabelle

		Hierarchische Struktur		Minimalistisch	
Kriterien	Gf(%)	Zf	TN	Zf	TN
Performance	16,66666667	4	66,666667	2	33,33333
Übersichtlich	20	4	80	1	20
Rekursive	18,33333333	4	73,333333	4	73,33333
Hierarchie	6,666666667	1	6,6666667	4	26,66667
K/W	18,33333333	4	73,333333	2	36,66667
Implementierung	20	2	40	4	80
Summe	100	GN:	340	GN:	270

Abbildung 5.2: Nutzwertanalyse für die beiden Konzepte

Wie man erkennen kann ist der GN zwischen den beiden Faktoren bei 70. Da kein Unterschied erkannt werden kann, werden die Wertmaßstäbe weiter verfeinert. Dadurch ändert sich die Punkteskala und die Tabelle wie folgt:

Erfüllung des Kriteriums	Zielerfüllungsfaktor
nicht erfüllt	0
mangelhaft	1
ausreichend	2
befriedigend	3
vollbefriedigend	4
gut	5
sehr gut	6
hervorragend	7
exzellent	8

Abbildung 5.3: Die Zf Tabelle

		Hierarchische Struktur		Minimalistisch	
Kriterien	Gf(%)	Zf	TN	Zf	TN
Performance	16,66666667	8	133,33333	4	66,66667
Übersichtlich	20	8	160	4	80
Rekursive	18,33333333	8	146,66667	8	146,6667
Hierarchie	6,666666667	4	26,666667	8	53,33333
K/W	18,33333333	7	128,33333	4	73,33333
Implementierung	20	4	80	6	120
Summe	100	GN:	675	GN:	540

Abbildung 5.4: Nutzwertanalyse für die beiden Konzepte

Durch die Verfeinerung liegt der Unterschied zwischen den beiden Faktoren bei 135. Wodurch das Konzept der hierarchischen Struktur eindeutig im Rank an der ersten Stelle steht.

5.2 VOR/NACHTEILE DER HIERARCHISCHEN STRUKTUR

Bei der ersten Tabelle (5.3) wurden der hierarchischen Struktur für Performance vier, für Übersichtlichkeit vier, für Rekursion vier, für Hierarchie eins, für K/W vier und für die Implementierung zwei Punkte gegeben. Die Performance hat vier bekommen, da die Effizienz durch den Algorithmus im Allgemeinfall um die 50 Mal effektiver ist. Dies ist eine enorme Steigerung, weshalb es die maximale Punktzahl bekommen hat. Die Übersichtlichkeit hat vier Punkte erhalten, weil die Entwickler einstimmig dieses Konzept als übersichtlicher empfinden. Zudem ist es einfacher festzustellen, welches Profil, welche Aufgabe hat. Aber es hat zwei Punkte verloren dadurch, dass die Grafik bei weiteren Profilen schwieriger zu lesen wird, da diese größer ist. Rekursion hat vier Punkte erlangt, da es durch die Regelung, dass Profile nur noch Profile oder Berechtigungen enthalten sowie die feste Struktur keine rekursiven Beziehungen möglich sind, sofern man nicht aktiv gegen die Regelungen verstößt. Deshalb hat es wie Performance vier Punkte erhalten. Für die Hierarchie hat die Struktur nur einen Punkt bekommen, weil es bei diesem Punkt darum ging die Hierarchie so stark wie möglich zu verringern. Es ist besser als die vorherige Hierarchie, aber dennoch sehr hierarchisch. Die K/W haben nur vier Punkte bekommen, da nach der Entwicklung der Profile, diese nicht mehr geändert werden sollen. Die Implementierung hat lediglich zwei Punkte bekommen, da diese aufwendig.

Nachdem die Zf erweitert wurde, haben sich die Werte wie folgt verändert. Der Performance wurden acht Punkte, der Übersichtlichkeit acht, der Rekursion acht, der Hierarchie vier, der K/W sieben und der Implementierung vier Punkte gegeben. Wie schon im vorherigen Absatz angegeben wurde, kann dieses Konzept 50 Mal effektiver sein. Deshalb habe ich diesem Punkt exzellent gegeben, da dies eine deutliche Verbesserung ist. Die Übersichtlichkeit hat ebenso eine exzellente Bewertung erhalten. Die Struktur ist geordnet

nach den Fachbereichen und hat ein Hierarchielimit von vier. Dies ist der Rahmen, wodurch die IT-Spezialisten dies als übersichtlich befinden. In der Kategorie Rekursion ändert sich nicht viel, weshalb es wieder volle Punktzahl erlangt. Die Hierarchie hat vier Punkte bekommen, da die Hierarchie, wenn auch nur minimal, verringert wurde. Dies würde nur drei Punkte geben, aber da auch die Hierarchiestufen auf vier limitiert wurden, hat dies einen weiteren Punkt gegeben. K/W hat nur sieben statt acht Punkte bekommen, da dieses Konzept, trotz dessen, dass es nicht geändert werden soll, in einem regelmäßigen Zyklus gewartet werden muss. Dies liegt daran, dass man überprüfen muss, ob nicht ein Entwickler aus Faulheit die Struktur geändert hat. Daher ist es eine hervorragende Lösung, aber man muss dennoch etwas berücksichtigen.

Zusammenfassend hat das Konzept der hierarchischen Struktur viele positive Aspekte. Unter diese Fallen zum Beispiel die erhöhte Performance sowie die Rekursion und die Übersichtlichkeit. Auf der anderen Seite ist dieses Konzept weiterhin sehr hierarchisch und die Implementierung ist aufwendig. Dies würde einiges an Personentagen sowie weiteres Geld kosten.

5.3 VOR/NACHTEILE MINIMALISTISCH

Das minimalistische Konzept hat für die Performance zwei, die Übersichtlichkeit eins, die Rekursion vier, die Hierarchie vier, die K/W zwei und die Implementierung vier Punkte erhalten. Durch die verringerte Struktur hat sich die Performance ebenso verbessert, aber dies ist keine permanente Lösung, da ein Ansteigen der Profilanzahl diesen Bonus nichtig macht. Aus diesem Grund hat es nur zwei Punkte bekommen. Die Übersichtlichkeit hat es nur einen Punkt erlangt. Auch wenn durch das Entfernen der Hierarchie weniger Verwirrung herrscht, ist es dennoch sehr unübersichtlich, wenn alle Berechtigungen, mit Ausnahme der Standardberechtigungen, direkt am Profil hängen. Da es keine tiefe Hierarchie mehr gibt, ist es auch unmöglich, dass es eine Rekursion gibt. Weshalb dieses Konzept in diesem Punkt die maximale Anzahl von Punkten erlangt. Wie schon angesprochen geht es bei dem Punkt Hierarchie darum, die Hierarchie so stark wie möglich zu reduzieren und dieses Konzept hat die Hierarchiestruktur auf ein Minimum gebracht. Somit erhält es vier Punkte. Die K/W haben zwei Punkte erlangt, da regelmäßig überprüft werden muss, ob Entwickler nicht aus verschiedenen Gründen zusätzliche Profile hinzufügen. Dies ist eine Sorge, da genau dies zur unübersichtlichen Berechtigungsstruktur geführt hat, die die Helvetia aktuell hat.

Nach der Spezifizierung hat sich die Bewertung des minimalistischen Konzepts wie folgt geändert. Die Performance wurde auf vier Punkte angepasst. Ebenso wurde die Übersichtlichkeit auf vier, die Rekursion auf acht, die Hierarchie auf acht, die K/W auf vier und die Implementierung auf sechs Punkte geändert. Der Punkt Performance hat die Bewertung befriedigend bekom-

men, da diese eine Verbesserung zur ursprünglichen Struktur ist. Dennoch muss berücksichtigt werden, dass dies sich mit einer wachsenden Struktur verschlechtern wird, weshalb diese Verbesserung nur temporär ist. Die Übersichtlichkeit hat die Note gut statt ein vollbefriedigend erhalten. Auch wenn durch die Struktur die Beziehungen zwischen den Berechtigungen und dem Nutzer simpler sind, ist das Betrachten dieser schwierig, wenn die Anzahl der Berechtigungen wächst. Dies liegt daran, dass die Berechtigungen nicht mehrmals an verschiedenen Stellen dem Profil zugewiesen werden. Die Rekursion erlangt ein exzellent, da es nicht möglich ist, eine rekursive Beziehung zu erstellen, außer, wenn ein Standardprofil auf sich selber zeigt. Die Hierarchie hat ebenso wie die Rekursion ein exzellent erhalten, da eine weitere Reduktion der Hierarchie für lediglich mehr Chaos sorgen würde, da dann alle Berechtigungen direkt am Nutzer hängen. Die K/W erlangt vier Punkte. Das minimalistische Konzept hat nicht viele Konventionen die überprüft werden müssen. Ebenso ist die Überprüfung einfach, da die Struktur so minimalistisch ist, aber es regelmäßig überprüft werden muss und das Risiko, dass ein Entwickler die Struktur ändert, ist hoch.

Zusammenfassend kann gesagt werden, dass das minimalistische Konzept am Hilfsreichsten ist, wenn man nach spezifischen Berechtigungen sucht. Durch die minimale Hierarchie gibt es nicht viele Stellen, die überprüft werden müssen oder Stellen, an denen Rekursionen entstehen können. Auf der anderen Seite ist jedoch die Verbesserung der Performance nicht stabil und kann sich schnell ändern, wenn weitere Profile hinzugefügt werden. Die Implementierung ist im Verhältnis zum Konzept der hierarchischen Struktur deutlich einfacher, da für jeden Fachbereich die Standardprofile entwickelt werden müssen und ansonsten die restlichen Berechtigungen direkt den Nutzern zu geteilt werden. Dadurch müssen keine neuen Profile entwickelt werden. Jedoch besteht die Gefahr, dass bei der Menge von Berechtigungen gewisse Nutzer bestehende Berechtigungen verlieren. Zudem könnte die Anzahl der individuellen Berechtigungen ein Problem darstellen, wenn diese abgespeichert werden sollen.

5.4 ABLÖSUNG INS RACF

Neben dem aktuellen DB2 Tabellen Modell ist auch intern der Gedanke aufgekommen, dass die bestehende Struktur in das Resource Access Control Facility (RACF) ausgelagert werden kann. Den die Helvetia verwendet aktuell schon Customer Information Control System (CICS) von IBM für die Kommunikation der internen Prozesse. Dabei wird auch das RACF verwendet. Aus diesem Grund wurde überlegt, ob nicht die DB2 Tabellen ebenso in diese Umgebung integriert werden sollen. Das hätte den Vorteil, dass sämtliche Prozesse an einem Ort stattfinden und daher die Suche etwas vereinfacht ist. Zudem würde man sich von der Welt des Hosts weiter distanzieren. Dies wäre ein positiver Aspekt, wenn das Unternehmen sich in der Zukunft vom Host lösen möchte.

Für den Wechsel zwischen der DB2 Tabelle zu RACF würden die Profile, Nutzer und Berechtigungen wie folgt geändert werden:

- Die HDM-Vorgangsprofile werden mittels Data Control Groups dargestellt
- Die Berechtigungen werden durch General Resource Profiles abgebildet
- Die Nutzer werden anhand von Holding Group verkörpert

Die Data Control Groups fungieren als ein Schnittpunkt für die Daten, welche vor nicht autorisierten Zugriff geschützt werden sollen. [IBM22a] Die General Ressource Profiles bieten einen Schutz an für Computer Ressourcen sowie andere Datenformate wie zum Beispiel Berechtigungen. [IBM23] Die Nutzer werden als Holding Group dargestellt, da diese den Nutzer in das bestehende System integriert, dieser aber kaum Berechtigungen erhält, wodurch er keinen Zugriff auf die Berechtigungen hat. Dies muss über einen Administrator, welcher über die CONNECT Autorität verfügt, verwaltet werden, damit der Nutzer seine Berechtigungen erhält. [IBM22b]

Auf der anderen Seite bestehen jedoch die folgenden Probleme:

- Bestehende Schnittstellen
- Transfer der Daten
- Schulung des Personals

Die aktuelle DB2 Tabelle verfügt über verschiedene Schnittstellen für die Abfrage von Berechtigungen. Wenn diese durch das RACF ersetzt werden sollen, müssen diese durch neue Schnittstellen ersetzt werden. Im Gespräch mit den IT-Spezialisten wurde gesagt, dass dies ein großes Problem aufweist, da dafür eine spezielle Application Programming Interface (API) entwickelt werden müsste. Dies würde neben dem normalen Wechsel von den DB2 Tabellen zu RACF für weitere Kosten sorgen.
Ein anderes Problem ist auch der Transfer der bestehenden Daten in das RACF. Für diesen Prozess müsste auch hier eine Schnittstelle entwickelt werden, welche bei dem Transfer die Daten in das richtige Dateiformat transformiert. Neben den steigenden Kosten bestehen auch das Risiko, dass bei der Transformation ein Fehler geschieht.
Selbst wenn die vorherigen beiden Punkte kein Problem darstellen, muss dennoch das gesamte Personal, welches mit den Tabellen gearbeitet hat, für das RACF geschult werden. Dies würde wieder Geld und Zeit kosten. Aufgrund dieser Faktoren ist der Wechsel in das RACF nicht ratsam, da zu viele große Probleme bestehen, welche Geld und Zeit kosten werden.
Sollte sich jedoch doch für das RACF entschieden werden, würde der Algorithmus wie folgt aussehen:

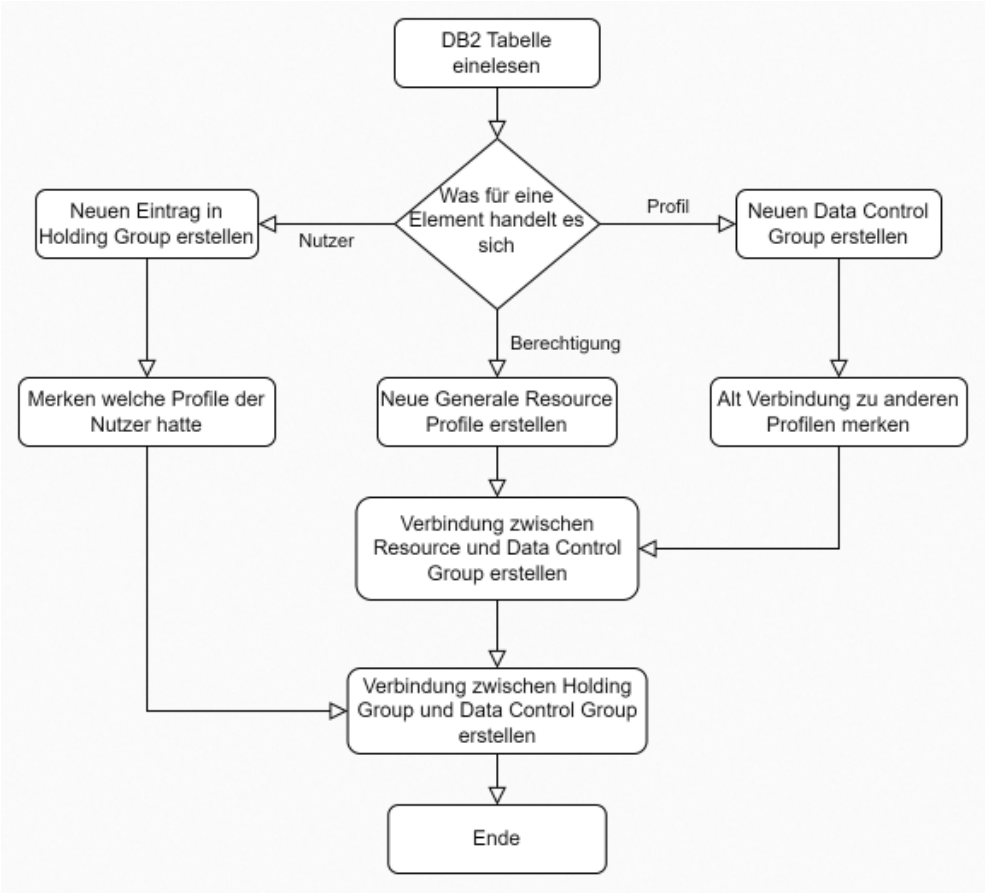

Abbildung 5.5: Algorithmus für den Wechsel zu RACF

6 FAZIT

6.1 EMPFEHLUNG

Die beiden Konzepte hierarchische Struktur sowie Minimalistisch haben ihr Vor- und Nachteile. Die je nach Umgebung besser oder schlechter geeignet sind. Im Falle der Helvetia ist zum Beispiel die hierarchische Struktur besser geeignet.
Die Implementierung ist definitiv aufwendiger als die des minimalistischen Konzepts, aber dafür ist diese übersichtlicher. Das minimalistische Konzept eignet sich mehr für eine Berechtigungsstruktur, die über weniger Berechtigungen verfügt, da ansonsten die Anzahl der individuellen Berechtigungen, die ein Nutzer hat, zu unübersichtlich wird. Bei einem kleinen Unternehmen, welches zum Beispiel nur über 50 Berechtigungen verfügt, wäre das minimalistische Konzept besser geeignet als das Konzept der hierarchischen Struktur, da bei einem solch kleinen Unternehmen die Mitarbeiter für verschiedenste Aufgaben arbeiten müssen. Daher sollte das Berechtigungskonzept einfach genug gestaltet sein, dass die Vergabe und das Entfernen von individuellen Berechtigungen so leicht wie möglich ist. Auf der anderen Seite braucht ein größeres Unternehmen wie die Helvetia mehr standardisierte Profile, da es nicht die Zeit und Ressourcen gibt, für jeden einzelnen Mitarbeiter ein individuelles Profil zu erstellen. Zudem muss auch berücksichtigt werden, dass diese Profile und Berechtigungen vermerkt werden müssen. Dies könnte sich als eine Herausforderung herausstellen, wenn ein Mitarbeiter über 100 zusätzliche Berechtigungen verfügt.
Außerdem ist die hierarchische Struktur im Bereich der Performance besser als das minimalistische Konzept. Dies ist allerdings kein Aspekt gewesen, welcher beim Projektantrag erwähnt wurde. Dennoch ist es von einer hohen Wichtigkeit, dass eine Versicherung in der Lage ist, zu jeder Zeit auf ihre Verträge sowie andere wichtige Dokument zugreifen zu können.
Zudem sollte auch die Wartung einfacher verlaufen, da es schneller auffällt, wenn ein Profil an einer Stelle hinzugefügt wurde, an der es nicht sein sollte. Dadurch wird die Wahrscheinlichkeit verringert, dass die Berechtigungsstruktur in der Zukunft unkontrolliert weiter wächst. Deswegen empfehle ich das Konzept der hierarchischen Struktur, da diese den Anforderungen besser genügt. Ebenso schätze ich die Langlebigkeit des Konzeptes höher ein sowie entspricht die hierarchischen Struktur auch eher dem Best Practice von Datenbanken.

6.2 AUSBLICK

Wie während der Arbeit sich herausgestellt hat, ist das Entwickeln von Konzepten für eine Berechtigungsstruktur keine einfache Aufgabe. Um eine geeignetes Konzept zu entwickeln, muss erstmal festgestellt werden, was die aktuellen Probleme sind. Methoden dabei wie Befragungen und Umfragen kosten viel Zeit und sind aufwendig zu gestalten, um so akkurate Ergebnisse wie möglich zu erhalten. Sowie muss sich informiert werden, welche Grundvoraussetzungen erfüllt werden müssen, die entweder vom Unternehmen oder der gesetzlichen Seite gestellt werden. Dabei variiert auch die Evaluierung der Konzepte, da je nach Anforderung dies sich ändern kann.
Bei der Arbeit wurden hauptsächlich Definitionen sowie Best Practises verwendet, da es wenig Material zum Thema Entwicklung von Konzepten für Berechtigungsstrukturen gibt. Wobei das Best Practise immer möglich ist umzusetzen. Dabei ergibt sich die Fragen, infolge dieser Arbeit die genannte Vorgehensweise auch für andere Strukturen genutzt werden kann.
Zudem muss in der Zukunft weiterhin auf die Berechtigungsstrukturen geachtet werden. Denn diese haben eine wichtige Rolle im Bereich der Versicherungen wie den Banken. Sollte es dabei zu Problem kommen, hätte dies einen hohen finanziellen Preis. In der Zukunft ist es möglich, dass es Tools geben wird, die automatisch solche Strukturen generieren, basierend an den Anforderungen. Natürlich müssten diese von Personen überprüft werden, dass es keine Fehler gab, aber diese könnte bessere Strukturen für individuelle Problem generieren im Vergleich zu einem Menschen.

LITERATUR

[BaF] BaFin. *Rundschreiben 10/2018 (VA) in der Fassung vom 03.03.2022*. https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1810_vait_va_Aktualisierung_2022.html;jsessionid=9DC73C48C10237A42D3E6023C1849A5B.1_cid502?nn=9021442. Accessed: 2022-01-06.

[Cal+17] Zach Calhoun, Patrick Maribojoc, Ned Selzer, Leah Procopi, Nicola Bezzo und Cody Fleming. "Analysis of Identity and Access Management alternatives for a multinational information-sharing environment". In: *2017 Systems and Information Engineering Design Symposium (SIEDS)*. 2017, S. 208–213. DOI: 10.1109/SIEDS.2017.7937718.

[Cen] Pew Research Center. *Writing Survey Questions*. https://www.pewresearch.org/our-methods/u-s-surveys/writing-survey-questions/. Accessed: 2022-12-26.

[Cor+09] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest und Clifford Stein. *Introduction to Algorithms, Third Edition*. 3rd. The MIT Press, 2009. ISBN: 0262033844.

[Dic] Oxford Learner's Dictionaries. *Structure*. https://www.oxfordlearnersdictionaries.com/definition/english/structure_1. Accessed: 2022-01-08.

[Hei] Bundesministerium des Innern und für Heimat. *6.5.2 Qualitative Bewertungsmethoden*. https://www.orghandbuch.de/OHB/DE/Organisationshandbuch/6_MethodenTechniken/65_Wirtschaftlichkeitsuntersuchung/652_Qualitative/qualitative_inhalt.html. Accessed: 2022-01-21.

[Hel] Helvetia. *Hast du angebissen?* Accessed: 2022-01-16; Interne Webseite der Helvetia.

[IBM] IBM. *What is a mainframe?* https://www.ibm.com/topics/mainframe. Accessed: 2022-01-06.

[IBM21] IBM. *Understanding user groups*. https://www.ibm.com/docs/en/imdm/10.1?topic=transactions-understanding-user-groups. Accessed: 2022-01-20. März 2021.

[IBM22a] IBM. *Data control groups*. https://www.ibm.com/docs/en/zos/2.5.0?topic=groups-data-control. Accessed: 2022-02-06. Mai 2022.

[IBM22b] IBM. *Holding groups*. https://www.ibm.com/docs/en/zos/2.5.0?topic=groups-holding. Accessed: 2022-02-06. Okt. 2022.

[IBM23] IBM. *RACF general resource profiles*. https://www.ibm.com/docs/en/cics-ts/5.6?topic=facilities-racf-general-resource-profiles. Accessed: 2022-02-06. Jan. 2023.

[Koma] Europäische Kommision. *Was geschieht, wenn eine Behörde die Datenschutzvorschriften nicht erfüllt?* https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-if-public-administration-fails-comply-data-protection-rules_de. Accessed: 2022-02-13.

[Komb] Europäische Kommision. *Was ist eine Verletzung des Schutzes personenbezogener Daten und was ist in einem solchen Fall zu tun?* https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_de. Accessed: 2022-02-13.

[ML19] Liam McNabb und Robert S. Laramee. "How to Write a Visualization Survey Paper: A Starting Point". In: *Eurographics 2019 - Education Papers*. Hrsg. von Marco Tarini und Eric Galin. The Eurographics Association, 2019. DOI: 10.2312/eged.20191026.

[Mic22] Microsoft. *Users and Groups (Master Data Services)*. https://learn.microsoft.com/en-us/sql/master-data-services/users-and-groups-master-data-services?view=sql-server-ver16. Accessed: 2022-01-20. Nov. 2022.

[Moh19] Ishaq Azhar Mohammed. "CLOUD IDENTITY AND ACCESS MANAGEMENT – A MODEL PROPOSAL." In: 6.pp. 1-8 (Okt. 2019).

[Polo7] Dave Burhop DMV CIO; Chair Marie Greenberg DMV Director of IT Security; Joanne Maxwell DMV Director of Policy. *Identity and Access Management "I AM Who I Say I AM"*. Techn. Ber. Virginia IT Agency, Juni 2007.

[RAE09] Shamkant B. Navathe Ramez A. Elmasri. *Grundlagen von Datenbanksystemen*. 3. Aufl. Pearson Studium, 2009.

[SSD15] Anuja Sharma, Sarita Sharma und Meenu Dave. "Identity and access management- a comprehensive study". In: *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. 2015, S. 1481–1485. DOI: 10.1109/ICGCIoT.2015.7380701.

[ST] National Institute of Standards und Technology. *Security Authorization*. https://csrc.nist.gov/glossary/term/security_authorization. Accessed: 2022-01-07.

[Sta22] Statista. *Did your company encounter incidents concerning data theft, corporate espionage or sabotage during the last year?* https://www.statista.com/statistics/429724/cyber-attacks-directed-at-companies-germany/. Accessed: 2022-12-20. März 2022.

[Wol20a] Sven Woltmann. *Insertion Sort - Algorithmus, Quellcode, Zeitkomplexität*. https://www.happycoders.eu/de/algorithmen/insertion-sort/. Accessed: 2022-01-24. Juni 2020.

[Wol20b] Sven Woltmann. *Mergesort – Algorithmus, Quellcode, Zeitkomplexität*. https://www.happycoders.eu/de/algorithmen/mergesort/. Accessed: 2022-01-24. Aug. 2020.